# SolQDebug: Debug Solidity Quickly for Interactive Immediacy in Smart Contract Development

Inseong Jeon[1], Sundeuk Kim[1], Hyunwoo Kim[1], Hoh Peter In[1*]

[1*]Department of Computer Science, Korea University, 145, Anam-ro, Seonbuk-gu, 02841, Seoul, Republic of Korea.

*Corresponding author(s). E-mail(s): hoh_in@korea.ac.kr;
Contributing authors: iwwyou@korea.ac.kr; sd_kim@korea.ac.kr; khw0809@korea.ac.kr;

**Abstract**

Debugging Solidity contracts remains cumbersome and slow. Even a simple inspection, such as tracking a variable through a branch, requires full compilation, contract deployment, preparatory transactions, and step-by-step bytecode tracing. Existing tools operate only after execution and offer no support while code is under construction. We present SolQDebug, the first interactive, source-level assistant for Solidity developers that provides millisecond feedback before compilation or chain interaction. SolQDebug extends the Solidity grammar with interactive parsing, incrementally maintains a dynamic control-flow graph, and performs interval-based abstract interpretation guided by inline test annotations, enabling developers to simulate symbolic inputs and inspect contract behavior as in traditional debugging environments. In an evaluation on real-world functions, SolQDebug enables low-latency, statement-level analysis during development without requiring compilation or deployment.

**Keywords:** Smart Contract Development, Solidity, Debugging, Abstract Interpretation

## 1 Introduction

Smart contracts are the backbone of decentralized applications, and Solidity has become the dominant language for writing them (3; 29). As contracts grow more complex and control more assets, developers must reason about correctness throughout the development cycle—not just at deployment. Large language models (LLMs) such as

ChatGPT (2) or Llama (17) can assist with code generation but offer no guarantees of correctness. Ultimately, developers remain responsible for understanding variable interactions, control flow, and numeric boundaries during authoring.

Unfortunately, the debugging workflow for Solidity lags far behind traditional programming environments. Even a single inspection requires full compilation, deployment, transaction-based state setup, and manual bytecode-level tracing. Tools like Remix IDE (23), Hardhat (12), and Foundry Forge (8) replicate this costly pipeline, providing no live feedback during edits. A prior study found that 88.8% of Solidity developers described debugging as painful, and 69% attributed this to the absence of interactive, source-level tooling Zou et al. (42). Despite this widely acknowledged pain point, we find no existing research or tooling that provides interactive feedback during Solidity code authoring—a gap that this paper aims to fill.

This paper presents SolQDebug, a source-level interactive Solidity debugger powered by abstract interpretation. Rather than replacing runtime debuggers, it complements them by enabling symbolic, per-statement inspection during code authoring—before compilation or deployment. It targets the Solidity pattern of single-contract, single-transaction execution, where each function is isolated and stateless—ideal for static reasoning but difficult to simulate manually. To support this, SolQDebug applies interval-based abstract interpretation, which generalizes over symbolic inputs, exposes edge-case behaviors, and provides sound results with low overhead. This approach gives developers immediate feedback and enables them to reason efficiently about how symbolic inputs influence variable behavior. Although these inputs enable generalization across multiple cases, certain input configurations or control structures may lead to wider output ranges. We evaluate these behaviors empirically and propose annotation strategies that help maintain interpretability across typical Solidity patterns.

To achieve this goal, SolQDebug builds on two core ideas. First, it extends the Solidity grammar with interactive parsing rules and dynamically updates the control-flow graph to reflect incremental edits, enabling keystroke-level structural changes during code authoring. Second, it performs abstract interpretation seeded by inline annotations. These annotations, written directly in the source code, allow developers to specify symbolic values for both parameters and storage variables, similar to how traditional debuggers let users configure initial states and explore control flow.

We evaluate SolQDebug on real-world functions from Zheng et al. (40), demonstrating millisecond-scale responsiveness under symbolic input. Beyond latency, we analyze how input interval structure affects interpretability in common Solidity patterns, such as division-normalized arithmetic.

This paper makes the following contributions:

- We identify the main barriers to interactive Solidity debugging: latency from compilation, deployment, and transaction setup, and EVM constraints that prevent lightweight re-execution.
- We design an interactive parser and dynamic control-flow graph (CFG) engine that supports live structural updates and syntactic recovery.
- We introduce an abstract interpreter that incorporates developer annotations as symbolic input, supporting fast, deployment-free debugging workflows.

- We implement and evaluate SolQDebug on real-world contracts, demonstrating its millisecond responsiveness and exploring annotation strategies that maintain interpretability under a range of symbolic input patterns.

# 2 Background

## 2.1 Structure of Solidity Smart Contract

Solidity smart contracts may declare contracts, interfaces, and libraries. Executable business logic typically resides in contracts, and functions serve as transaction entry points. Variables are usefully grouped as global (EVM metadata such as msg.sender or block. timestamp), state (persistent storage owned by a contract), and local (scoped to a call). Types include fixed-width integers, address, booleans, byte arrays, and user-defined structs; containers include arrays and mappings. A mapping behaves like an associative array with an implicit zero value for unseen keys and is not directly iterable. Storage classes (storage, memory, calldata) indicate lifetime and mutability; we mention them only to fix terminology. Visibility and mutability qualifiers (public, external, internal, private; pure, view, payable) exist but are not central to our single-contract, single-transaction setting. Control flow (if/else, while/for/do-while, break/continue, return) follows C/Java conventions.

**Listing 1** Minimal example used to illustrate grammar elements relevant to our analysis

```
1  contract Example {
2      address public owner;
3      uint256 public totalSupply = 1000;
4      mapping(address => uint256) private balances;
5
6      modifier onlyOwner() {
7          require(msg.sender == owner, "not owner");
8          _;
9      }
10
11     function burn(uint256 amount) public onlyOwner {
12         uint256 bal = balances[msg.sender];
13         uint256 delta;
14         if (bal >= amount) {
15             balances[msg.sender] = bal - amount;
16             delta = amount;
17         }
18         else {
19             delta = 0;
20         }
21         totalSupply -= delta;
22     }
23 }
```

The example highlights the specific features we rely on later. State variables include general types (owner, totalSupply) and a mapping from addresses to balances; global variables appear implicitly in guards via msg.sender. The function burn introduces

parameters and a local variable (bal). The modifier onlyOwner performs a precondition check before the function body executes; the placeholder underscore marks where the original body is inserted when the modifier is inlined. In analysis, such modifiers are expanded at their precise positions around the function body in the control-flow graph.

These grammar elements connect directly to our semantics. Guards such as require narrow feasible ranges along taken branches. Modifiers are inlined so that their precondition checks are analyzed in sequence with the function body. Containers like mappings remain symbolic until a concrete key is accessed, at which point an abstract value is materialized for that access. This level of detail suffices for our abstract interpretation in the single-contract, single-transaction scope without introducing parts of the language that our evaluation does not exercise.

## 2.2 Solidity Execution Model

To execute a Solidity contract on the blockchain, it must first be deployed. Deployment occurs through a one-time transaction that stores the compiled bytecode on-chain and invokes the constructor exactly once. After deployment, all subsequent interactions are message-call transactions. In these, the caller specifies a public function along with encoded calldata. Once the transaction is mined into a block, the Ethereum Virtual Machine (EVM) jumps to the designated entry point and executes the corresponding function sequentially. At runtime, Solidity variables fall into three distinct storage classes (29):

- **Global variables** represent implicit, read-only metadata provided by the EVM, such as `block.timestamp`, `msg.sender`, and `msg.value`.
- **State variables** store persistent data within the contract and retain their values across transactions.
- **Local variables** include function parameters and temporary values scoped to a single execution context.

These three classes share a unified type system comprising primitive types like `uint` , `int`, `bool`, and `address`, as well as composite types such as arrays, mappings, and structs. Composite values can be nested to arbitrary depth using field access (`.`) or indexing (`[]`). Control flow follows familiar C-style constructs such as `if`/`else`, `while`, `for`, and `return`, alongside Solidity-specific statements like `emit` and `revert`.

As a result, debuggers must resolve potentially complex, multi-step expressions to analyze deeply nested elements within the contract state.

## 2.3 Root Causes of the Solidity-Debugging Bottleneck

Debugging Solidity programs remains significantly slower than traditional application development workflows due to two orthogonal obstacles.

**(1) Environmental disconnect.** Unlike conventional IDEs such as PyCharm (14) or Visual Studio (20), where the source editor and execution engine run in the same process, Solidity development involves external coordination with a blockchain node at every stage of the workflow. Even a single debugging cycle must pass through four sequential stages (see Fig.1). First, the contract must be compiled. Then, the bytecode

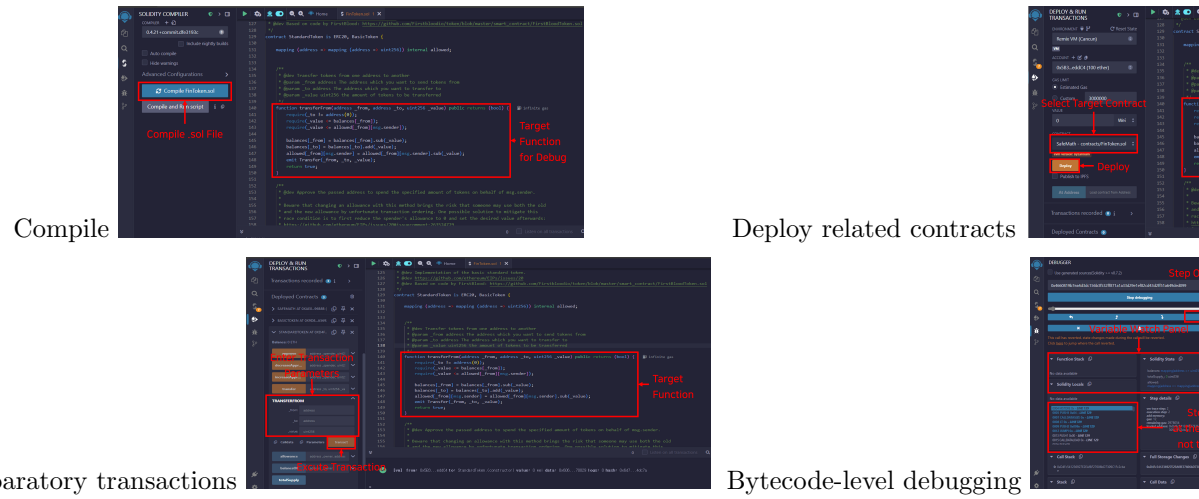


**Fig. 1** Traditional Solidity debugging workflow

is deployed to a local or test chain. Next, developers must manually initialize the on-chain state by sending setup transactions. Finally, the target function is invoked, and its execution is traced step by step at the bytecode level.

This workflow introduces several seconds to minutes of latency per iteration, fundamentally breaking the fast "type-and-inspect" feedback cycle expected in modern development tools. To mitigate this friction, developers often rely on `emit` logs or event outputs to observe intermediate values. However, such instrumentation provides only runtime snapshots and lacks the structural insight needed to understand symbolic variation or control-flow behavior. Moreover, modifying the expression of interest typically requires recompilation and redeployment, compounding latency and disrupting iteration. The final stage—tracing raw EVM opcodes—is particularly costly, as developers are forced to mentally reconstruct source-level semantics. This not only adds execution overhead but also imposes significant cognitive burden during fault localization and fix validation.

**(2) Architectural limitations of the EVM.** The Ethereum Virtual Machine (EVM) is a state-based execution engine in which each transaction mutates a globally persistent storage. Once a function executes, its side effects are irreversible unless external intervention is performed. Re-executing the same function along the same control path is nontrivial: developers must either redeploy the entire contract to restore the initial state, or manually reconstruct the required preconditions via preparatory transactions—both of which incur significant overhead.

Additionally, if a function includes conditional guards that depend on the current state—such as account balances or counters—then any debugging session must first ensure that those conditions are satisfied. Fig. 2 illustrates this challenge: the debug target function enforces a check on `_balances[account]`, requiring developers to manually assign a sufficient balance before they can observe the downstream effects on `_totalSupply`. Without such setup, the function exits early, preventing inspection of the intended execution path.

In short, these constraints make repeated debugging iterations costly and fragile. According to a developer study (42), 88.8% of Solidity practitioners reported frustration with current debugging workflows, with 69% attributing this to the lack of interactive, state-aware tooling.

### 2.4 Proposed Methodology and Technical Challenges

SolQDebug addresses the two root causes of Solidity's debugging bottleneck—external latency from blockchain round trips, and internal opacity due to storage-based semantics—through a pair of lightweight but complementary techniques.

**(1) Eliminating blockchain latency via in-editor interpretation.** The traditional debugging workflow requires compilation, deployment, transaction-based state setup, and bytecode tracing—each incurring significant latency. SolQDebug replaces this round trip by performing both parsing and abstract interpretation directly inside the Solidity Editor. To support live editing, we extend the Solidity grammar with interactive parsing rules tailored for isolated statements, expressions, and control-flow blocks. When the developer types or edits code, only the affected region is reparsed using a reduced grammar.

Each parsed statement is inserted into a dynamic control-flow graph (CFG), and abstract interpretation resumes from the edit point. The interpreter uses an interval lattice, assigning each variable a conservative range $[l, h]$ to expose edge conditions (e.g., overflows or failing guards) and to approximate groups of concrete executions that follow the same path. This enables millisecond-scale feedback on code structure and control flow without compilation or chain interaction.

**(2) Re-instantiating symbolic state without redeployment.** The EVM does not support reverting to a prior state without redeploying the contract or replaying transactions—both of which disrupt iteration. SolQDebug introduces batch annotations as a lightweight mechanism for symbolic state injection. In essence, this reflects a core debugging activity: varying inputs or contract state to observe control-flow outcomes. Rather than reconstructing such conditions through live transactions, developers can write annotations at the top of the function to define initial abstract values. These values are injected before analysis begins and rolled back afterward, ensuring test-case isolation.

This approach brings the debugging workflow closer to the source by making state manipulation explicit and reproducible within the code itself. Developers can explore alternative execution paths by editing annotations alone—without modifying the contract logic or incurring compilation and deployment overhead. It effectively decouples symbolic input configuration from the analysis cycle, while preserving the intuitive debugging process developers already follow.

