

SolContractEval: A Benchmark for Evaluating Contract-Level Solidity Code Generation

Zhifan Ye^{†§}, Jiachi Chen[†], Zhenzhe Shao[‡], Lingfeng Bao^{†§}, Xiaohu Yang^{†§}, Zhongxin Liu^{†§*}

[†]The State Key Laboratory of Blockchain and Data Security, Zhejiang University, China

[§]Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security, China

[‡]Sun Yat-sen University, China

{yezhiban, lingfengbao, yangxh, liu_zx}@zju.edu.cn, chenjjch86@mail.sysu.edu.cn, shaozhzh3@mail2.sysu.edu.cn

Abstract—The rise of blockchain has brought smart contracts into mainstream use, creating a demand for smart contract generation tools. While large language models (LLMs) excel at generating code in general-purpose languages, their effectiveness on Solidity, the primary language for smart contracts, remains underexplored. Solidity constitutes only a small portion of typical LLM training data and differs from general-purpose languages in its version-sensitive syntax and limited flexibility. These factors raise concerns about the reliability of existing LLMs for Solidity code generation. Critically, existing evaluations, focused on isolated functions and synthetic inputs, fall short of assessing models’ capabilities in real-world contract development.

To bridge this gap, we introduce *SolContractEval*, the first contract-level benchmark for Solidity code generation. It comprises 124 tasks drawn from real on-chain contracts across nine major domains. Each task input, consisting of complete context dependencies, a structured contract framework, and a concise task prompt, is independently annotated and cross-validated by experienced developers. To enable precise and automated evaluation of functional correctness, we also develop a dynamic evaluation framework based on historical transaction replay. Building on *SolContractEval*, we perform a systematic evaluation of six mainstream LLMs. We find that Claude-3.7-Sonnet achieves the highest overall performance, though evaluated models underperform relative to their capabilities on class-level generation tasks in general-purpose programming languages. Second, current models perform better on tasks that follow standard patterns but struggle with complex logic and inter-contract dependencies. Finally, they exhibit limited understanding of Solidity-specific features and contextual dependencies.

Index Terms—Large Language Model, Contract-level Code Generation, Smart Contract, Benchmark

I. INTRODUCTION

The ongoing advancement of blockchain technology and decentralized finance (DeFi) has led to the widespread adoption of smart contracts across various sectors, including finance, gaming, and supply chain [1]. According to DeFiLlama [2], the total value locked (TVL) in Ethereum DeFi protocols exceeded \$80 billion by December 2024, marking a two-year high. Meanwhile, Etherscan [3] data show a steady rise in the daily deployment of new smart contracts, reflecting growing demand for smart contract development. This surge underscores the need for smart contract development tools, including automated code generation solutions.

Recent advances in large language models (LLMs) have shown state-of-the-art performance in automated code generation, particularly in general-purpose languages such as Python and Java [4]–[6]. OpenAI o1 [7], for instance, achieves an impressive 89% pass rate on the HumanEval benchmark [8]. However, their effectiveness remains largely unverified for Solidity [9], the primary language of blockchain development. Moreover, Solidity accounts for only 0.01% of The Stack v2, the pretraining dataset used by models like StarCoder 2 [10], indicating limited training exposure. Solidity differs fundamentally from general-purpose languages in both design and constraints, posing unique challenges for code generation. On one hand, the rapid evolution of the Solidity compiler introduces challenges such as frequent version updates, syntax changes, and inconsistent feature support. On the other hand, its limited language flexibility increases the difficulty of implementing complex functionalities, such as managing dynamic data structures or expressing advanced control logic. This naturally raises a critical question: given the scarcity of training data, can existing LLMs meet Solidity smart contract development requirements?

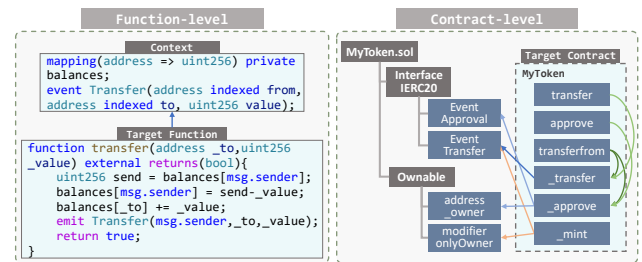


Fig. 1. Function-Level vs. Contract-Level

Notably, most existing research [11], [12] focuses on function-level tasks that mainly assess syntactic correctness and limited contextual reasoning. As illustrated in Figure 1, function-level tasks involve limited context compared to contract-level ones. For example, the target function *transfer* depends only on relevant variables and events within the same contract. This limited scope means function-level generation does not reflect the full complexity of real-world development. In contrast, contract-level generation must handle the full contract, as in the case of *MyToken*, which includes complex

*Corresponding author.

internal calls and dependencies on external contracts such as *IERC20* and *Ownable*. These factors substantially increase generation difficulty, highlighting the limitations of function-level benchmarks for practical evaluation. Furthermore, current evaluation methods largely depend on synthetic test cases or fuzz testing techniques [11], [13], which struggle to capture the dynamic constraints and behavioral patterns of real on-chain transactions. As a result, existing approaches suffer from notable limitations in both task granularity and evaluation methods, making them inadequate for providing a comprehensive analysis of LLM generation quality.