## 3 The design of SolQDebug

### 3.1 System Architecture

SolQDebug receives incremental edits as its primary input—typically a snippet of Solidity code or an inline debug annotation. Rather than expecting complete programs,

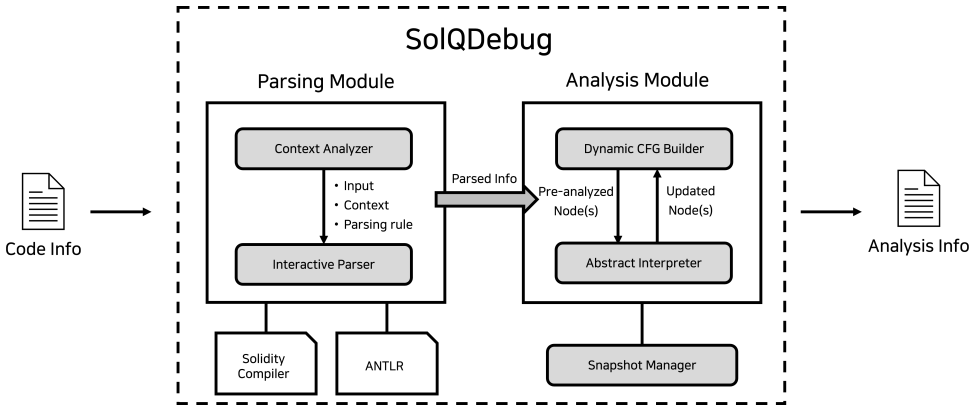


**Fig. 2** SolQDebug architecture.

the system is designed to accept fragments ranging from full statements to partial control-flow constructs. These edits include partial Solidity fragments and batch annotations, which are processed in isolation without requiring recompilation or transaction replay. The system assumes that each line contains at most one statement; compound forms such as `if (...) return;` are not supported. The structure of these inputs is described in Section 3.B; here, we outline the four-stage processing pipeline.

**(1) Parsing Module.** Each incoming edit first passes through the *Context Analyzer*, which reconstructs a source-level snapshot surrounding the modified lines, determines the enclosing contract or function, and selects the appropriate interactive grammar rule. Subsequently, the Interactive Parser, built atop ANTLR (1), applies an extended grammar that incorporates seven additional reduction rules to support isolated Solidity constructs such as expressions, statements, and definitions. A separate rule is dedicated to debug annotations, allowing single-line analysis directives to be parsed as valid units. To ensure syntactic integrity, the reconstructed source is also verified using the Solidity compiler before analysis proceeds. This allows the system to reject malformed fragments early and maintain consistency across the abstract syntax tree and control-flow graph. Debug annotations are parsed as valid syntactic units and forwarded for interpretation; their semantic effects are described in the analysis stage.

**(2) Analysis Module.** Each parsed statement is enriched with contextual metadata. This includes its enclosing contract and function, its semantic role (e.g., declaration or condition), and its static type. The statement is then forwarded to the Dynamic CFG Builder, which inserts a basic block at the precise edit point and rewires the surrounding control edges accordingly. Conditional branches merge incoming states using $\sqcup$, and loop headers are updated via localized fixpoint computation. The Abstract Interpreter propagates abstract values using a classic interval lattice. Types such as uintN and intN are interpreted as $N$-bit intervals. Boolean values are modeled as $\{0, 1\}$ intervals, and addresses as 160-bit unsigned intervals. Byte arrays and strings remain symbolic throughout. For composite containers such as structs, arrays, and mappings, the container itself is treated as symbolic until a specific field, element, or key is accessed. At that point, the interpreter materializes a fresh abstract

**Table 1** Incremental inputs for the running example

| Step | Lines of Input Fragment | Fragment |
|---|---|---|
| 1 | 11--12 | `function burn(uint256 amount) public onlyOwner {`<br>`}` |
| 2 | 12 | `uint256 bal = balances[msg.sender];` |
| 3 | 13 | `uint256 delta;` |
| 4 | 14--15 | `if (bal >= amount) {`<br>`}` |
| 5 | 15 | `balances[msg.sender] = bal - amount;` |
| 6 | 16 | `delta = amount;` |
| 7 | 18--19 | `else {`<br>`}` |
| 8 | 19 | `delta = 0;` |
| 9 | 21 | `totalSupply -= delta; // new input` |

value. If the base type is elementary, it receives the corresponding interval; otherwise, a new symbolic placeholder is propagated. Before each batch run, the Snapshot Manager saves the full abstract memory. Once execution completes, the snapshot is restored. This guarantees that consecutive test cases remain isolated and do not interfere with each other, even when global or local bindings are modified.

**(3) Line-Level Output.** After interpretation, the system emits a per-statement summary of relevant variable intervals. This includes:

- **Variable declarations:** the initial interval of the declared variable.
- **Assignments:** the updated interval of the left-hand side variable after evaluation.
- **Return statements:** the interval of the returned value or tuple of values.
- **Loops:** intervals for variables that changed during loop execution, computed after fixpoint convergence (loop delta).

All outputs are mapped to source line numbers and displayed directly in the Solidity editor, providing immediate, deployment-free feedback to developers.

## 3.2 Running Example

To make the architecture concrete, we walk through a small running example that exercises the main components of SolQDebug. The system operates as follows. First, each incremental source fragment is interpreted under abstract semantics to compute interval for the variables it touches. Second, the corresponding expression is stored in a CFG node that is inserted at a semantically valid point, determined from the edit's context and the existing control-flow. Third, when batch annotations are present, the entire function is reinterpreted using the pre-built CFG with the updated abstract state. We illustrate both modes—incremental source edits and batch annotations—using the burn function from Listing 1, and then refer back to the detailed mechanisms in §§3.3–3.5.

### 3.2.1 Source Code Analysis Example

Table 1 lists the incremental fragments a developer types for the function burn in Listing 1. SolQDebug accepts two kinds of fragments: (i) block fragments such as a

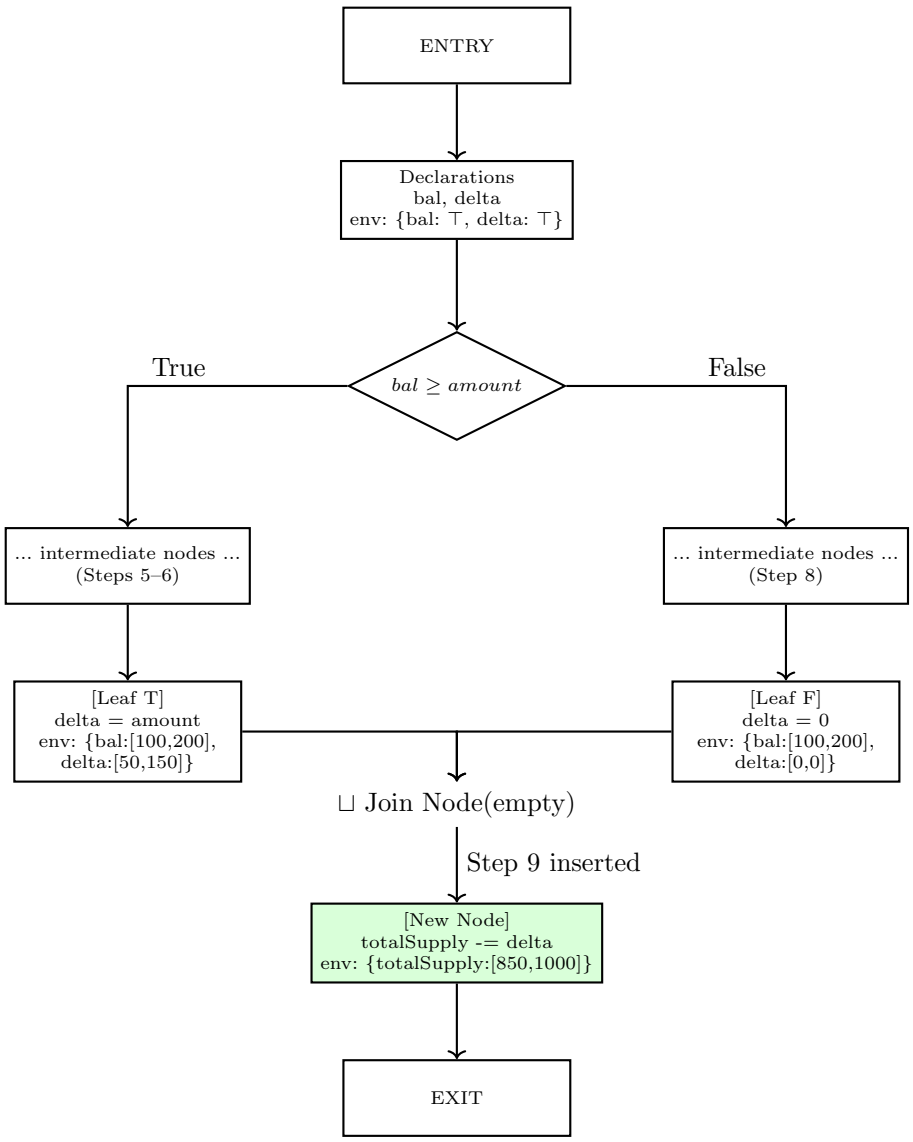


**Fig. 3** CFG structure showing Step 9 insertion. Each statement occupies a separate basic node; intermediate nodes along each branch are omitted, showing only the leaf nodes before the join point. The join point node is empty and serves only to merge the environments from both branches.

function header or an if/else block, and (ii) single statements that end with a semicolon. Most editors auto-insert a closing brace when "{" is typed, so a block fragment arrives as two lines at once (e.g., function ... { and the matching }). As the body is filled, the auto-inserted closing brace is pushed downward. The line numbers shown in the table refer to the listing 1; intermediate edits may temporarily place the closing brace earlier.

Figure 3 visualizes the state of the CFG after Steps 1–8 have already been integrated and shows how the new input in Step 9 (totalSupply -= delta;) is analyzed and inserted. For clarity, we focus on the function body in this running example and ignore the modifier referenced in the header; modifiers and their placement are treated in §3.5.

SolQDebug uses the following node semantics and bookkeeping rules:

- **Basic nodes.** A basic node contains a straight-line sequence of statements. As statements are evaluated in order, the node maintains the abstract environment at the end of the node—i.e., the interval for each variable. For later re-analysis (e.g., under batch annotations), the node also records its statement list.
- **Condition nodes.** A condition node stores only the predicate (e.g., `bal >= amount`) and does not update the environment at that point.
- **Branch refinement.** When the true/false successors of a condition are created, the incoming environment is pruned along each edge: the true successor refines intervals under the predicate, while the false successor refines them under its negation. Subsequent statements are analyzed under these pruned environments.

With these rules in place, the arrival of Step 9 proceeds as follows:

**(1) Parsing and semantics.** The interactive parser recognizes `totalSupply -= delta;` as a single assignment and constructs its abstract transfer function (§3.3).

**(2) Finding the insertion point.** Using the current edit context (line number and the stack of enclosing constructs) together with the existing CFG, SolQDebug locates the semantically valid insertion point. In this case the context indicates the join after the if/else, not merely the preceding line (§3.5).

**(3) Join environment (and localized fixpoint if needed).** If the insertion point has multiple predecessors, SolQDebug computes the least upper bound ($\sqcup$, JoinBranches) of their environments to create a join point node. If a loop header is on the path, a localized fixpoint is computed at the header before joining (§3.5).

**(4) Evaluation and rewiring.** A new basic node is created immediately after the join point node, and the assignment is evaluated in this new node using the joined environment to produce the new interval for `totalSupply`. The outgoing edges from the two branch leaves are rewired to the join point, which flows into the new node and then to the exit.

**(5) Reinterpretation from the insertion point.** To maintain soundness of the abstract interpretation, SolQDebug reinterprets all nodes reachable from the newly inserted node. Since the insertion changes the incoming environment for subsequent statements, the `reinterpret_From` function propagates the updated environment forward through the CFG, ensuring that all downstream intervals remain valid.

This design allows SolQDebug to reuse all path-local computations accumulated up to the leaves while maintaining semantic correctness at the insertion site. Although the narrative assumes sequential input, the same procedure applies to out-of-order edits (e.g., adding an else later). The insertion-point search, leaf collection, join/fixpoint handling, and edge rewiring remain unchanged and safely update the existing CFG.

### 3.2.2 Batch Annotation Analysis Example

**Listing 2** Burn function with batch annotations

```
function burn(uint256 amount) public onlyOwner {
    // @Debugging BEGIN
    // @StateVar balances[msg.sender] = [100,200]
    // @LocalVar amount = [50,150]
    // @Debugging END
    uint256 bal = balances[msg.sender];
    uint256 delta;
    if (bal >= amount) {
        balances[msg.sender] = bal - amount;
        delta = amount;
    }
    else {
        delta = 0;
    }
    totalSupply -= delta;
}
```

Batch annotations provide a declarative way for developers to specify initial state and parameters as symbolic (interval) values and to obtain line-level results by reinterpreting the program in a single pass over the already built CFG. In this work, "debugging" refers to the interactive exploration during pre-deployment editing in which the developer varies inputs (and state) to observe branch reachability, guard validity, and value bounds. Consequently, variables that are not given an initial range via annotations remain at the conservative $\top$, which can make results vacuous; this underscores the need for meaningful initialization in debugging. Batch annotations supply this initialization in a consistent and reproducible form.

In the running example, we augment the function `burn` in Listing 1 with the following lines: //@StateVar `balances[msg.sender]` $= [100, 200]$ and //@LocalVar `amount` $= [50, 150]$. We set the initial total supply to $totalSupply = 1000$. This choice makes the condition $bal \geq amount$ partially true, so both the then and else branches are reachable; it thereby exposes how pruning at branches and joining after the conditional affect the resulting bounds.

An annotation block is written between `//@Debugging BEGIN` and `//@Debugging END`, with one directive per line of the form "target L-value $\leftarrow$ abstract value (interval or symbolic)." Targets may be global, state, or local variables, and nested L-values (e.g., `a[i].x`, `balances[addr]`) are allowed. Integers are normalized to intervals respecting their declared bit width; addresses are interpreted as 160-bit unsigned intervals; booleans as $\{0, 1\}$.

Given a batch block, SolQDebug executes a lightweight pipeline: (i) parse each line, resolve symbols, and type-check; (ii) snapshot the current abstract memory and overlay the initial environment with the annotated values; (iii) traverse the existing CFG once from the function entry and perform abstract interpretation; condition nodes record only the predicate and do not immediately change the environment, while the true/false successor blocks refine (prune) their incoming environments under the

predicate and its negation; if loops are present, a localized fixpoint is computed at the loop header; and (iv) restore the snapshot to guarantee isolation across runs. This process is coordinated by the Snapshot Manager.

Importantly, batch annotations do not alter the CFG structure. No new nodes are inserted; only the initial environment changes, and the same CFG is reused. Each basic block retains its statement list and the abstract environment at the end of the block (interval per variable), enabling fast reevaluation. The rules for branch pruning, least upper bound (LUB) at joins (JoinBranches), and loop fixpoints are identical to those in the source-code example (§3.2.1). On the pre-built CFG in Figure 3, a batch run proceeds "entry → branch pruning → join → exit" in a single pass.

The concrete effect of the above annotations is as follows. From the statement $bal = \texttt{balances[msg.sender]}$ we obtain

$$bal \in [100, 200], \qquad amount \in [50, 150].$$

The guard $bal \geq amount$ is only partially true, thus both branches are reachable. After pruning, along the true branch the constraint $bal \geq amount$ raises the lower bound of $bal - amount$ to 0, yielding

$$\texttt{balances[msg.sender]} := bal - amount \;\Rightarrow\; [0,\ 200-50] = [0, 150], \qquad \delta := amount \;\Rightarrow\; [50, 150].$$

Along the false branch we only set $\delta := 0$, and `balances[msg.sender]` remains at its annotated initial range $[100, 200]$. At the join we compute

$$\delta \in [50, 150] \sqcup [0, 0] = [0, 150], \qquad \texttt{balances[msg.sender]} \in [0, 150] \sqcup [100, 200] = [0, 200].$$

We then evaluate the assignment to the total supply once in the join environment. With $totalSupply = [1000, 1000]$ initially,

$$totalSupply -= \delta \;\Rightarrow\; [1000, 1000] - [0, 150] = [850, 1000].$$

Thus, by combining branch-specific pruning with an LUB at the join, even a simple interval domain avoids unnecessary blow-up (e.g., the negative region of $bal - amount$ is eliminated on the true path) while conservatively aggregating the effects of both paths.

Containers (arrays, mappings, structs) are kept at $\top$ by default and are concretized on access or when a specific key/field is annotated. In our example, the mapping entry `balances[msg. sender]` is concretized by the annotation, and its effects propagate through the branch body and the join. State variables with explicit initial values, such as *totalSupply*, start from a fixed interval, so a single assignment yields directly interpretable bounds.

In summary, batch annotations standardize the essential debugging act of initial state specification via a simple comment syntax, enabling the developer to explore an intended input range in one shot. SolQDebug reuses the CFG and performs a single-pass reinterpretation, delivering lightweight yet semantically sound results. Formal details and algorithms appear in §3.3 and §3.5.

## 3.3 Interactive Parser

The standard Solidity parser accepts only whole files (`sourceUnit` → `EOF` ) and thus rejects partial fragments produced during editing. SolQDebug's interactive parser chooses fragment-specific entry rules based on the current editing context and parses each fragment into a syntactically well-formed subtree suitable for incremental analysis. The entry rules fall into two groups: (A) rules for Solidity program fragments (functions, blocks, and other constructs) and (B) rules for debugging-annotation blocks (`debugUnit`). We illustrate both groups with representative inputs.

### 3.3.1 Entry rules for Solidity program fragments

**1) `interactiveSourceUnit` — top-level declaration fragments**

- *Purpose.* Accepts top-level snippets such as function headers with empty bodies, contracts, interfaces, libraries, pragmas, imports, and state variables. Editors typically auto-insert a closing brace when "{" is typed, so a "skeleton" declaration arrives as two lines.
- *Example (cf. Table 1, Step 1).*

```
function burn(uint256 amount) public onlyOwner {
}
```

  *Selected entry:* `interactiveSourceUnit`. *Internal match:* `interactiveFunctionElement` → `functionDefinition`.
- *Other top-level examples.*

```
contract Example {}
uint256 public totalSupply = 1000;
```

  *Selected entry:* `interactiveSourceUnit` (matching `contractDefinition` / `stateVariableDeclaration`).

**2) `interactiveEnumUnit` — enum *member* lists added incrementally**

- *Two-phase input.*
  1. First, the empty enum *shell* at top level:

```
enum Status {}
```

     *Selected entry:* `interactiveSourceUnit`. *Internal match:* `interactiveStateVariableElement` → `interactiveEnumDefinition`.
  2. Then, members are supplied in subsequent fragments:

```
Pending, Shipped

Delivered
```

     *Selected entry:* `interactiveEnumUnit`. *Internal match:* `interactiveEnumItems`.
- *Rationale.* The enum *definition shell* and *member items* are parsed by different entry rules, allowing members to be typed incrementally after the shell is present.

**3) `interactiveStructUnit` — struct *member* declarations added incrementally**

- *Two-phase input.*

  1. First, the empty struct *shell*:

     ```
     struct A {}
     ```

     *Selected entry:* `interactiveSourceUnit`. *Internal match:* `interactiveStateVariableElement` → `interactiveStructDefinition`.
  2. Then, members are added one line at a time:

     ```
     uint a;
     address owner;
     ```

     *Selected entry:* `interactiveStructUnit`. *Internal match:* `structMember`.

**4) `interactiveBlockUnit` — block-local statements and skeleton control flow**

- *Purpose.* Accepts semicolon-terminated statements and fully-braced control-flow skeletons typed inside a block or function body.
- *Examples (cf. Table 1, Steps 2,3,5,6,8,9).*

  ```
  uint256 bal = balances[msg.sender];
  uint256 delta;
  balances[msg.sender] = bal - amount;
  delta = amount;
  delta = 0;
  totalSupply -= delta;
  ```

  *Selected entry:* `interactiveBlockUnit`. *Internal match:* `interactiveBlockItem` → `interactiveStatement` → `interactiveSimpleStatement`.
- *If-skeleton (cf. Table 1, Step 4).*

  ```
  if (bal >= amount) {
  }
  ```

  *Selected entry:* `interactiveBlockUnit`. *Internal match:* `interactiveBlockItem` → `interactiveIfStatement` .

**5) `interactiveDoWhileUnit` — the *while-tail* of a `do{...}` loop**

- *Two-phase input.*

  1. First, the `do` body skeleton:

     ```
     do {
     }
     ```

     *Selected entry:* `interactiveBlockUnit`. *Internal match:* `interactiveBlockItem` → `interactiveDoWhileDoStatement`.
  2. Then, the `while` tail is typed later:

     ```
     while (i < n);
     ```

*Selected entry:* `interactiveDoWhileUnit`. *Internal match:* `interactiveDoWhileWhileStatement`.

**6)** `interactiveIfElseUnit` — `else` / `else if` **tails**

- *Two-phase input.*
  1. First, the `if` skeleton (as above, parsed by `interactiveBlockUnit`).

     ```
     if (cond) {
     }
     ```

  2. Then, the tail is added:

     ```
     else {
     }
     ```

     or

     ```
     else if (guard) {
     }
     ```

     *Selected entry:* `interactiveIfElseUnit`. *Internal match:* `interactiveElseStatement`.

- *Context handling.* The parser uses the construct stack to attach the tail to the closest unmatched `if`, not merely the preceding line.

**7)** `interactiveCatchClauseUnit` — `catch` **clauses following a** `try`

- *Two-phase input.*
  1. First, the `try` skeleton:

     ```
     try doSomething() {
     }
     ```

     *Selected entry:* `interactiveBlockUnit`. *Internal match:* `interactiveTryStatement`.
  2. Then, one or more `catch` clauses:

     ```
     catch {
     }
     ```

     or

     ```
     catch Error(string memory) {
     }
     ```

     *Selected entry:* `interactiveCatchClauseUnit`. *Internal match:* `interactiveCatchClause`.

**Context-aware entry-rule selection**

- *Construct stack.* The context analyzer maintains a lightweight stack tracking:
  - Current nesting: contract → function → block depth
  - Unmatched constructs: open `if`, `do`, `try` awaiting their tails

- *Selection algorithm.*
  1. Inspect stack top to determine enclosing context
  2. Match fragment's first token against candidate entry rules
  3. For two-phase constructs (enum/struct members, `else`, `catch`), check if corresponding shell exists
  4. Select the most specific rule; fall back to `interactiveSourceUnit` for top-level
- *Consistency guarantee.* Each selected rule produces a syntactically well-formed subtree that can be spliced into the global AST/CFG without invalidating existing structure.

### 3.3.2 Entry rules for debugging-annotation fragments

**`debugUnit` — batch-annotation lines inside `//@Debugging` blocks**

- *Purpose.* Parses annotation lines that assign abstract values (intervals or symbolic tags) to designated variables, independent of Solidity AST completeness. Enables developers to specify initial states for interactive exploration without deploying contracts.
- *Annotation types.*
  - `@StateVar`: Assigns values to contract state variables and their nested elements (mappings, arrays, structs)
  - `@LocalVar`: Assigns values to function parameters and local variables
- *Supported L-value patterns.*
  - Simple variables: `amount`, `totalSupply`
  - Array/mapping access: `balances[msg.sender]`, `arr[0]`
  - Struct fields: `user.balance`, `data[key].field`
  - Nested combinations: `a[i].x`, `m[addr].arr[j]`
- *Value specification syntax.*
  - Integer intervals: `[100,200]` (normalized to declared bit width: `uint8` $\rightarrow$ `[0,255]`, `int256` $\rightarrow$ `[`$-2^{255}$`,`$2^{255}$`-1]`)
  - Address intervals: `[0x0,0xFFFF...FFFF]` (160-bit unsigned, clamped to valid range)
  - Boolean intervals: `[0,1]` representing {`true`, `false`}, or explicit `true`/`false`
  - Symbolic values: `TOP` or omitted (defaults to $\top$, representing all possible values)
- *Block structure and examples.*

```
// @Debugging BEGIN
// @StateVar balances[msg.sender] = [100,200]
// @LocalVar amount = [50,150]
// @StateVar totalSupply = [1000,1000]
// @Debugging END
```

  Each directive occupies one line. Multiple directives are processed sequentially, building up the initial abstract environment before function reinterpretation begins.

- *Selected entry:* `debugUnit`.
- *Internal match:* `debugStateVar` / `debugLocalVar`.
- *Error handling.*
  - Type mismatches: Rejected with diagnostic (e.g., assigning string interval to `uint256`)
  - Undefined variables: Reported as parse errors referencing the annotation line
  - Out-of-bounds intervals: Clamped to type's valid range with warning (e.g., `uint8` interval `[0,300]` → `[0,255]`)
  - Invalid L-values: Rejected if base container type does not support the access pattern
- *Integration with analysis pipeline.* The parsed annotations are consumed by the Snapshot Manager (§3.4.3) to overlay the initial abstract environment. The Abstract Interpreter (§3.5) then re-executes the function on the pre-built CFG without recompilation or deployment, producing line-level interval results under the specified initial conditions.

## 3.4 Dynamic CFG Construction

This section explains how we dynamically extend the control-flow graph while a user edits code. We proceed in three steps. First, we construct and splice a CFG fragment for each statement form and rewire only the neighborhood of the current node. Second, we locate the insertion site (the current block) using a successor-first, line-aware selection strategy. Third, we re-interpret only the affected region after splicing to update abstract environments.

### 3.4.1 Statement-Local, Incremental Construction

We introduce the node kinds that make up the CFG, then show how each major statement is translated into a small CFG fragment and spliced locally. Every edit operates at an INSERTION SITE—the block immediately preceding the new fragment—without restructuring the rest of the graph.

**Node kinds.**

- BASIC NODE: Holds exactly one statement (e.g., a variable declaration, an assignment, or a function call).
- CONDITION NODE: Represents branching constructs such as `if`, `else if`, `while`, `require`/`assert`, and `try`.
- RETURN NODE: A statement node whose outgoing edge is immediately rewired to the function's unique RETURN EXIT.
- ERROR NODE: The function's unique ERROR EXIT (targets the exceptional path).
- FIXPOINT EVALUATION NODE ($\phi$): The loop join used for widening and narrowing.
- LOOP EXIT NODE: The false branch that leaves a loop.

Figure 4 shows a simple statement. The builder creates one BASIC NODE and splices it between the current node and the original successors. Incoming environment is copied from the current node; all outgoing edges of the current node are reattached

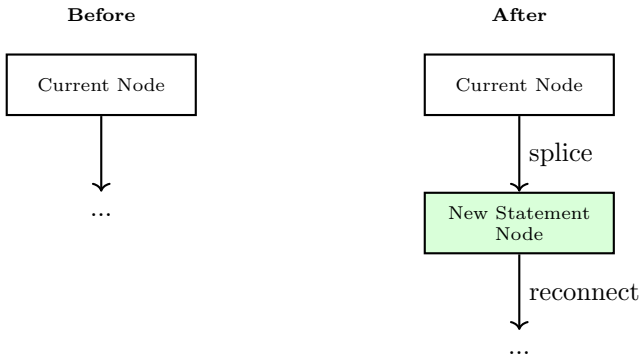


**Fig. 4** Simple statement insertion. The builder creates one node and splices it between the current node and the original successors.

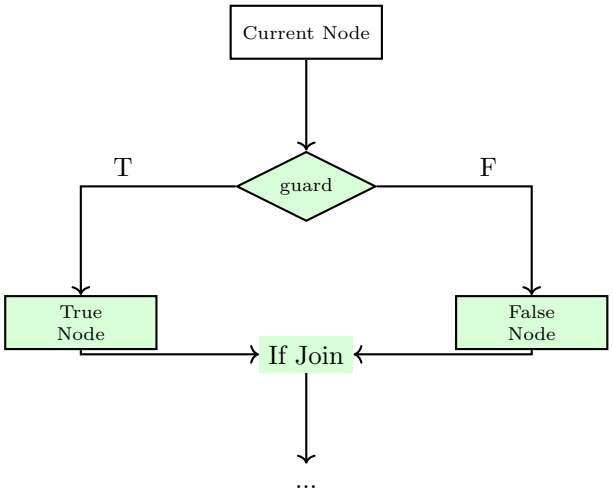


**Fig. 5** If statement insertion. The builder creates a CONDITION NODE, two nodes for true/false arms, and an IF JOIN.

to the new basic node. We deliberately store *exactly one* statement per basic node so that mid-line insertions become $O(1)$ splices via the editor-to-CFG line map, without scanning or splitting multi-statement blocks.

Figure 5 shows an `if`. The builder inserts a CONDITION NODE for the guard, two BASIC NODES for the true/false arms, and an IF JOIN. Edges: current → condition; condition → true basic (true edge) and → false basic (false edge); both basics → if join; the if join reconnects to the original successors. Environments on the two edges are refined by the truth value of the guard.

Figure 6 shows an `else if`. The builder removes the previously created false arm of the nearest preceding `if`/`else if` at the same nesting depth and splices a fragment consisting of a new CONDITION NODE, two BASIC NODES, and an ELSE-IF JOIN. The

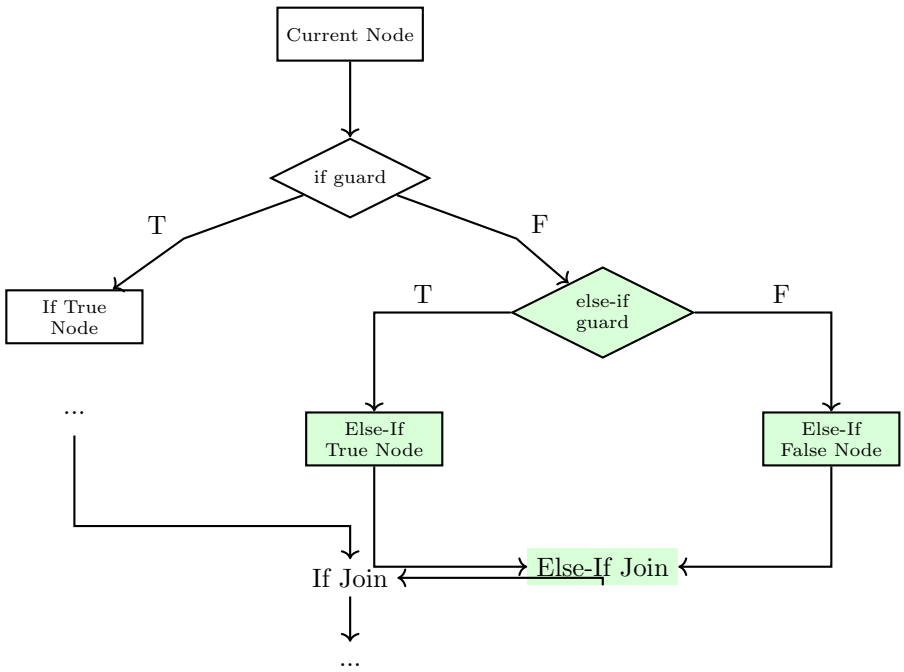


**Fig. 6** Else-if statement insertion. The builder replaces the false arm with a new CONDITION NODE, two nodes, and an ELSE-IF JOIN.

else-if join is connected to the existing IF JOIN so the overall shape remains a single diamond toward the if join.