To address the gap in smart contract generation research, this study explores the more challenging and practical contract-level code generation task. Specifically, we focus on generating a single complete and functional contract selected from multi-contract Solidity files, based on a corresponding natural language description. To support this task, we manually construct *SolContractEval*, the first contract-level code generation benchmark. *SolContractEval* comprises 124 generation tasks, with contract code sourced from Etherscan [3], covering nine mainstream application domains, e.g., decentralized finance (DeFi) [14], decentralized gaming (GameFi) [15], and decentralized autonomous organizations (DAOs) [16]. Each task input includes *contract context dependencies*, a *target contract framework*, and a clear *task prompt*. To ensure data quality, each task input is independently annotated and cross-validated by two developers with three years of experience in smart contract development. Furthermore, to accurately and automatically assess the functional correctness of generated contracts, we introduce a **transaction replay mechanism** using real on-chain transactions. By comparing execution results and compilation success, this approach enables a practical evaluation of generation quality.

Building upon the proposed benchmark, we conduct the **first systematic evaluation** of LLMs on contract-level code generation. Specifically, our experiments involve six widely used LLMs that vary in model sizes, underlying architectures, and source providers. For each generated code snippet, we integrate it back into the original contract file and assess the generation performance with two metrics: *Compile@k*, which measures compilation correctness, and *Pass@k*, which evaluates functional correctness.

Based on our empirical study, we summarize the following key findings: *First*, Claude-3.7-Sonnet [17] and o4-mini [18] demonstrate the strongest performance in contract-level code generation, followed by GPT-4o [19], DeepSeek-R1 [20], and Qwen2.5-Coder-32b [21]. *Second*, current LLM shows weaker performance on Solidity contract-level generation than on class-level generation in general-purpose languages. *Third*, models perform relatively well on the most common ERC20 contract type, but show significant shortcomings in generating more complex contracts like ERC721 and DeFi. *Finally*, our error analysis reveals persistent limitations in handling Solidity-specific language features (e.g., compiler version compatibility, type system) and contextual dependency resolution across tested models.

In summary, this paper makes the following contribution:

- The first benchmark *SolContractEval* for contract-level code generation in Solidity, constructed from real-world on-chain contracts and enhanced with historical transaction replay for realistic and reliable functional validation
- The first systematic evaluation of mainstream LLMs on contract-level Solidity code generation, addressing a critical research gap in smart contract development.
- In-depth analysis of model-generated errors, revealing common failure patterns and providing implications for improving LLMs on Solidity-specific generation tasks.
- All code and data for this study are publicly available at <https://github.com/ZJU-CTAG/SolContractEval>.

II. BACKGROUND

A. Explanations of Terminologies

■ **Solidity Source File.** Solidity source files follow a standardized modular architecture [22], which includes the following components: *license identifier* (clarify intellectual property terms), *pragma directive* (ensure version compatibility), *import statements* (enable code modularization and reuse), and *contract definitions* (the core entity for business logic).

■ **Transaction Replay.** Transaction replay verifies state changes by re-executing historical transactions [23]. It restores account states to their pre-execution condition and re-runs the transaction in the same context. Since blockchain nodes usually retain only the latest world state, replaying transactions requires external sources such as archive nodes or state snapshots. In our study, we use this technique to extract post-execution state changes from the first 1,000 transactions for comparison and analysis.

■ **Events.** In Solidity, an event is a logging mechanism used to record critical operations and state changes [24]. An event consists of a declaration and its parameters, and is triggered using the *emit* keyword. Once emitted, the event data is written to the transaction receipt rather than the contract state, enabling low-cost persistence. Their immutable on-chain storage enables reliable asynchronous communication between smart contracts and off-chain systems.

■ **Solidity Compiler Versions.** As of May 2025, the Solidity compiler has officially released 8 major versions and 112 minor versions [9]. Mainstream smart contract development is currently concentrated between versions 0.4 and 0.8, with 0.4 (27 minors) and 0.8 (30 minors) being most prevalent.