Figure 7 shows an `else`. No new condition is created; the builder attaches a BASIC NODE to the false branch of the corresponding `if`/`else if` and connects it to the same IF JOIN as the true branch. The figure assumes a canonical `if`/`else if`/`else` chain. For nested patterns (e.g., `if { if {} else {} }`), the else attaches to the false arm of its matching guard according to standard block matching.

Figure 8 shows a `while`. The builder creates a FIXPOINT EVALUATION NODE $\phi$, a CONDITION NODE, a true-arm BASIC NODE as the loop-body entry, and a LOOP EXIT NODE (false arm). Rewiring: current $\rightarrow \phi \rightarrow$ condition; condition(true) $\rightarrow$ body; body $\rightarrow \phi$ (back edge); condition(false) $\rightarrow$ loop exit; the loop exit reconnects to the original successors. The $\phi$ node stores both the pre-loop baseline and the running snapshot for widening/narrowing.

Figure 9 shows a `break`. The statement becomes a BASIC NODE whose outgoing edge is redirected to the LOOP EXIT NODE. The loop exit's environment is conservatively joined with the environment at the break site.

Figure 10 shows a `continue`. The statement becomes a BASIC NODE whose outgoing edge is redirected to the loop's FIXPOINT EVALUATION NODE $\phi$. Operationally, this keeps the back-edge shape and joins the current environment into the loop's join state.

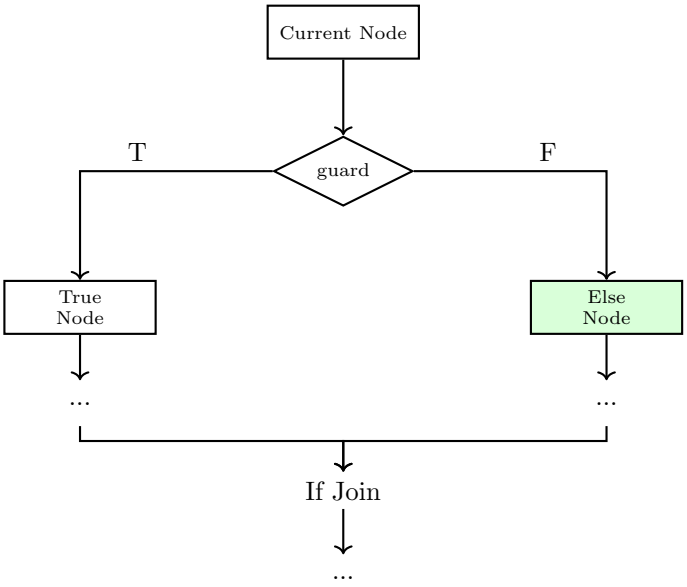


**Fig. 7** Else statement insertion. The builder attaches a node to the false branch of the corresponding `if`/`else if`, connecting to the IF JOIN.

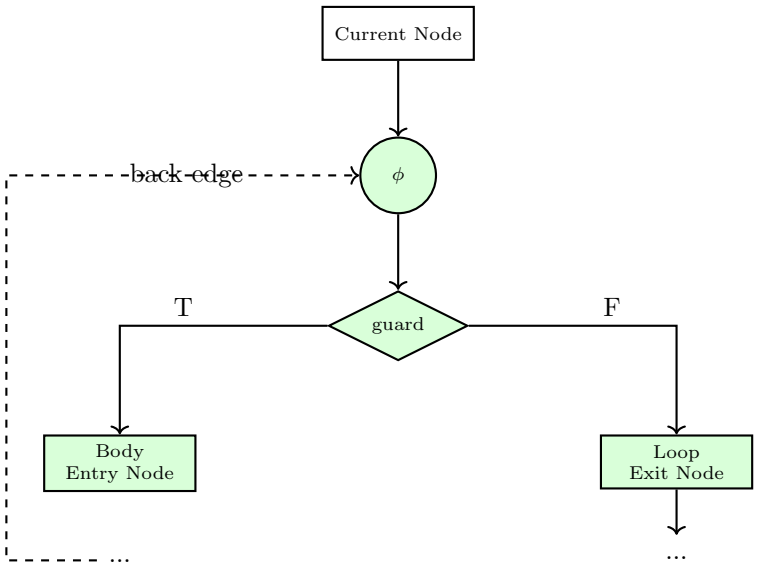


**Fig. 8** While loop insertion. The builder creates a FIXPOINT EVALUATION NODE $\phi$, a CONDITION NODE, a loop body node, and a LOOP EXIT NODE.

Figure 11 shows a `return`. The statement becomes a RETURN NODE and is immediately rewired to the function's unique RETURN EXIT; the return value is recorded there and the original successors of the current node are detached.

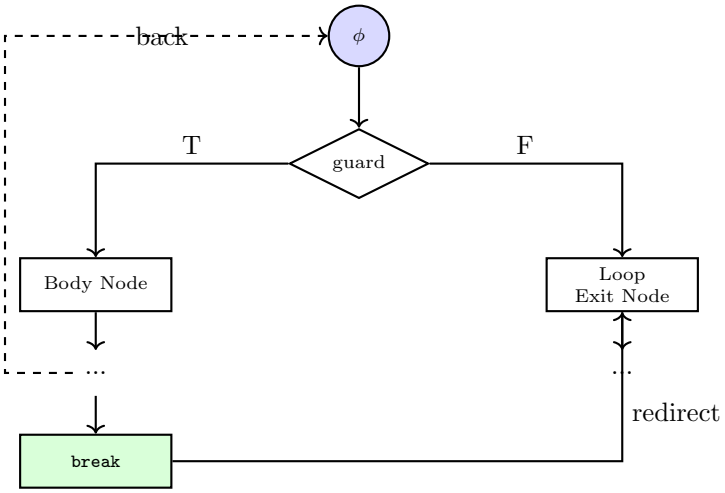


**Fig. 9** Break statement insertion. The `break` node's outgoing edge is redirected to the LOOP EXIT NODE.

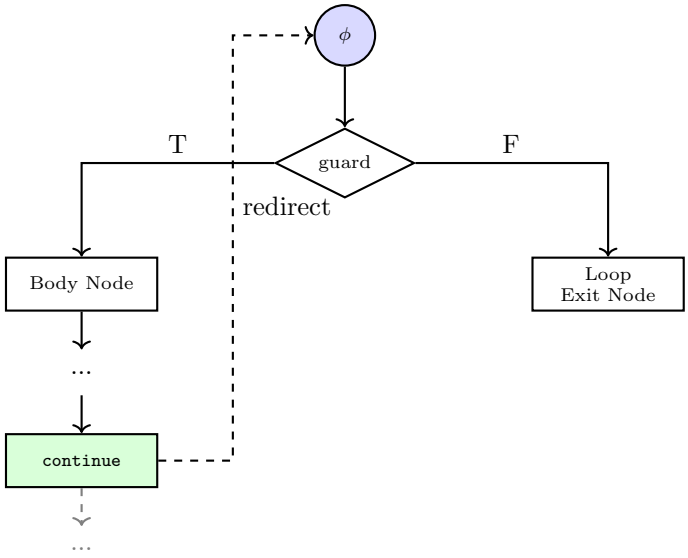


**Fig. 10** Continue statement insertion. The `continue` node's outgoing edge is redirected to the loop's FIXPOINT EVALUATION NODE $\phi$.

Figure 12 shows `require`/`assert`. The builder inserts a CONDITION NODE for the predicate, makes the true edge point to a BASIC NODE, and connects the false edge directly to the function's ERROR EXIT. The true basic then reconnects to the original successors, forming a one-sided diamond.

**Other constructs.** Similar patterns apply to the remaining control-flow constructs:

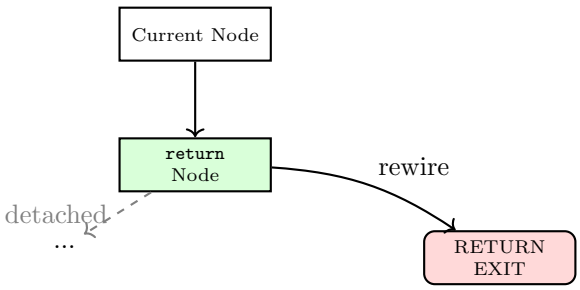


**Fig. 11** Return statement insertion. The `return` node is rewired to the function's unique RETURN EXIT.

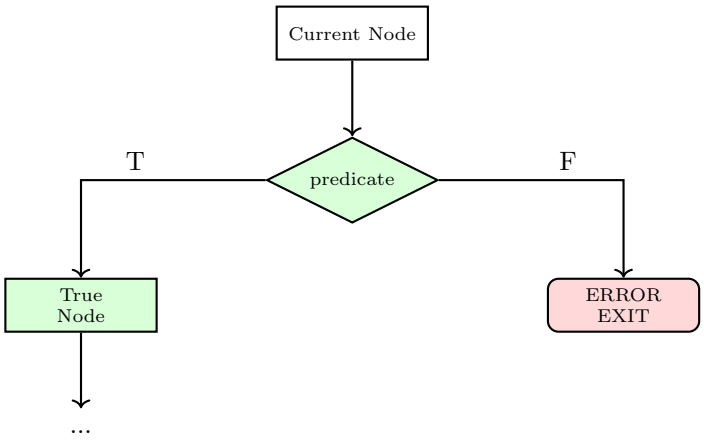


**Fig. 12** Require/assert statement insertion. The builder creates a CONDITION NODE with true edge to a node and false edge to the ERROR EXIT.

- `for` loops: Handled as a $\phi$ node and condition like `while`, optionally preceded by an initialization node and followed by an increment node on the back edge.
- `do{} while`: Built in two steps. First, a body pair is created and closed. Later, the trailing `while` line attaches a $\phi$, condition, and loop exit, and wires the back edge to the existing body.
- `try{} catch{}`: Represented by a CONDITION NODE tagged as `try` whose true edge goes to the success block and whose false edge is replaced by a catch entry/end pair when a matching `catch` appears.

### 3.4.2 Line-Aware Successor-First Insertion-Site Selection

We keep a lightweight line–to–node index to make insertion local. Each newly created node is attached to one or two source lines depending on whether the construct is single-line (terminated by ";") or brace-delimited. This index is used only to locate the insertion site; the algorithm below does not mutate the graph.

**Line-to-node index mapping.** We attach each CFG node to source lines based on the statement type:

- **Sequential statements** (variable declaration, assignment, function call, unary operations): Index the statement block at its source line.
- **Conditional branches** (`if`/`else if`): Index the condition node at the guard line and the join node at the closing brace line.
- **Else branches**: Index the else block at the `else` line and reuse the preceding guard's join node.
- **Loops** (`while`/`for`): Index the condition node at the guard line and the loop-exit node at the closing brace line.
- **Loop control** (`continue`/`break`): Index the statement block at its source line.
- **Terminating statements** (`return`/`revert`): `return` creates a new block; `revert` uses the current block directly.
- **Assertions** (`require`/`assert`): Index the condition node at the statement line.
- **Exception handling** (`try`/`catch`): Index the try condition at the `try` line and catch entry at the `catch` line.

We dispatch insertion-site selection based on the edit context:

- **Branch contexts** (`else`/`else if`/`catch`) use Algorithm 1 to find the preceding condition node by traversing predecessors.
- **Regular statements** use Algorithm 2, which employs a SUCCESSOR-FIRST strategy: locate the earliest CFG node after the edit span and determine the most local predecessor.

Both algorithms never mutate the graph and rely solely on the line–to–node index for efficient lookup.

**Algorithm 1: Branch-Context Insertion.** For `else`/`else if`/`catch`, we must attach the new branch to a previously created condition node. The algorithm:

- **Line 1–4:** Retrieves CFG nodes at the current line $L$ (or searches backward if $L$ is empty). For `else_if`/`else`, it also identifies the outer join node at $L$, if present.
- **Line 9–24:** Performs BFS through CFG predecessors to find the matching condition node: for `else_if`/`else`, it looks for a node of type `if` or `else_if`; for `catch`, it looks for type `try`.
- **Line 11–12:** When the matching condition is found for `else_if`/`else`, the algorithm returns both the condition node and the outer join (if the outer join was not found at line $L$, a fallback uses the graph structure).

**Algorithm 2: Successor-First Insertion.** For regular statements, we look ahead to determine the insertion site:

- **Line 1–3:** FIRSTNODEAFTER($L$) scans lines strictly larger than $L$ in the line–to–node index and returns the first node; if none is found, we default to `EXIT`.
- **Line 5–14 (loop-exit):** If the successor $s$ is a loop-exit node, we search backward from $L$ to find the previous line's nodes. If the previous line contains a condition node (the loop header), we return its TRUE branch (the loop body entry); otherwise, we return the last node of the previous line.

**Algorithm 1** Branch-Context Insertion-Site Selection (GetBranchContext)

**Require:** CFG $G = (V, E)$, edit context $ctx \in \{\texttt{else\_if}, \texttt{else}, \texttt{catch}\}$, current line $L$
**Ensure:** Condition node $c \in V$ (and optionally outer join $j \in V$ for `else_if`/`else`)

```
1:  N ← NodesAtLine(L)                                  ▷ all CFG nodes indexed at line L
2:  if N = ∅ then
3:      N ← NodesAtPreviousLine(L)                      ▷ search backward if L is empty
4:  end if
5:  j_outer ← ⊥
6:  if ctx ∈ {else_if, else} then
7:      for n ∈ N do
8:          if isJoin(n) then
9:              j_outer ← n  break                      ▷ outer join at current line
10:         end if
11:     end for
12: end if
13: Queue ← N; Visited ← ∅                              ▷ BFS through predecessors
14: while Queue ≠ ∅ do
15:     n ← Dequeue(Queue)
16:     if n ∈ Visited then continue
17:     end if
18:     Visited ← Visited ∪ {n}
19:     if isCond(n) then
20:         τ ← CondType(n)                             ▷ type: if, else_if, try, etc.
21:         if ctx ∈ {else_if, else} and τ ∈ {if, else_if} then
22:             if j_outer = ⊥ then
23:                 j_outer ← OuterJoinFromGraph(n)     ▷ fallback
24:             end if
25:             return (n, j_outer)
26:         else if ctx = catch and τ = try then
27:             return n
28:         end if
29:     end if
30:     for p ∈ Predecessors(n) do
31:         if p ∉ Visited then
32:             Enqueue(Queue, p)
33:         end if
34:     end for
35: end while
36: error "No matching condition node found for context ctx"
```

- **Line 16–23 (join):** If $s$ is a join node (closing a selection), we apply the same backward search. If a condition node is found, we return its TRUE branch (default for `if` constructs); otherwise, return the last previous node.
- **Line 25–28 (basic successor):** If $s$ is a regular basic node, we return its unique predecessor, or choose the predecessor closest to line $L$ if multiple exist.