■ **NatSpec.** Solidity supports **Ethereum Natural Specification Format (NatSpec)**, a specialized syntax for structured documentation of functions, parameters, and more [25].

B. Distinctive Language Features of Solidity

While Solidity borrows syntax from JavaScript and C++, it differs fundamentally from general-purpose languages in its technical design [26], posing unique challenges for LLMs that perform well in conventional languages but struggle with Solidity's specialized constraints.

1) *Gas Mechanism*: Developers must explicitly manage computational resources, as each state-changing operation incurs a Gas cost. Unlike general-purpose languages optimized for CPU or memory, Solidity prioritizes Gas efficiency.

2) *Immutability*: Solidity’s immutability requires rigorous verification before deployment, since any logic change demands redeploying the entire contract. This contrasts with hot-update mechanisms in traditional software.

3) *State Layering Mechanism*: Solidity enforces a distinction between state storage and temporary memory: storage variables persist on-chain, occupying storage and incurring Gas costs, while memory variables exist only during transaction execution and are charged based on usage.

C. Large Language Models for Code Generation

Code generation, or natural language to code (NL2Code), aims to generate executable code from natural language descriptions automatically and has attracted growing attention from both academia and industry [5], [27], [28]. Large language models (LLMs), including general-purpose models such as GPT-4 [19] and Claude [17], as well as code-focused models like StarCoder 2 [10] and Code Llama [29], have shown strong performance on code generation benchmarks such as HumanEval [8], [30]. This success largely stems from pretraining on large corpora of high-quality code, enabling models to learn general syntax and semantics across languages.

However, training data for these models is heavily imbalanced. Popular languages like Python and JavaScript are richly represented. In contrast, Solidity, the primary language for smart contracts, comprises just 0.01% of Stack v2, the pretraining dataset used by models such as StarCoder 2 [10]. This limited exposure raises concerns about whether current models can generalize effectively to Solidity code generation.

III. BENCHMARK CONSTRUCTION

A. Overview of SolContractEval

SolContractEval is a benchmark dataset for contract-level Solidity code generation, comprising 124 generation tasks. Specifically, **contract-level code generation** means generating a complete, functional target contract from a multi-contract Solidity file based on a natural language description. In our setting, the contract to be generated is the **target contract**, and the original Solidity file it’s drawn from is the **original contract**. All original contracts are real-world contracts deployed on the Ethereum mainnet [31], covering major domains like Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), and GameFi. The table I presents the overall statistics of our benchmark, as well as detailed statistics for the three contract categories with the highest proportions within the benchmark.

Each task consists of three components: (1) **input information** that guides the language model to generate the target contract; (2) a **test suite**, which verifies the functional correctness of the generated code; and (3) the corresponding **original contract**, which serves as a reference for both functionality and structural design.

TABLE I
STATISTICS OF SOLCONTRACTEVAL BENCHMARK.
SCS:SMART CONTRACTS. TXS:TRANSACTIONS PER TEST.

	#Tasks	#Funcs	#Tokens	#Context SCs	#Context Tokens	#TXs
ERC20	52	11.23	1206.79	4.33	1074.04	1000
DeFi	28	9.75	1117.82	4.75	702.50	1000
ERC721	23	17.26	1628.35	16.22	4841.30	1000
Others	21	8.00	1124.38	6.19	1549.33	1000
Overall	124	11.47	1250.93	6.94	1769.40	1000

// Below are some contexts potentially relevant to target contract.		Task Prompt
library MerkleProof {		Context Information
...}		
interface IMerkleDistributor {		
...}		
// You task is to complete the smart contract {MerkleDistributor} strictly according to the provided context and description. Note that the contract is deployed using compiler version {0.6.11}, and do not introduce any additional contracts, dependencies, or unrelated code. Deliver only the complete and functional target contract without any extraneous implementations or examples.		Task Prompt
/**		Contract Description
* @notice A contract for distributing tokens based on a Merkle tree,		
* allowing users to claim their tokens by providing a valid Merkle proof.		
* @dev The contract uses a Merkle tree to verify the validity of claims.		
* It also uses a bit map to keep track of which claims have been made.		
*/		
contract MerkleDistributor is IMerkleDistributor {		Contract Name
address public immutable override token;		State Variable Definition
bytes32 public immutable override merkleRoot;		
mapping(uint256 => uint256) private claimedBitMap;		
constructor(address token, bytes32 merkleRoot_) public {		Constructor
token = token_;		
merkleRoot = merkleRoot_;		
}		
/**		Function Description
* @notice Checks if a particular index has already been claimed.		
* @param index The index in the Merkle tree to check.		
* @return bool True if the index has been claimed, false otherwise.		
* @dev Uses a bit map to efficiently store and check the claimed status of each index.		
*/		
function isClaimed(uint256 index) public view override returns (bool)		Function Signature
{		
}		Function Body
}		