**Algorithm 2** Successor-First Insertion-Site Selection (GetInsertionSite)

**Require:** CFG $G = (V, E)$, edit span ending at line $L$
**Ensure:** Insertion-site node $A \in V$ (no graph mutation here)

$s \leftarrow$ FirstNodeAfter($L$) ▷ scan lines $> L$ until the first indexed node
**if** $s = \perp$ **then**
  $s \leftarrow$ EXIT
**end if**
$\ell \leftarrow$ LineOf($s$)
**if** isLoopExit($s$) **then** ▷ closing a loop
  $N_{prev} \leftarrow$ NodesAtPreviousLine($L$) ▷ search backward from $L$ to find previous nodes
  **if** $N_{prev} \neq \emptyset$ **then**
    $c \leftarrow$ LastCondInNodes($N_{prev}$) ▷ check if previous line has a condition
    **if** $c \neq \perp$ **then**
      **return** BranchBlock($c$, true) ▷ insert in TRUE branch (loop body)
    **else**
      **return** Last($N_{prev}$) ▷ last node of previous line
    **end if**
  **else**
    **return** FirstPredecessor($s$) ▷ fallback
  **end if**
**else if** isJoin($s$) **then** ▷ closing a selection
  $N_{prev} \leftarrow$ NodesAtPreviousLine($L$)
  **if** $N_{prev} \neq \emptyset$ **then**
    $c \leftarrow$ LastCondInNodes($N_{prev}$)
    **if** $c \neq \perp$ **then**
      **return** BranchBlock($c$, true) ▷ default to TRUE branch for `if`
    **else**
      **return** Last($N_{prev}$)
    **end if**
  **else**
    **return** FirstPredecessor($s$)
  **end if**
**else** ▷ basic successor
  $Pred \leftarrow$ Predecessors($s$)
  **if** $|Pred| = 1$ **then**
    **return** the unique element of $Pred$
  **else**
    **return** NearestByLine($Pred$, $L$) ▷ choose closest to current line $L$
  **end if**
**end if**

**Helper functions.**

- NodesAtLine($L$) / NodesAtPreviousLine($L$): Return all CFG nodes indexed at line $L$ or the first non-empty line before $L$.
- FirstNodeAfter($L$): Returns the first CFG node indexed at any line $> L$.
- LastCondInNodes($N$): Scans node list $N$ in reverse to find the last condition node.
- BranchBlock($c, t$): Returns the successor of condition $c$ along the edge labeled with truth value $t$.
- OuterJoinFromGraph($c$): Walks the graph from condition $c$ through its TRUE branch to find the join node.
- NearestByLine($X, \ell$): Returns $\arg\min_{x \in X} |\text{LineOf}(x) - \ell|$.
- Predecessors($s$), FirstPredecessor($s$): Standard CFG predecessor queries.

### 3.4.3 Abstract Interpretation for Incremental Analysis

Our system handles two types of edits during interactive debugging, each triggering a different analysis strategy. Debug annotation input follows a batch-and-flush pattern: annotations are accumulated and processed together, culminating in a full interpretation of the entire function CFG from `ENTRY` to `EXIT` (Algorithm 3). This ensures that all annotated inspection points receive freshly computed abstract states. In contrast, source code edits—such as inserting `require`, assignments, or control structures—are processed immediately: dynamic CFG construction (Algorithms 1 and 2) splices the new nodes into the graph, and change-driven reinterpretation (Algorithm 4) propagates updates only along affected paths, providing instant feedback without reanalyzing the entire function. Both strategies invoke the same loop fixpoint subroutine (Algorithm 5) when encountering loop headers.

Algorithm 3 performs initial interpretation when debug annotations are first introduced to a function. It begins with the `ENTRY` node enqueued and propagates abstract environments forward through the entire CFG using a standard worklist iteration. Algorithm 4, in contrast, handles source code edits: the dynamic CFG builder returns one or more seed nodes (never sinks) that mark the insertion points, and the algorithm propagates updates only along forward-reachable paths from these seeds. The choice of seed depends on the statement type: sequential statements (`assignment`, `function call`) seed at the newly inserted block; control-flow constructs (`if`/`while`/`for`) seed at their join or loop-exit node to capture all downstream effects; terminating statements (`return`/`revert`) seed at the original successors before rewiring; and assertions (`require`/`assert`) seed at the true-branch successor. Seeds corresponding to sink nodes (`EXIT`, `ERROR`, `RETURN`) are filtered out because they contribute nothing to downstream analysis.

Both algorithms share the same core iteration structure. Each node computes its incoming environment $\hat{\sigma}_{in}$ by joining all predecessor flows. For predecessors that are condition nodes, we apply path-sensitive refinement: the environment is updated according to the condition and the edge's truth label (true or false), and infeasible branches—where the refined environment contradicts the guard—are pruned by setting $\sigma_p$ to $\bot$. This ensures that only feasible execution paths contribute to the analysis.

**Algorithm 3** Initial Function Interpretation (InterpretFunctionCFG)

**Require:** CFG $G = (V, E)$ with designated `ENTRY` node
**Ensure:** All nodes have computed abstract environments

$WL \leftarrow \langle$`ENTRY`$\rangle$; $inQ \leftarrow \{$`ENTRY`$\}$; $Out \leftarrow$ snapshot map
**while** $WL \neq \langle\rangle$ **do**
  $n \leftarrow WL$.pop(); $inQ \leftarrow inQ \setminus \{n\}$
  $\hat{\sigma}_{in} \leftarrow \bot$ ▷ compute incoming environment from all predecessors
  **for all** $p \in$ Predecessors$(n)$ **do**
    $\sigma_p \leftarrow (p)$
    **if** isCond$(p)$ $\wedge$ hasTruthLabel$(p \to n)$ **then**
      $t \leftarrow$ edgeLabel$(p \to n)$
      $\sigma_p \leftarrow$ Refine$(\sigma_p, p.\text{cond}, t)$
      **if** $\neg$Feasible$(\sigma_p, p.\text{cond}, t)$ **then**
        $\sigma_p \leftarrow \bot$
      **end if**
    **end if**
    $\hat{\sigma}_{in} \leftarrow \hat{\sigma}_{in} \sqcup \sigma_p$
  **end for**
  **if** isLoopHeader$(n)$ **then**
    $exitNode \leftarrow$ Fixpoint$(n)$ ▷ Algorithm 5
    **for all** $u \in (exitNode)$ **do**
      **if** $\neg$isSink$(u)$ $\wedge$ $u \notin inQ$ **then**
        $WL$.enqueue$(u)$; $inQ \leftarrow inQ \cup \{u\}$
      **end if**
    **end for**
    **continue**
  **end if**
  $\hat{\sigma}_{out} \leftarrow$ Transfer$(n, \hat{\sigma}_{in})$
  **if** $\hat{\sigma}_{out} \neq Out[n]$ **then**
    $(n) \leftarrow \hat{\sigma}_{out}$; $Out[n] \leftarrow \hat{\sigma}_{out}$
    **for all** $u \in (n)$ **do**
      **if** $\neg$isSink$(u)$ $\wedge$ $u \notin inQ$ **then**
        $WL$.enqueue$(u)$; $inQ \leftarrow inQ \cup \{u\}$
      **end if**
    **end for**
  **end if**
**end while**

Loop headers receive special treatment in both algorithms. When the worklist reaches a loop header, we invoke a dedicated fixpoint procedure (Algorithm 5) that recomputes abstract states for the entire loop body using widening and narrowing. The fixpoint returns the loop-exit node, whose successors are then enqueued for further propagation. This design localizes loop effects: in Algorithm 4, any edit inside a loop body naturally triggers a fresh fixpoint once the header is encountered, without requiring the builder to seed every loop-internal change explicitly.

**Algorithm 4** Change-Driven Reinterpretation (ReinterpretFrom)

**Require:** CFG $G = (V, E)$; seed set $S$ returned by the builder
**Ensure:** Environments updated along forward-reachable paths from $S$

$WL \leftarrow \langle\rangle$; $inQ \leftarrow \emptyset$; $Out \leftarrow$ snapshot map
**for all** $s \in S$ **do** ▷ filter and enqueue all non-sink seeds
  **if** $\neg$isSink$(s) \wedge s \notin inQ$ **then**
    $WL$.enqueue$(s)$; $inQ \leftarrow inQ \cup \{s\}$
  **end if**
**end for**
**while** $WL \neq \langle\rangle$ **do**
  $n \leftarrow WL$.pop(); $inQ \leftarrow inQ \setminus \{n\}$
  $\hat{\sigma}_{in} \leftarrow \bot$ ▷ compute incoming environment from all predecessors
  **for all** $p \in$ Predecessors$(n)$ **do**
    $\sigma_p \leftarrow (p)$
    **if** isCond$(p) \wedge$ hasTruthLabel$(p \to n)$ **then** ▷ refine by condition
      $t \leftarrow$ edgeLabel$(p \to n)$
      $\sigma_p \leftarrow$ Refine$(\sigma_p, p.\text{cond}, t)$ ▷ apply path constraint
      **if** $\neg$Feasible$(\sigma_p, p.\text{cond}, t)$ **then**
        $\sigma_p \leftarrow \bot$
      **end if** ▷ prune infeasible
    **end if**
    $\hat{\sigma}_{in} \leftarrow \hat{\sigma}_{in} \sqcup \sigma_p$
  **end for**
  **if** isLoopHeader$(n)$ **then** ▷ handle loop by local fixpoint
    *exitNode* $\leftarrow$ Fixpoint$(n)$ ▷ compute fixpoint; returns loop-exit node
    **for all** $u \in$ (*exitNode*) **do**
      **if** $\neg$isSink$(u) \wedge u \notin inQ$ **then**
        $WL$.enqueue$(u)$; $inQ \leftarrow inQ \cup \{u\}$
      **end if**
    **end for**
    **continue** ▷ skip standard transfer for loop header
  **end if**
  $\hat{\sigma}_{out} \leftarrow$ Transfer$(n, \hat{\sigma}_{in})$ ▷ apply statement effects
  **if** $\hat{\sigma}_{out} \neq Out[n]$ **then** ▷ change detected
    $(n) \leftarrow \hat{\sigma}_{out}$; $Out[n] \leftarrow \hat{\sigma}_{out}$
    **for all** $u \in (n)$ **do**
      **if** $\neg$isSink$(u) \wedge u \notin inQ$ **then**
        $WL$.enqueue$(u)$; $inQ \leftarrow inQ \cup \{u\}$
      **end if**
    **end for**
  **end if**
**end while**

**Table 2** Abstract syntax (subset of Solidity) used by our analysis — meta, literals, and types

| Symbol | Set | Definition / Forms |
|---|---|---|
| *Meta and identifiers* | | |
| $N$ | BitW | Integer bit width, $N \in \{8, 16, \ldots, 256\}$. |
| $x$ | Var | Program variables (state or local). |
| $f$ | Field | Struct fields. |
| $C$ | Struct | Struct identifiers. |
| $E$ | Enum | Enum identifiers. |
| *Literals* | | |
| $n$ | $\mathbb{Z}_{2^N}$ | Integer numeral typed by $N$ (signed via unary $-$ when needed). |
| $b$ | $\mathbb{B}$ | $\{\mathsf{true}, \mathsf{false}\}$. |
| *addr* | $\mathbb{A}$ | Address literal $(0 \ldots 2^{160}-1)$. |
| *Types* | | |
| $\tau_b$ | ValType | $\mathsf{uint}N \mid \mathsf{int}N \mid \mathsf{bool} \mid \mathsf{address}$. |
| $\kappa$ | Key | $\mathsf{uint}N \mid \mathsf{int}N \mid \mathsf{address} \mid \mathsf{enum}\ E$. |
| $\mu$ | CType | $\mathsf{mapping}(\kappa \Rightarrow \tau) \mid \tau[] \mid \mathsf{struct}\ C \mid \mathsf{enum}\ E$, where $\tau ::= \tau_b \mid \mu$. |

The change guard mechanism is critical for efficiency. After computing the transfer function's result $\hat{\sigma}_{out}$, we compare it with the previous snapshot $Out[n]$. Only when a change is detected do we update the node's environment, refresh the snapshot, and enqueue non-sink successors. This guarantees termination and avoids redundant work: if downstream nodes remain unaffected, propagation halts. Crucially, it does not miss any updates, because any upstream alteration that modifies a node's input will also alter its output (even for identity transfers on join or condition nodes), thus triggering further propagation.

## 3.5 Design of the Abstract Interpretation Framework for Solidity

This section presents the formal framework for our abstract interpretation-based debugger. We begin with the program syntax covering the subset of Solidity we analyze, then define the concrete semantics as a baseline, introduce the abstract domains we use for scalable approximation, and finally describe the abstract semantics that power our incremental debugging analysis.

### 3.5.1 Program Syntax

Our analysis focuses on standard structured constructs including variable declarations, assignments, if, while, do–while, for, return, assert/require, delete, and calls as statements. Low-level features such as inline assembly and unchecked arithmetic are out of scope for this section; modifiers are assumed to be desugared into the control flow.

**Table 3** Abstract syntax (subset) — l-values, expressions, statements, programs

| Symbol | Set | Definition / Forms |
|---|---|---|
| *L-values and expressions* | | |
| $lv$ | LVal | $x \mid lv.f \mid lv[idx] \mid lv[key]$. |
| $idx$ | IdxExp | Numeric index expression (int/uint). |
| $key$ | KeyExp | Mapping key expression of type $\kappa$. |
| $a$ | AExp | $n \mid addr \mid lv \mid -a \mid \sim a \mid a \oplus a$, $\oplus \in \{+, -, *, /, \%, \ll, \gg, \&, \mid, \wedge\}$. |
| $p$ | BExp | $b \mid a \bowtie a \mid \neg p \mid p \wedge p \mid p \vee p$, $\bowtie \in \{=, \neq, <, \leq, >, \geq\}$. |
| *Statements* | | |
| $s$ | Stmt | skip \|s; s\|{$\overline{s}$} |
| | | $\tau_b\ x$; \|$\tau_b\ x = a$; \|lv := a\| delete lv |
| | | if $p$ then $s$ else $s$ |
| | | while $p$ do $s$ \| do s while p |
| | | for($s_0$; $p$?; $u$?) $s$ ( $u$ is an update as an assignment/compound ) |
| | | return $a$? \| assert(p) \| require(p) |
| | | call($\overline{a}$) (*external or unknown call, as a statement*) |
| *Programs* | | |
| $f$ | Fun | function $id(\overline{x : \tau_b})$ $s$ (*single-contract, single-tx*; modifiers desugared). |

### 3.5.2 Concrete Semantics (Denotational)

We define the concrete semantics denotationally to establish a baseline for correctness. Let stores be $\sigma : \mathsf{Var} \rightharpoonup \mathsf{CVal}$. L-value resolution $\mathrm{loc}_\sigma(lv) = \ell$ and write $\mathrm{write}(\sigma, \ell, v)$ update the store, where arrays and mappings lazily materialize missing cells on access. Expressions are pure and evaluate to values: $e_\sigma \in \mathsf{Val}$. To model control effects such as early returns and assertion failures, we introduce an outcome domain

$$\mathsf{Res} \ ::= \ (\sigma) \ \mid \ (v, \sigma) \ \mid$$

with a sequencing (Kleisli) operator

$$\begin{aligned} (\sigma) \ \triangleright \ K &:= K(\sigma), \\ (v, \sigma) \ \triangleright \ K &:= (v, \sigma), \\ \triangleright \ K &:= . \end{aligned}$$

We write $s : \sigma \mapsto \mathsf{Res}$ for the denotation of statements. Table 4 defines the concrete semantics for each statement form.

For arrays and mappings, $\mathrm{loc}_\sigma(a[i])$ extends dynamic array $a$ up to index $i$ with default cells if needed, and $\mathrm{loc}_\sigma(m[k])$ creates mapping entry $m[k]$ lazily if absent. These conventions apply to both reads and writes. Note that for and do-while loops

**Table 4** Concrete denotational semantics (statements)

| Statement | Meaning |
|---|---|
| skip | $\mathsf{skip}(\sigma) = (\sigma)$. |
| $s_1; s_2$ | $s_1; s_2(\sigma) = \big(s_1(\sigma)\big) \triangleright (\lambda\sigma'.\, s_2(\sigma'))$. |
| $\{\overline{s}\}$ | Right-associative fold of sequencing over $\overline{s}$. |
| $\tau\ x;$ | $\tau\ x; (\sigma) = \big(\sigma[x \mapsto \mathrm{zero}_\tau]\big)$. |
| $\tau\ x = e;$ | $\tau\ x = e; (\sigma) = \big(\sigma[x \mapsto e_\sigma]\big)$. |
| $lv := e$ | $lv := e(\sigma) = \big(\mathrm{write}(\sigma,\, \mathrm{loc}_\sigma(lv),\, e_\sigma)\big)$. |
| delete $lv$ | $\mathsf{delete}\ lv(\sigma) = \big(\mathrm{write}(\sigma,\, \mathrm{loc}_\sigma(lv),\, \mathrm{zero}_{\tau(lv)})\big)$. |
| if $p$ then $s_t$ else $s_f$ | $\cdot(\sigma) = \begin{cases} s_t(\sigma) & \text{if } p_\sigma = \mathsf{true}, \\ s_f(\sigma) & \text{if } p_\sigma = \mathsf{false}. \end{cases}$ |
| while $p$ do $s$ | Let $F(H)(\sigma) = \begin{cases} \big(s(\sigma)\big) \triangleright H & \text{if } p_\sigma = \mathsf{true}, \\ (\sigma) & \text{if } p_\sigma = \mathsf{false}. \end{cases}$ Then $\mathsf{while}\ p\ \mathsf{do}\ s = \mathrm{lfp}(F)$. |
| return $e$ | $\mathsf{return}\ e(\sigma) = (e_\sigma,\, \sigma)$. |
| assert($p$), require($p$) | $\cdot(\sigma) = \begin{cases} (\sigma) & \text{if } p_\sigma = \mathsf{true}, \\ & \text{if } p_\sigma = \mathsf{false}. \end{cases}$ |
| revert($\cdots$) | $\mathsf{revert}(\cdots)(\sigma) =$. |
| call($\overline{e}$) | Internal calls evaluate the callee's body with parameter binding; external/unknown calls are left unspecified here (treated in the abstract setting by a conservative effect). |

are desugared to while in our framework, and we treat require identically to assert at the level of control effects since both abort on failure.

### 3.5.3 Abstract Domain

**Atomic abstract values.** We use interval domains for integer types and a specialized set domain for address types:

$$\begin{aligned} \widehat{\mathbb{U}}_N &:= \{[\ell, u] \mid 0 \le \ell \le u \le 2^N{-}1\} \ \cup\ \{\bot, \top_N\}, \\ \widehat{\mathbb{Z}}_N &:= \{[\ell, u] \mid -2^{N-1} \le \ell \le u \le 2^{N-1}{-}1\} \ \cup\ \{\bot, \top_N^{\pm}\}, \\ \widehat{\mathbb{B}} &:= \{\bot, \widehat{\mathsf{false}}, \widehat{\mathsf{true}}, \top\}, \qquad \widehat{\mathbb{A}} := \wp_{\le K}(\mathbb{A}) \cup \{\top\}, \\ \widehat{\mathsf{Enum}}(E) &:= \{[\ell, u] \mid 0 \le \ell \le u \le |E| - 1\} \cup \{\bot, [0, |E| - 1]\}. \end{aligned}$$

Here $\widehat{\mathbb{A}}$ represents the address domain as a set abstraction with at most $K$ concrete address identifiers, generalizing to $\top$ when capacity is exceeded. This enables precise tracking of contract addresses in debugging scenarios while maintaining scalability.
**Order/Join/Meet.** For intervals,

$$[\ell_1, u_1] \sqsubseteq [\ell_2, u_2] \iff \ell_2 \le \ell_1 \wedge u_1 \le u_2, \quad [\ell_1, u_1] \sqcup [\ell_2, u_2] = [\min(\ell_1, \ell_2), \max(u_1, u_2)],$$

$$[\ell_1, u_1] \sqcap [\ell_2, u_2] = \begin{cases} [\max(\ell_1, \ell_2), \min(u_1, u_2)] & \text{if } \max(\ell_1, \ell_2) \leq \min(u_1, u_2), \\ \bot & \text{otherwise.} \end{cases}$$

Widening $\nabla$ is the standard interval widening (per bit width); narrowing $\Delta$ follows the dual pattern.

**Composite values.** Our framework supports Solidity's composite data structures through careful abstraction:

- *Structs*: $\widehat{\mathsf{Struct}}(C) = \prod_{f \in \mathsf{fields}(C)} \widehat{\mathsf{Val}}_f$ represents structs as products over their fields with pointwise order, enabling field-sensitive analysis.
- *Arrays (on-access materialization)*: $\widehat{\mathsf{Arr}}(\tau) = (\hat{\ell}, \hat{d}, M)$ where $\hat{\ell} \in \widehat{\mathbb{U}}_{256}$ is an abstract length, $\hat{d} \in \widehat{\tau}$ is a default element value, and $M : \mathbb{N}_{\text{fin}} \rightharpoonup \widehat{\tau}$ is a finite map tracking observed indices. This design enables strong updates for known indices while maintaining soundness for unknown accesses.
- *Mappings (on-access materialization)*: $\widehat{\mathsf{Map}}(\kappa \Rightarrow \tau) = (\hat{d}, M)$ with default $\hat{d} \in \widehat{\tau}$ and finite $M : \widehat{\kappa}_{\text{fin}} \rightharpoonup \widehat{\tau}$. Mappings materialize entries on first access, supporting both concrete keys (for strong updates) and symbolic keys (for weak updates).
- *Enums*: represented as bounded unsigned intervals over $[0, |E| - 1]$.

**Value domains and store.** The complete abstract value hierarchy is:

$$\widehat{\mathsf{Val}} ::= \bigcup_N (\widehat{\mathbb{U}}_N \cup \widehat{\mathbb{Z}}_N) \cup \widehat{\mathbb{B}} \cup \widehat{\mathbb{A}} \cup \widehat{\mathsf{Enum}}(E),$$

$\widehat{\mathsf{CVal}} ::= \widehat{\mathsf{Val}} \mid \widehat{\mathsf{Struct}}(C) \mid \widehat{\mathsf{Arr}}(\tau) \mid \widehat{\mathsf{Map}}(\kappa \Rightarrow \tau), \qquad \hat{\sigma} : \mathsf{Var} \rightharpoonup \widehat{\mathsf{CVal}}$ (pointwise order/join).

The abstract store $\hat{\sigma}$ maps variables to abstract values with pointwise ordering and join operations, providing the foundation for our flow-sensitive analysis.

Table 5 summarizes the mapping from Solidity types to abstract domains. Addresses use a set domain that tracks up to $K$ concrete identifiers before generalizing to $\top$, providing precise aliasing information for contract addresses commonly encountered in debugging. Arrays and mappings employ finite observed maps with default values, ensuring soundness under unknown indices or keys while enabling strong updates for observed accesses.

### 3.5.4 Abstract Semantics (Denotational)

We lift the concrete semantics to abstract domains systematically. Let $\hat{\sigma} : \mathsf{Var} \rightharpoonup \widehat{\mathsf{CVal}}$ be the abstract store. Expressions evaluate to abstract values $e^{\sharp}_{\hat{\sigma}} \in \widehat{\mathsf{Val}}$ using bit-width–aware interval arithmetic for integers, set operations for addresses, and standard operations for booleans and composites. Abstract outcomes mirror the concrete case:

$$\widehat{\mathsf{Res}} ::= \curlyvee(\hat{\sigma}) \mid \curlyvee(\hat{v}, \hat{\sigma}) \mid \lightning,$$

**Table 5** Type → abstract domain mapping (summary)

| Solidity type | Abstract domain |
|---|---|
| $\mathsf{uint}N$ | $\widehat{\mathbb{U}}_N \quad (N \in \{8, \ldots, 256\})$ |
| $\mathsf{int}N$ | $\widehat{\mathbb{Z}}_N$ |
| bool | $\widehat{\mathbb{B}}$ |
| address | $\widehat{\mathbb{A}}$ (set domain) |
| enum $E$ | $\widehat{\mathsf{Enum}}(E)$ |
| $\tau[]$ | $\widehat{\mathsf{Arr}}(\tau)$ |
| $\mathsf{mapping}(\kappa \Rightarrow \tau)$ | $\widehat{\mathsf{Map}}(\kappa \Rightarrow \tau)$ |
| struct $C$ | $\widehat{\mathsf{Struct}}(C)$ |

ordered componentwise, with sequencing

$$\begin{aligned} \curlywedge(\hat{\sigma}) \ \triangleright^\sharp \ K &:= K(\hat{\sigma}), \\ \curlywedge(\hat{v}, \hat{\sigma}) \ \triangleright^\sharp \ K &:= \curlywedge(\hat{v}, \hat{\sigma}), \\ \frown \ \triangleright^\sharp \ K &:= \frown. \end{aligned}$$

Branch refinement $\mathrm{refine}(\hat{\sigma}, p, b)$ narrows operands of condition $p$ using interval meets to improve precision along branches. Abstract writes distinguish between *strong* updates when the target is unique (e.g., singleton index or concrete key) and *weak* updates that join the new value with the existing value when the target is uncertain. For joining branch outcomes we use

$$\mathrm{joinRes}(r_1, r_2) = \begin{cases} \curlywedge(\hat{\sigma}_1 \sqcup \hat{\sigma}_2) & r_i = \curlywedge(\hat{\sigma}_i), \\ \curlywedge(\hat{v}_1 \sqcup \hat{v}_2, \ \hat{\sigma}_1 \sqcup \hat{\sigma}_2) & r_i = \curlywedge(\hat{v}_i, \hat{\sigma}_i), \\ \text{the obvious mixed cases: componentwise join and/or carry } \frown. \end{cases}$$

Table 6 defines the abstract semantics for each statement form.

For array and mapping accesses, reading with a singleton index or concrete key returns the corresponding cell, while reading with a range or symbolic key returns the join of all materialized cells, or the element type's $\top$ if none exist. Dynamic array `length` is tracked as a singleton interval when observed; otherwise it is conservatively approximated as $\top_{\mathsf{uint256}}$. Writes follow the same singleton versus non-singleton criterion: concrete indices and keys enable strong updates that precisely overwrite values, while symbolic or range indices trigger weak updates that join new values with existing ones to maintain soundness.

# 4 Evaluation

To evaluate how SolQDebug performs in practical debugging scenarios, we organize our study around three research questions:

**Table 6** Abstract denotational semantics (statements)

| Statement | Meaning |
|---|---|
| skip | $\mathsf{skip}^\sharp(\hat{\sigma}) = \curlyvee(\hat{\sigma})$. |
| $s_1; s_2$ | $s_1; s_2^\sharp(\hat{\sigma}) = \big(s_1^\sharp(\hat{\sigma})\big) \triangleright^\sharp (\lambda\hat{\sigma}'.\, s_2^\sharp(\hat{\sigma}'))$. |
| $\tau\ x;$ | $\tau\ x;^\sharp(\hat{\sigma}) = \curlyvee\big(\hat{\sigma}[x \mapsto \widehat{\mathrm{init}}(\tau)]\big)$, where $\widehat{\mathrm{init}}$ sets $\mathsf{int/uint/bool} \mapsto \bot$, $\mathsf{address} \mapsto \top_{160}$, composites to empty summaries. |
| $\tau\ x = e;$ | $\tau\ x = e;^\sharp(\hat{\sigma}) = \curlyvee\big(\hat{\sigma}[x \mapsto \alpha_\tau(e^\sharp_{\hat{\sigma}})]\big)$. |
| $lv := e$ | $lv := e^\sharp(\hat{\sigma}) = \curlyvee\big(\widehat{\mathrm{write}}(\hat{\sigma},\, lv,\, e^\sharp_{\hat{\sigma}})\big)$; non-singleton index/key $\Rightarrow$ weak update (join). |
| delete $lv$ | $\mathsf{delete}\ lv^\sharp(\hat{\sigma}) = \curlyvee\big(\widehat{\mathrm{write}}(\hat{\sigma},\, lv,\, \widehat{\mathrm{zero}}_{\tau(lv)})\big)$; arrays/maps/structs wiped recursively. |
| if $p$ then $s_t$ else $s_f$ | Let $\hat{\sigma}_t = \mathrm{refine}(\hat{\sigma}, p, \mathsf{true})$ and $\hat{\sigma}_f = \mathrm{refine}(\hat{\sigma}, p, \mathsf{false})$. Then $\cdot^\sharp(\hat{\sigma}) = \mathrm{joinRes}\big(s_t^\sharp(\hat{\sigma}_t),\ s_f^\sharp(\hat{\sigma}_f)\big)$. |
| while $p$ do $s$ | Define $G^\sharp(H)(\hat{\sigma}) = \mathrm{joinRes}\big(s^\sharp(\mathrm{refine}(\hat{\sigma}, p, \mathsf{true})) \triangleright^\sharp H, \curlyvee(\mathrm{refine}(\hat{\sigma}, p, \mathsf{false}))\big)$. Then $\mathsf{while}\ p\ \mathsf{do}\ s^\sharp = \underbrace{\mathrm{lfp}^\nabla(G^\sharp)}_{\text{widening pass}} \triangle \underbrace{\mathrm{narrow}^k}_{\textbf{mandatory},\ k\geq 1}$, i.e., compute the widening-based post-fixpoint and then apply at least one narrowing round to regain precision. |
| return $e$ | $\mathsf{return}\ e^\sharp(\hat{\sigma}) = \curlyvee(e^\sharp_{\hat{\sigma}},\, \hat{\sigma})$. |
| assert($p$), require($p$) | As guards: if $p$ must-hold $\Rightarrow \curlyvee(\mathrm{refine}(\hat{\sigma}, p, \mathsf{true}))$; if $p$ must-fail $\Rightarrow \widehat{\ }$; otherwise both may happen and joinRes carries the possibilities. |
| revert($\cdots$) | $\mathsf{revert}(\cdots)^\sharp(\hat{\sigma}) = \widehat{\ }$. |
| call($\overline{e}$) | Internal calls analyze the callee body under parameter binding (same abstract machinery); external/unknown calls conservatively havoc their footprint or are modeled by $\widehat{\ }$ per analysis policy. |

- **RQ1 – Responsiveness**: How much edit–to–inspect latency does SolQDebug eliminate compared to Remix?
- **RQ2 – Precision Sensitivity to Annotation Structure**: In a common Solidity pattern where inputs are normalized by division, how does the structure of operand intervals—overlapping vs. distinct—impact interval growth?
- **RQ3 – Loops**: Which loop structures lead to loss of precision, and how do symbolic inputs influence the stability of analysis?