Fig. 2. An Example of the Input Information

To guide the large language model in generating realistic and functional contract code, each code generation task takes the following three components as input, as illustrated in Figure 2: (1) **context information**, which includes relevant functions, variables, and contract definitions extracted from real-world repositories; (2) **target contract framework**, a structured scaffold that outlines contract-level elements; (3) **task prompt**, which specifies the task requirements, including the desired contract name and the compiler version for deployment. The target contract framework serves as the structural backbone for code generation. It contains the contract name, state variable definitions, constructor, function signatures, and their corresponding descriptions. Since this framework is directly used to replay historical transactions and run automated tests, the correctness of generated code critically depends on maintaining consistent interfaces. To enforce this, we preserve the original function signatures and only leave the function bodies blank for the large language model to complete, while keeping all other structural elements intact.

We feed the pre-constructed input information into the model to obtain its response. From the model’s output, we ex-

tract the corresponding target contract implementation and replace the original implementation within the contract structure to form a new generated contract. Both the original contract and the generated contract are then evaluated using the test suite. The evaluation process first checks compilation success, followed by a comparison of execution states, event emissions, and storage results, to further assess the functional correctness and behavioral consistency of the generated contract.

B. Benchmark Construction

This section details the construction of our benchmark for evaluating Solidity code generation, as illustrated in Figure 3, covering source file selection, target contract identification, context extraction, human annotation, and testing generation.

1) **Source File Selection:** We begin by collecting verified smart contract source files from the dataset used in the study by Ajibola et al. [32], sourced from Etherscan [3], the largest repository of open-source, verified contract implementations. To ensure active usage and suitability for transaction-based tests, we filter contracts with more than 1,000 historical transactions, as Zhang et al. [33] demonstrated that this threshold covers common contract functionalities sufficiently. Only contracts with publicly available and compiler-verified source code are retained to enable precise static and dynamic analysis. This process yields 4,640 contract source files, which are then deduplicated using a SimHash [34] algorithm to eliminate syntactically near-identical implementations (e.g., forks or minimal modifications), resulting in 1,278 unique contract source files. To ensure balanced representation across compiler versions, we group deduplicated contracts by their declared Solidity version and randomly select up to 50 source files per group. If a group has fewer than 50, all files are included. This yields 50 files each for the commonly used 0.4.x and 0.8.x versions, and 18, 20, and 16 files for versions 0.5.x, 0.6.x, and 0.7.x, respectively.

2) **Target Contract Identification:** From each collected Solidity source file, we select one **target contract** for the code generation task, mirroring real-world development practices where developers typically implement individual contracts sequentially. To ensure the quality and reliability of the benchmark evaluation, we exclude interface contracts, which contain only function declarations without implementations, abstract contracts, which rely on child contracts to complete their logic, and contracts that only define constructors without implementing any additional functional logic. After filtering, we randomly select one contract from each source file as the target for generation. Random selection minimizes human bias and enhances the benchmark’s objectivity. Finally, we performed deduplication to ensure each contract in the final dataset was unique, preventing potential statistical bias during evaluation, ultimately obtaining 124 distinct contracts.

3) **Context Extraction:** While our task focuses on contract-level code generation, maintaining source file context is crucial for compilation and execution. Missing or unresolved dependencies, such as libraries, inherited contracts, or utility functions, can cause compilation failures or runtime errors

due to undefined references. As illustrated in the contract-level dependency diagram in Figure 1, the arrows represent dependency relationships. For example, the target contract *MyToken* depends on external interfaces like *IERC20* and *Ownable*; if these are not provided, the model may generate undefined references, resulting in compilation errors.

Algorithm 1 Algorithm to Extract Context for Contract

Input: *SC*, *TargetContract* {Input: Smart contract and target contract block}

Output: *Context* {Output: Context of target contract}

```

1: FCG  $\leftarrow$  BuildFCG(SC)
2: Funcs  $\leftarrow$  GetFuncs(TargetContract)
3: ExtFuncs  $\leftarrow$   $\emptyset$ 
4: Context  $\leftarrow$   $\emptyset$ 
5: for each function f  $\in$  Funcs do
6:   Deps  $\leftarrow$  GetExternalDeps(f)
7:   for each dependency dep  $\in$  Deps do
8:     if dep not in ExtFuncs then
9:       ExtFuncs  $\leftarrow$  ExtFuncs  $\cup$  {dep}
10:    end if
11:  end for
12: end for
13: for each function f  $\in$  ExtFuncs do
14:   DepContract  $\leftarrow$  FindContract(f)
15:   Range  $\leftarrow$  GetCodeRange(DepContract, f)
16:   Add(f, Range) to Context
17: end for
18: Return Context

```

Algorithm 1 outlines the systematic process for context extraction, ensuring that generated contracts remain compilable, executable, and functionally equivalent to their original counterparts. The process begins by parsing the target Solidity source file to collect all relevant definitions, including imports, global variables, functions, and inheritance hierarchies. This step aims to capture every element necessary for the contract to operate as intended within its original environment.