## 4.1 Experimental Setup

We evaluate SolQDebug on a controlled local setup with the following hardware and software configuration:

- **CPU**: 11th Gen Intel® Core™ i7-11390H @ 3.40GHz
- **RAM**: 16.0 GB

- **Operating System**: Windows 10 (64-bit)
- **Implementation Language**: Python

The dataset is derived from DAppSCAN (40), a large-scale real-world benchmark for smart contract analysis. From 3,345 Solidity files using `>=0.8.0`, we sample 128 contracts across three size brackets (1–10 KB, 11–20 KB, and over 20 KB). After filtering out logic-free functions (e. g., those containing only assignments or return statements), we retain 242 single-transaction handlers. From these, we select 30 representative examples covering key Solidity idioms, including structs, mappings, dynamic arrays, control flow, and arithmetic logic.

Since Remix IDE lacks built-in automated benchmarking capabilities, we developed `remix_benchmark`, a Selenium-based automation framework that programmatically drives the Remix web interface to measure edit-to-inspect latency. For each test function, `remix_benchmark` automates the full workflow: compilation, contract deployment, state variable initialization via manual storage slot assignment, parameter entry, transaction execution, and step-through debugging. We measure two latency metrics: *pure debug time*, capturing only the debugger step-through duration, and *total time*, which includes compilation, deployment, and state setup overhead. The difference between these metrics reflects the additional manual effort required in traditional debugging workflows.

Although SolQDebug is designed for interactive use within a Solidity editor, all experiments simulate this behavior in a controlled scripting environment. For each function, we reconstruct a sequence of incremental edits and annotations that mimic realistic developer activity. These fragments are streamed into the interpreter to measure latency and interval growth under reproducible conditions.

## 4.2 RQ1 - Responsiveness

To evaluate responsiveness, we measure edit-to-inspect latency—defined as the time from a code change to the appearance of updated variable information—under a single contract, single transaction scenario.

We evaluated 30 functions across 4 test-case widths $\Delta \in \{0, 2, 5, 10\}$, yielding 120 total measurements for SolQDebug. For Remix, we measured each function once using `remix_benchmark`, capturing both pure debug time (debugger step-through only) and total time ( including compilation, deployment, and state initialization).

For Remix, the pure debug time ranged from 25.1 to 124.6 seconds (median: 53.0 s), reflecting the time required to step through bytecode operations in the debugger. The total time, however, ranged from 71.1 to 168.3 seconds (median: 98.1 s), as it includes approximately 35 seconds for compilation and deployment, plus 0–11.8 seconds for manual state variable initialization (median: 2.9 s). Functions requiring more state slots incur proportionally higher setup overhead, with state initialization time growing linearly with the number of storage variables.

In contrast, SolQDebug completed analysis in 0.03–5.09 seconds (median: 0.15 s) across all 120 measurements, requiring no compilation, deployment, or state setup. Fig. **??** visualizes this performance gap: Remix pure debug time alone exceeds SolQDebug's total latency by a median factor of ˜350×, while total Remix latency

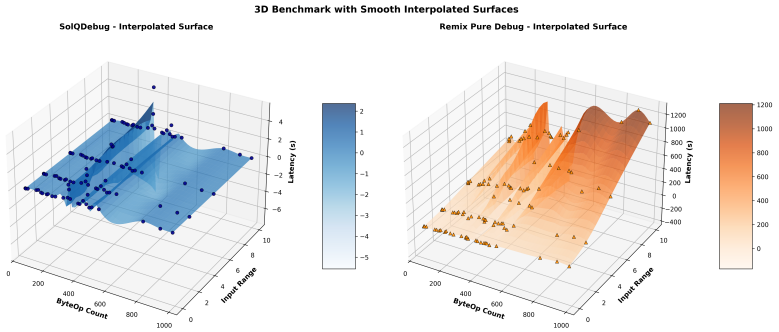


**Fig. 13** Edit-to-inspect latency comparison between Remix and SolQDebug across varying test-case widths and execution passes. The x-axis represents the cost estimate, y-axis shows TestCase width ($\Delta$), and z-axis displays latency in seconds. While Remix maintains constant high latency regardless of iteration, SolQDebug demonstrates significantly lower latency that quickly reaches a floor after the initial pass.

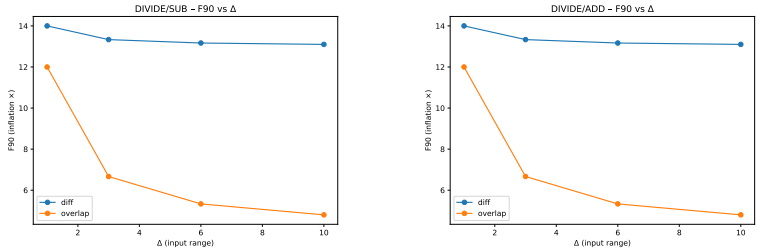


**Fig. 14** Interval growth after normalization in `pending` function from `Lock.sol`. Left: original version with subtraction; right: modified version where subtraction is replaced with addition

(including setup) exceeds it by ˜650×. This demonstrates that SolQDebug eliminates the compile–deploy–setup cycle entirely, enabling immediate feedback during code editing.

## 4.3 RQ2 - Precision Sensitivity to Annotation Structure

Smart contracts often normalize raw inputs via division—e.g., converting timestamps to time units—before combining the results using addition or subtraction. To isolate the impact of the final arithmetic operator from the shared division step, we analyze two variants of the same control-flow structure: one using addition, the other using subtraction.

Each variant is tested under two annotation styles. In the DIFF style, each operand is assigned a distinct input interval (e.g., $[10, 20]$ and $[30, 40]$). In the OVERLAP style, the intervals are partially aligned (e.g., $[10, 20]$ and $[15, 25]$), such that they share a subrange but are not fully identical. For each combination, we sweep the annotation width $\Delta \in \{1, 3, 6, 10\}$ and report $F_{90}$, the 90th percentile of the inflation factor $F = \textit{exit\_width}/\textit{input\_width}$.

Results in Fig.7 show that interval growth is more sensitive to the structure of input ranges than to the arithmetic operator. DIFF inputs consistently trigger early widening as $\Delta$ increases, while OVERLAP inputs maintain tighter bounds even under addition, which typically increases output range.

This suggests that in division-normalized logic, the alignment of operand intervals—whether disjoint or overlapping—has a stronger influence on interval growth than the choice between addition and subtraction. Overlapping inputs consistently result in smaller output ranges, reducing the degree of over-approximation as input width increases.

### 4.4 RQ3 - Loops

Two loop patterns emerge from the benchmarks. In the first, the loop condition itself bounds the updated variable, and the loop body performs only direct assignments. In such cases, abstract interpretation converges naturally. For example, `updateUserInfo` in AOC_BEP iterates from 1 to 4, and the interval for `level` stabilizes at $[1, 4]$.

In contrast, loops that interact with external or conditionally populated state tend to diverge under widening. For instance, `revokeStableMaster` in CORE terminates immediately under the contract's default state, but diverges once annotations populate the relevant lists. These lists trigger cascading updates, and their interactions produce imprecision even though the loop count is implicit.

In short, loop precision tends to hold when updates are tightly coupled to bounded loop indices, but approximation still arises due to joins at merge points. Precision degrades further when variables are updated independently of the loop condition. This includes dormant paths activated by symbolic input, or loops that iterate over data-driven structures such as mappings or dynamic lists.

## 5 Discussion

### 5.1 Why use Abstract Interpretation for Debugging

In this work, we use debugging to mean a developer-led, interactive exploration activity that happens before deployment during code authoring: the developer varies symbolic (interval) inputs and immediately observes branch reachability, guard validity, and value bounds at the source level. This edit-time feedback loop calls for a technique that (1) terminates quickly, (2) explains results in a way developers can inspect, and (3) scales to near-keystroke responsiveness.

We chose abstract interpretation (AI) over symbolic execution and proof-based verification for three reasons:

- **Termination.** AI enforces convergence via widening at loops and joins at merges, avoiding the path explosion common in symbolic execution.
- **Explainability.** Each result is an abstract value in a well-defined lattice. With interval domains, the mapping from inputs to outputs is explicit as ranges, which makes dataflow effects easy to trace and debug at the line level.

- **Responsiveness.** Interval transfer functions are lightweight, enabling millisecond-scale updates that fit the edit cycle. Symbolic engines routinely explore many paths even for small edits, which can break interactivity.

Formal verification provides stronger guarantees, but requires fully specified properties and invariants, which are costly to author during early iterations. SolQDebug is designed to bridge the gap between writing code and running tests or verification—offering immediate, sound, conservative feedback with low annotation overhead.

***Why the interval domain?***

For debugging, intervals strike a practical balance between precision and speed. They (i) align with developers' mental model of "possible ranges," (ii) expose boundary effects (e.g., overflow thresholds, guard satisfaction regions) without committing to a single concrete input, and (iii) compose predictably through joins and widenings. In our setting, intervals are also a natural surface for annotations: developers can *shape* symbolic inputs (e.g., make them overlapping or disjoint) and directly see how that affects control flow and computed ranges.

***Managing the accuracy–latency trade-off.***

AI's precision is conservative by design; edit-time usability depends on giving developers simple levers to steer precision without sacrificing responsiveness. We expose three such levers that proved effective in our study:

- **Annotation structure.** Overlapping operand intervals often bound output ranges more tightly than disjoint ones in division-normalized arithmetic (cf. RQ2). This reduces false alarms with no runtime cost.
- **Annotation width.** Narrower inputs shrink joins and delay widening; developers can start narrow and broaden gradually ("zoom out") to probe stability.
- **Guard-guided narrowing.** Making explicit the intended `require`/`if` guards in annotations tightens feasible states early and improves precision along the taken branch at negligible cost.

Where stricter precision is essential (e.g., inside data-driven loops), the workflow can temporarily fall back to concrete inputs for local inspection, then return to intervals for broader exploration. This "concrete when needed, symbolic by default" rhythm preserves interactivity while keeping results actionable.

## 5.2 Evaluation Implication

***RQ1: Edit-time responsiveness, not just "a few seconds faster."***

Traditional debuggers (e.g., Remix, Hardhat Debug) require compile–deploy–execute per iteration, typically taking tens of seconds. In contrast, our interpreter updates in milliseconds (median $\sim$14 ms on the first pass and 5–35 ms on the second), yielding *orders-of-magnitude* lower edit-to-inspect latency. This difference is qualitative: it enables near-keystroke feedback, which changes how developers explore code. Because results are symbolic, a single pass summarizes many concrete executions; developers

can see when guards always hold/fail for an interval, when a branch becomes unreachable, or when a value may cross a critical threshold—all without leaving the editor. In short, SolQDebug complements runtime debuggers by moving fast, informative checks *into* the authoring loop.

***RQ2: Annotation design as a precision knob.***

RQ2 shows that, in division-normalized patterns common in Solidity, *how* intervals are shaped can matter more than *which* arithmetic operator is used. Overlapping inputs systematically produced smaller output ranges than disjoint inputs, delaying or avoiding early widening. Practical takeaway: when investigating arithmetic joins, start with partially overlapping intervals and widen only as needed; keep operands aligned where normalization is present.

***RQ3: When loops converge—and when they don't.***

Widening can degrade precision in loops, but RQ3 highlights that not all loop updates lead to divergence. Loops whose updated variables are bounded by the loop index (or by monotone guards) often converge to tight ranges quickly; data-driven loops over symbolic containers tend to widen early. Practical takeaway: (i) prefer index-bounded annotations (e.g., bound the iteration count or accessed keys) for loop-local exploration, (ii) materialize only the keys or indices the loop actually touches, and (iii) where necessary, switch to concrete inputs for a small slice of the loop to confirm behavior, then return to symbolic exploration.

Overall, these findings suggest a debugging workflow that starts symbolic and broad, then *shapes* annotations to tighten precision where it matters (overlap, narrow, guard-guided), and finally uses concrete spot checks only for stubborn hot spots (e.g., deeply data-dependent loops).

## 5.3 Limitation

Our current scope and measurements introduce several limitations.

***Scope (external validity).***

We focus on single-contract, single-transaction functions. Inter-contract calls, multi-transaction workflows, proxies, and inheritance hierarchies are out of scope in the present implementation. As a result, we have not yet conducted a developer study in larger project settings; the usability and interpretability of edit-time feedback across multi-contract workflows remain unvalidated.

***Measurement (internal validity).***

Latency numbers combine interpreter execution time (timed in Python) with an estimate for annotation effort per variable (manual input). This procedure ignores UI-event latency and cursor dynamics, and it assumes a consistent operator for annotation entry. Likewise, our precision metric ($F_{90}$: 90th percentile of exit-/input-width inflation) captures a salient aspect of interval growth but does not reflect all developer notions of "useful precision." These choices provide a consistent basis for tool-level

comparison but may under- or over-estimate end-to-end IDE latency or perceived precision.

***Mitigations and future work.***

We plan to (i) extend the analysis to inter-contract calls and multi-transaction scenarios, (ii) instrument editor events to directly measure human-in-the-loop latency and refine the annotation cost model, and (iii) run a controlled developer study once multi-contract support stabilizes. On the analysis side, loop summarization and selective use of lightweight relational domains (e. g., applied on demand to hot spots) are promising avenues to improve precision while preserving interactivity.