Next, we employ Slither [35], a static analysis framework for Solidity, to identify external references that the target contract depends on but does not define internally. These dependencies may include externally invoked functions, inherited contracts, or library methods referenced but not implemented within the target contract.

For each external dependency detected, we locate its definition within the Solidity file’s contracts or libraries and extract the minimal set of required components, specifically the functions, variables, or structures used by the target contract. We isolate the code ranges of referenced functions to avoid including extraneous logic. By incorporating only essential dependencies, we ensure correctness while reducing overhead.

4) **Human Annotation:** In Solidity code generation tasks, the quality of the prompt significantly influences the performance of the generated outputs. To ensure accurate and standardized function descriptions, we engage two developers with at least three years of Solidity development experience



Fig. 3. Overview of SolContractEval Construction Process

to manually write the descriptions for all functions and target contracts in each code generation task. The inclusion of human-annotated comments serves two purposes: 1) to minimize the potential memorization effects of LLMs, as they may have encountered the original comments during pre-training. 2) to provide accurate and consistent function descriptions, ensuring high-quality annotations for the benchmark.

The annotation process follows key standards. First, all comments must comply with the NatSpec documentation format officially recommended by Solidity, using a structured style. Second, to minimize noise, non-functional comments such as copyright notices or irrelevant content are excluded. Third, each function’s purpose and parameters must be described with precision and completeness. Each task instance undergoes dual independent annotation based on these criteria, followed by cross-verification. In cases of disagreement, annotators resolve conflicts through discussion to reach consensus.

5) **Testing Generation:** Evaluating the correctness of smart contract generation is challenging due to the dynamic and stateful nature of contract execution. Unlike traditional code, smart contracts are tightly coupled with the blockchain, where correctness depends not only on isolated function behavior but also on interactions with historical on-chain data, external calls, and mutable state. This complexity renders static analysis and manually crafted test cases insufficient, as they fail to capture real-world execution scenarios.

To address these challenges, we introduce a transaction-driven dynamic validation framework inspired by Zhang et al. [33]. The key idea is to leverage real transaction data to construct realistic test suites that mirror actual contract behavior in production. We implement this by replaying authentic transaction sequences on generated contracts and dynamically monitoring their execution to assess correctness. As shown in Figure 4, this approach enables robust, automated validation under realistic conditions and improves evaluation reliability.

a) **On-Chain Transaction Trace Capture:** We collect the target contract’s historical transaction data through an Ethereum archive node, capturing the complete lifecycle of its first 1,000 transactions. For each transaction, we extract four key categories of execution information to support fine-grained behavioral analysis:

- **Opcode Tracing:** The `debug_traceTransaction` interface is used to record the sequence of EVM instructions.

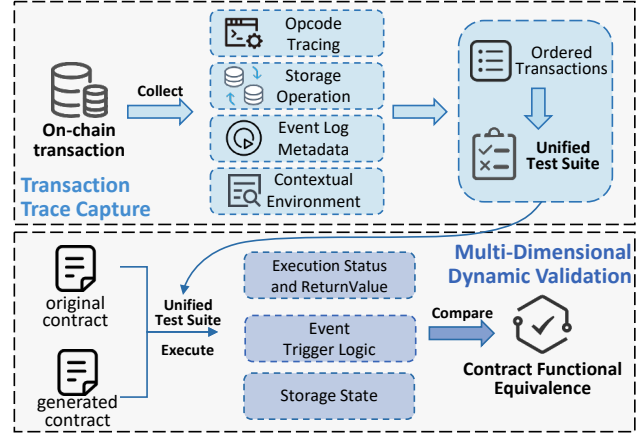


Fig. 4. The Technical Workflow of Testing Generation

- **Storage Operation Snapshot:** All persistent storage *read/write* operations for each transaction are recorded in a structured format as $\langle \text{slot}, \text{oldValue}, \text{newValue} \rangle$ triplets.
- **Event Log Metadata:** Event signatures, indexed parameters, and non-indexed parameters are parsed according to the Application Binary Interface (ABI) specification.
- **Contextual Environment:** The system records the full execution context, including the sender address (`msg.sender`), and block-level context parameters (`block.timestamp`, `block.number`).

To ensure high-quality validation, we integrate the first 1,000 historical transactions into a single unified test sequence, strictly preserving their original on-chain execution order. We avoid splitting these transactions into multiple isolated test cases, as this would break critical dependencies between transactions. Treating them as a coherent whole allows us to more comprehensively capture the behavioral context of the target contract, ensuring the test sequence can reliably assess the functional correctness of the generated contract in realistic environments. Empirical evidence from Zhang et al. [33] further supports this approach, showing that the first 1,000 transactions typically cover commonly used functionalities of a contract, validating the effectiveness of our testing design.

We implement this on the Hardhat [36] local testing network, resetting blockchain state before execution to avoid

cross-test interference. Each transaction is replayed with original contextual parameters (e.g., *msg.sender*, *msg.value*), ensuring consistent state evolution and reliable functional validation.

b) Multi-Dimensional Dynamic Validation: We employ a unified test suite to verify functional equivalence between original and generated contracts across three systematic dimensions. Functional correctness is confirmed only when all three dimensions exhibit consistent behavior.

- **Execution Status and Output Consistency:** The system compares the status field in transaction receipts, requiring strict correspondence between success and revert outcomes. Additionally, the return values are validated byte-by-byte to ensure semantic equivalence of outputs.
- **Event Trigger Logic Equivalence:** Based on the contract ABI, event structures are parsed and validated through a dual-constraint mechanism. First, generated contract event signatures must precisely match the original. Next, parameters undergo rigorous comparison, including hash verification of indexed parameters and value-by-value checks for non-indexed ones. These checks ensure structural and content-level accuracy in event behavior.
- **Storage State Consistency:** Key state variables (e.g., *totalSupply*, *allowance*) are hashed before and after each transaction using SHA3-256. A state evolution chain is constructed to verify consistent state transitions across the original and generated contracts.

IV. EXPERIMENTAL SETUP

Using SolContractEval, we conduct a comprehensive study to evaluate LLMs on contract-level Solidity code generation, guided by the following research questions.

- **RQ1 (Overall Correctness):** How do LLMs perform on Solidity contract-level code generation?
- **RQ2 (Performance across Different Contract Categories):** How does model performance vary across smart contract categories?
- **RQ3 (Incorrect Case Analysis):** What are the common errors during Solidity contract-level code generation?

A. Studied LLM

In this study, we evaluate six state-of-the-art LLMs that have demonstrated strong performance in code generation and are widely adopted in recent research [37], [38]. For closed-source models, we select leading commercial options, including OpenAI’s GPT-4o [19] and o4-mini [18], Anthropic’s Claude-3.7-sonnet [17], and Google DeepMind’s Gemini-2.0-flash-exp [39]. For open-source models, we include DeepSeek-AI’s DeepSeek-R1 [20] and Alibaba’s Qwen2.5-Coder-32b-instruct [21]. These models have exhibited strong performance across multiple code generation benchmarks, demonstrating their capabilities in practical applications.

B. Evaluation Metrics

In this study, we adopt the *Pass@k* and *Compile@k* metrics to evaluate the generated Solidity code in terms of functional and compilation correctness, respectively. Both are based on

the widely used *Pass@k* framework [8], [40], [41]. For each task, the model generates n candidate code samples, and the task is considered successful if at least one of the top- k samples meets the evaluation criterion, passing all unit tests for *Pass@k* or compiling successfully for *Compile@k*. To mitigate the variance introduced by random sampling, we adopt the unbiased estimator from the HumanEval benchmark [8]:

$$\text{Compile@k/Pass@k} = \mathbb{E}_{\text{Problems}} \left[1 - \frac{\binom{n-c}{k}}{\binom{n}{k}} \right] \quad (1)$$

where n is the total number of generated samples, c is the number of correct (i.e., passing or compilable) samples, and k is the sampling budget per task.

To compare contract-level generation with function-level generation, we introduce two evaluation metrics for this setting: *Function Pass Rate (FPR)* and *Contract Full Pass Rate (CFPR)*. Each has two variants, with subscripts “c” and “p” indicating compilation and test success, respectively.

Function Pass Rate (FPR) measures the accuracy of the model when generating individual functions. Specifically, FPR is the ratio of successfully compiled (or tested) functions P to the total number of generated functions M , i.e., $FPR_c/FPR_p = \frac{P}{M}$. This metric reflects function-level Pass@1, assuming one generation attempt per function.