# 6 Related Works

## 6.1 Solidity IDEs and Debuggers

Modern Solidity development environments either embed a debugger or integrate external debugging plug-ins. Remix IDE (23) is the most widely used web IDE; it supports syntax highlighting, one-click compilation, and a bytecode-level debugger that lets users step through EVM instructions and inspect stack, memory, and storage. Hardhat (12) is a Node. js–based framework that couples the Solidity compiler with an Ethereum runtime; its Hardhat Debug plug-in attaches a Remix-style debugger to locally broadcast transactions inside Visual Studio Code. Foundry Forge (8) is a command-line toolchain oriented toward fast, reproducible unit testing; the command `forge test` spins up an ephemeral fork, deploys contracts, executes annotated test functions, and enables replay through Forge Debug. Solidity Debugger Pro (30) is a Visual Studio Code extension that performs runtime debugging over concrete transactions and integrates with Hardhat; in practice, many workflows create a small auxiliary contract that calls the target functions so that state changes can be observed step by step.

In short, these debuggers operate on compiled artifacts or post-deployment traces and rely on transaction replay and EVM-level stepping. They do not accept partial, in-flight source fragments nor provide symbolic (interval) input modeling or millisecond edit-time feedback. By contrast, SolQDebug targets pre-deployment authoring, accepts partial fragments and symbolic annotations, and reports line-level effects via abstract interpretation during editing.

## 6.2 Solidity Vulnerability Detection and Verification

A rich body of work analyzes smart contracts for security issues using four main families of techniques. Static analysis tools reason over source or bytecode without running the contract. Representative systems include rule- or pattern–based analyzers such as Securify and Slither (35; 36), symbolic-execution–assisted detectors like Mythril (38), knowledge-graph–based reasoning such as Solidet (13), and bytecode CFG refinement as in Ethersolve (22). Dynamic testing and fuzzing exercise deployed or locally simulated contracts to uncover faults and security issues: ContractFuzzer mutates ABI-level inputs (15), Echidna brings property-based fuzzing into developer workflows

(9), sFuzz adapts scheduling for higher coverage (21), TransRacer finds transaction-ordering races (18), and Ityfuzz leverages snapshotting to decouple executions from chain nondeterminism (26). Formal verification aims to prove safety properties or refute counterexamples at compile time; examples include ZEUS, VeriSmart, and SmartPulse (16; 27; 34). Finally, AI-based approaches train models to predict vulnerabilities or triage candidates, e. g., via data-flow–aware pretraining, IoT-oriented classifiers, or prompt-tuning for detector adaptation (37; 39; 41).

These approaches have substantially advanced vulnerability detection and property checking for fully written contracts. However, they are not designed to provide interactive, edit-time feedback to developers while code is still under construction. They typically analyze post-compilation artifacts or deployed bytecode and expect complete program units. SolQDebug complements this line of work by focusing on pre-deployment authoring: it accepts partial fragments and symbolic (interval) inputs and produces line-by-line feedback inside the editor.

## 6.3 Solidity-Specific Abstract Interpretation Frameworks

Abstract interpretation is a well-established framework for static analysis and has been adapted to many programming languages. Two recent studies apply it to Solidity (10; 11). The first uses the Pos domain to construct a theoretical model for taint (information-flow) analysis Halder et al. (10), while the second employs the Difference-Bound Matrix (DBM) domain to generate state invariants and detect re-entrancy vulnerabilities, including the DAO attack (11; 19). However, both approaches operate on fully written contracts and provide no support for line-by-line interpretation or developer interaction within an IDE.

SolQDebug adapts abstract interpretation for an interactive setting. It incrementally updates both the control-flow graph and the abstract state in response to each edit. Developer-supplied annotations serve as a first-class input mechanism, reflecting how debugging often involves varying symbolic inputs. These annotations are internally represented as linear-inequality constraints, and form an integral part of interactive debugging by enabling symbolic reasoning over developer-specified inputs. This design improves interpretability and control within the interval domain by leveraging symbolic constraints, while maintaining keystroke-level responsiveness. As a result, SolQDebug updates variable ranges directly in the Solidity editor, allowing developers to observe how values evolve in response to each edit.

## 6.4 Interactive Abstract Interpretation for Traditional Languages

In recent years, traditional languages have seen a surge of interest in making abstract interpretation interactive, integrating it directly into IDEs to provide live analysis feedback during editing (4; 7; 24; 32; 33). Stein et al. (32) proposed demanded abstract interpretation, which incrementally rebuilds only the analysis nodes touched by an edit. A follow-up Stein et al. (33) generalized this to procedure summaries, enabling inter-procedural reuse. Erhard et al. (7) extended Goblint with incremental support for multithreaded C, selectively recomputing only genuinely affected facts and maintaining

IDE-level responsiveness. Riouak et al. (24) introduced IntraJ, an LSP-integrated analyzer for Java 11 that computes only the AST and data-flow facts needed for the current view, keeping feedback under 100 ms. Chimdyalwar (4) achieved fast yet precise interval analysis on call graphs via one top-down and multiple bottom-up passes, and later introduced an incremental variant that revisits only the impacted functions.

Unlike these frameworks for C or Java, SolQDebug is designed specifically for Solidity. It supports in-flight code fragments and range annotations as first-class input. It incrementally updates only the current basic block in the CFG while reusing previously computed abstract states. Finally, it combines these with an interval domain guided by developer-supplied annotations, which act as input to represent the exploratory nature of debugging. This architecture enables keystroke-level feedback without requiring recompilation, redeployment, or transaction execution. It bridges the gap between Solidity development and the interactive tooling common in traditional programming environments.

# 7 Conclusion

We introduced SolQDebug, a source-level interactive debugger for Solidity that provides millisecond feedback without requiring compilation, deployment, or transaction replay. By combining interactive parsing, dynamic control-flow graph updates, and interval domain based abstract interpretation seeded by annotations, SolQDebug enables responsive, line-by-line inspection directly within the Solidity editor. Our evaluation shows that it reduces debugging latency compared to Remix, while enabling actionable feedback in response to symbolic inputs. These results demonstrate that SolQDebug's design effectively bridges the interactivity gap in Solidity debugging and brings the development experience closer to that of modern debugging workflows.

Future work includes extending SolQDebug to inter-contract and multi-transaction contexts, incorporating loop summarization for higher precision, and conducting user studies to assess its practical adoption and usability. We also plan to apply analysis based on the EVM Object Format (EOF) to support inter-contract debugging when source code is unavailable, as Ethereum moves toward structured bytecode formats in upcoming hard forks.

# References


ANTLR: https://www.antlr.org/ (2025). Accessed September 2025

ChatGPT: https://chatgpt.com/ (2025). Accessed September 2025

Chen, X., et al.: Characterizing smart contract evolution. ACM Transactions on Software Engineering and Methodology (2025)

Chimdyalwar, B.: Fast and precise interval analysis on industry code. In: 2024 IEEE 35th International Symposium on Software Reliability Engineering Workshops (ISSREW) (2024)

ConsenSys Diligence: Python Solidity Parser. https://github.com/ConsenSysDiligence/python-solidity-parser (2025). Accessed September 2025

Cousot, P., Cousot, R.: Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: Proceedings of the 4th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL) (1977)

Erhard, J., et al.: Interactive abstract interpretation: reanalyzing multithreaded C programs for cheap. International Journal on Software Tools for Technology Transfer (2024)

Foundry Forge: https://book.getfoundry.sh/reference/forge/forge/ (2025). Accessed September 2025

Grieco, G., et al.: Echidna: effective, usable, and fast fuzzing for smart contracts. In: Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), pp. 557–560 (2020)

Halder, R., et al.: Analyzing information flow in Solidity smart contracts. In: Distributed Computing to Blockchain, pp. 105–123. Academic Press (2023)

Halder, R.: State-based invariant property generation of Solidity smart contracts using abstract interpretation. In: 2024 IEEE International Conference on Blockchain (2024)

Hardhat: https://hardhat.org/ (2025). Accessed September 2025

Hu, T., et al.: Detect defects of Solidity smart contract based on the knowledge graph. IEEE Transactions on Reliability 73(1), 186–202 (2023)

JetBrains: PyCharm. https://www.jetbrains.com/pycharm/ (2025). Accessed September 2025

Jiang, B., Liu, Y., Chan, W.K.: ContractFuzzer: fuzzing smart contracts for vulnerability detection. In: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering (ASE) , pp. 259–269 (2018)

Kalra, S., Goel, S., Dhawan, M., Sharma, S.: ZEUS: analyzing safety of smart contracts. In: Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS) (2018)

Llama: https://www.llama.com/ (2025). Accessed September 2025

Ma, C., Song, W., Huang, J.: TransRacer: function dependence-guided transaction race detection for smart contracts. In: Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), pp. 947–959 (2023)

Mehar, M.I., et al.: Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. Journal of Cases on Information Technology (2019)

Microsoft Visual Studio: https://visualstudio.microsoft.com/ko/ (2025). Accessed September 2025

Nguyen, T.D., et al.: sFuzz: an efficient adaptive fuzzer for Solidity smart contracts. In: Proceedings of the 42nd ACM/IEEE International Conference on Software Engineering (ICSE), pp. 778–788 (2020)

Pasqua, M., et al.: Enhancing Ethereum smart-contracts static analysis by computing a precise control-flow graph of Ethereum bytecode. Journal of Systems and Software 200, 111653 (2023)

Remix IDE: https://remix.ethereum.org/ (2025). Accessed September 2025

Riouak, I., et al.: IntraJ: an on-demand framework for intraprocedural Java code analysis. International Journal on Software Tools for Technology Transfer (2024)

Rival, X., Yi, K.: Introduction to Static Analysis: an Abstract Interpretation Perspective (2020)

Shou, C., Tan, S., Sen, K.: Ityfuzz: snapshot-based fuzzer for smart contract. In: Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), pp. 322–333 (2023)

So, S., et al.: Verismart: a highly precise safety verifier for Ethereum smart contracts. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 1678–1694 (2020)

Solidity Compiler in Python (solcx): https://solcx.readthedocs.io/en/latest/ (2025). Accessed September 2025

Solidity documentation: https://docs.soliditylang.org/en/v0.8.29/ (2025). Accessed September 2025

Solidity Debugger Pro: https://www.soliditydbg.org/ (2025). Accessed September 2025

Solidity Language Grammar Rule of SolQDebug : https://github.com/iwwyou/SolDebug/blob/main/Parser/Solidity.g4 . Accessed September 2025

Stein, B., Chang, B.-Y.E., Sridharan, M.: Demanded abstract interpretation. In: Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation (PLDI) (2021)

Stein, B., Chang, B.-Y.E., Sridharan, M.: Interactive abstract interpretation with demanded summarization. ACM Transactions on Programming Languages and Systems (2024)

Stephens, J., et al.: SmartPulse: automated checking of temporal properties in smart contracts. In: 2021 IEEE Symposium on Security and Privacy (SP), pp. 555–571 (2021)

Tsankov, P., et al.: Securify: practical security analysis of smart contracts. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 67–82 (2018)

Tsankov, P., et al.: Slither: a static analysis framework for smart contracts. In: 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), pp. 8–15 (2019)

Wu, H., et al.: Peculiar: smart contract vulnerability detection based on crucial data-flow graph and pre-training techniques. In: 2021 IEEE 32nd International Symposium on Software Reliability Engineering (ISSRE), pp. 378–389 (2021)

Yao, Y., et al.: An improved vulnerability detection system of smart contracts based on symbolic execution. In: 2022 IEEE International Conference on Big Data (Big Data), pp. 3225–3234 (2022)

Yu, L., et al.: PSCVFinder: a prompt-tuning based framework for smart contract vulnerability detection. In: 2023 IEEE 34th International Symposium on Software Reliability Engineering (ISSRE), pp. 556–567 (2023)

Zheng, Z., et al.: Dappscan: building large-scale datasets for smart contract weaknesses in dApp projects. IEEE Transactions on Software Engineering (2024)

Zhou, Q., et al.: Vulnerability analysis of smart contract for blockchain-based IoT applications: a machine learning approach. IEEE Internet of Things Journal 9(24), 24695–24707 (2022)

Zou, W., et al.: Smart contract development: challenges and opportunities. IEEE Transactions on Software Engineering (2019)

**Algorithm 5** Loop Fixpoint at Header

**Require:** loop header (condition) node $h$
**Ensure:** Converged abstract environments at the loop exit and inside the loop

$L \leftarrow$ TraverseLoopNodes$(h)$ ▷ nodes dominated by $h$ and on some back-edge to $h$
$vis[\cdot] \leftarrow 0$; $In[\cdot], Out[\cdot] \leftarrow \bot$
$Start \leftarrow \bigsqcup\{(p) \mid p \in (h) \setminus L\}$ ▷ pre-loop env (exclude back-edges)
$In[h] \leftarrow Start$
$\tau \leftarrow$ EstimateIterations$(h, Start)$ ▷ visit threshold for widening

**// Widening phase (ascending)**
$WL \leftarrow \langle h \rangle$
**while** $WL \neq \langle\rangle$ **do**
  $n \leftarrow WL.\mathsf{pop}()$; $vis[n] \leftarrow vis[n] + 1$
  $\hat{o} \leftarrow$ Transfer$(n, In[n])$
  **if** IsJoin$(n) \wedge vis[n] > \tau$ **then**
    $\hat{o} \leftarrow$ Widen$(Out[n], \hat{o})$
  **else**
    $\hat{o} \leftarrow Out[n] \sqcup \hat{o}$
  **end if**
  **if** IsJoin$(n) \wedge$ CondConverged$(n)$ **then** ▷ optional early stop
    $Out[n] \leftarrow \hat{o}$; **break**
  **end if**
  **if** $\hat{o} \neq Out[n]$ **then**
    $Out[n] \leftarrow \hat{o}$
    **for all** $s \in (n) \cap L$ **do**
      $In[s] \leftarrow \bigsqcup \{$ Flow$(p \to s) \mid p \in (s) \cap L \}$ ▷ edge-pruned join
      $WL.\mathsf{push}(s)$
    **end for**
  **end if**
**end while**

**// Narrowing phase (descending)**
$WL \leftarrow$ any worklist ordering over $L$
**while** $WL \neq \langle\rangle$ **do**
  $n \leftarrow WL.\mathsf{pop}()$
  $\hat{o} \leftarrow$ Transfer$(n, In[n])$
  **if** IsJoin$(n)$ **then**
    $\hat{o} \leftarrow$ Narrow$(Out[n], \hat{o})$ ▷ at least one round; cap by $k_{\max}$
  **end if**
  **if** $\hat{o} \neq Out[n]$ **then**
    $Out[n] \leftarrow \hat{o}$
    **for all** $s \in (n) \cap L$ **do**
      $WL.\mathsf{push}(s)$
    **end for**
  **end if**
**end while**
**return** $Out$ ▷ in particular (LoopExit$(h)$) is now converged