Contract Full Pass Rate (CFPR) measures whether a contract can compile and pass all tests when each function is generated independently. If all individually generated functions can be re-integrated into the original contract and still compile (or pass tests), the contract is considered “fully passed”. Thus, CFPR is the ratio of fully passed contracts K to the total number of contracts N , i.e., $CFPR_c/CFPR_p = \frac{K}{N}$.

C. Implementation Details

We evaluate the generated contracts using two primary metrics: *Compile@k*, which measures compilation correctness, and *Pass@k*, which assesses functional correctness. Following recent practice [40], we adopt two sampling strategies for code generation: (1) **nucleus sampling**, in which five candidate code completions are generated per task using a temperature of 0.2 and top_p of 0.95 [8]; and (2) **greedy sampling**, in which a single deterministic completion is generated using a temperature of 0. For both metrics, greedy sampling is used when $k = 1$, while nucleus sampling is applied when $k > 1$. To ensure fair model comparison, we invoke APIs with consistent hyperparameter settings. All experiments are run on a high-performance server with Ubuntu 20.04.5 LTS, 128 Intel(R) Xeon(R) Platinum 8358P CPUs @ 2.60GHz, and 8 NVIDIA A800 GPUs (80GB each), providing a stable environment for large-scale code generation and evaluation.

V. RESULTS

A. RQ1: Overall Correctness

Our comprehensive evaluation of six state-of-the-art LLMs on the SolClassEval benchmark reveals their comparative performance, as detailed in Table II.

TABLE II
OVERALL RESULTS ON SOLCONTRACTBENCH.

Model	Compile@1(%)	Compile@3(%)	Compile@5(%)	Pass@1(%)	Pass@3(%)	Pass@5(%)
gemini-2.0-flash-exp	63.55	69.66	72.03	29.03	32.66	33.87
qwen2.5-coder-32b-instruct	68.54	78.62	84.67	25.97	33.63	35.48
deepseek-R1	67.74	81.77	86.29	29.84	37.10	40.32
gpt-4o	68.54	90.32	94.35	33.39	42.10	45.16
o4-mini	81.45	93.54	95.97	35.00	42.18	44.35
claude-3-7-sonnet-20250219	85.48	93.54	96.77	40.65	46.05	49.19

Compilation Correctness. Claude-3-7-Sonnet performs best, leading in both *Compile@1* (greedy sampling) and *Compile@k* (nucleus sampling) at the function level. o4-mini follows closely, with only a 4.03% lower *Compile@1* but nearly matching Claude-3-7-Sonnet at *Compile@k*, indicating comparable robustness. GPT-4o, DeepSeek-R1, and Qwen2.5-Coder-32b come next, all maintaining *Compile@1* rates around 68%. Notably, GPT-4o shows the greatest gain with nucleus sampling, suggesting strong performance under diverse decoding strategies. In contrast, Gemini-2.0-Flash-Exp performs worst due to recitation errors (see Section VI-A), which frequently lead to compilation failures under both sampling methods.

Functional Correctness. In terms of functional correctness, Claude-3-7-Sonnet again leads, with a *Pass@1* score 5.65% higher than the second-best model. Although o4-mini ranks highly in compilation success, its functional correctness is only slightly better than GPT-4o, indicating room for improvement in logical accuracy and context comprehension. Deepseek-R1, Qwen2.5-Coder-32b, and Gemini-2.0-Flash-Exp perform relatively poorly in functional implementation, with Qwen2.5-Coder-32b ranking last in *Pass@1*. Interestingly, Gemini-2.0-Flash-Exp, affected by the "recitation" issue, shows comparable functional correctness to Qwen2.5-Coder-32b.

Findings 1: In Solidity contract-level code generation, Claude-3-7-Sonnet and o4-mini lead, followed by GPT-4o, DeepSeek-R1, and Qwen2.5-Coder-32b, with Gemini-2.0-Flash-Exp performing the worst.

Contract-level code generation v.s. Function-level code generation. To assess the greater challenge posed by contract-level generation compared to function-level generation, we conduct function-level experiments on the benchmark using all six models. Specifically, for each target contract, we treat each function as an independent generation target, masking only the corresponding function body while preserving the implementation of other functions. This ensures that the contextual information remains consistent with the contract-level setting.

As shown in Table III, all models achieve significantly better performance under the function-level setting across various evaluation metrics. For example, the FPR_p , which reflects model accuracy on individual function generation, is higher than *Pass@1* by 38.52% on average. Claude-3-7-Sonnet achieves FPR_c/FPR_p scores of 96.23%/80.42%, while its *Compile@1/Pass@1* scores under the contract-level setting are

TABLE III
PERFORMANCE COMPARISON: FUNCTION-LEVEL VS. CONTRACT-LEVEL.

Model	Function		Contract Compile@1	Function		Contract Pass@1
	FPR_c	$CFPR_c$		FPR_p	$CFPR_p$	
gemini	82.77	68.18	63.55	68.67	55.45	29.03
qwen2.5	92.12	76.14	68.54	71.15	54.12	25.97
deepseek	92.62	77.53	67.74	67.09	53.37	29.84
gpt-4o	93.22	85.36	68.54	72.28	60.16	33.39
o4-mini	95.08	84.23	81.45	71.89	61.73	35.00
claude	96.23	86.71	85.48	80.42	65.85	40.65

only 85.48%/40.65%, indicating that models tend to perform better on isolated function tasks, possibly due to the more clearly defined context.

Furthermore, we compare the overall contract correctness under both settings by focusing on the CFPR for function-level and the corresponding metrics for contract-level. CFPR measures whether all functions within a contract can be independently compiled or pass their corresponding tests. The gap between the two settings is substantial. For example, GPT-4o achieves $CFPR_c/CFPR_p$ scores of 85.36%/60.16% at the function level, compared to just 68.54%/33.39% (*Compile@1/Pass@1*) at the contract level. This suggests that while models are capable of generating individual functions well, generating multiple functions simultaneously often leads to semantic inconsistencies or interaction errors, resulting in a significantly higher failure rate.

Findings 2: Higher function-level scores show isolated tasks are easier, while the gap with contract-level results highlights the challenge of maintaining inter-function consistency, essential in real-world development, making contract-level generation a more realistic and challenging setting.

Compare to Other Benchmark. To compare Solidity benchmarks with those for general-purpose programming languages, we select ClassEval [40], a class-level benchmark of similar granularity to ours. We evaluate the GPT-3.5 [42] model used in the ClassEval paper on SolContractEval to ensure fair comparison. The results show a performance gap: GPT-3.5 achieves 29.6%/34.9%/36.0% on ClassEval's *Pass@1/3/5* for class-level generation, while its performance on SolContractEval drops to 12.1%/15.6%/16.9%, respectively. This substantial gap highlights the unique challenges of smart contract generation compared to general-purpose code and underscores the importance of SolContractEval in evaluating LLM capabilities for Solidity code generation.

Findings 3: Compared to class-level code generation in general-purpose languages, current LLMs show weaker performance on Solidity contract-level generation, suggesting that contract-level tasks may pose additional challenges. This underscores the need for specialized benchmarks to better assess model capabilities in this domain.

B. RQ2: Performance across Different Contract Categories

To analyze performance variations across contract categories, we calculate metrics for each category, select the three most prevalent by sample size, compute the model’s average performance across them, and compare it with overall performance, as shown in Figure 5.

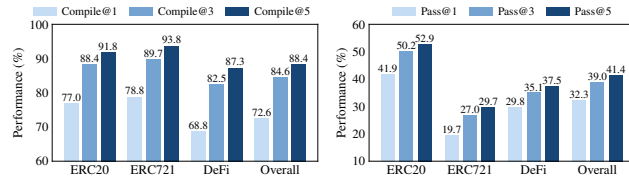


Fig. 5. Model Performance Across Different Contract Categories

ERC20. In this benchmark test, the ERC20 category accounts for the largest proportion, reaching 41.9%. The models exhibit better performance in this category compared to the overall average, with a slight improvement in compilation success rates and a substantial increase of 6.5% in *Pass@1*. This indicates that the models have a strong understanding of the ERC20 standard, which is widely adopted in practical development and features a stable, well-defined interface. This maturity enables the models to effectively learn diverse implementation patterns and best practices from training data. This extensive knowledge enhances the models’ ability to generate targeted and accurate code, resulting in notable improvements in both compilation success rates and functional performance.

ERC721. Similarly, ERC721, another standardized token category, accounts for 18.6% of the benchmark. Among the six models tested, four demonstrate significantly higher compilation success rates than the overall average, with overall performance surpassing that of ERC20. Only Qwen2.5-Coder-32b and Gemini-2.0-Flash-Exp show slightly inferior performance. However, in terms of functional correctness, ERC721 is the worst-performing category, with only Claude-3-7-sonnet reaching the overall average, while the remaining models exhibit varying degrees of decline.

Reason Analysis. The performance difference between ERC20 and ERC721 contracts stems from several factors. ERC20 contracts cover multiple compiler versions (0.4 to 0.8), posing challenges for models to handle syntax variations across versions. In contrast, ERC721 contracts mainly target version 0.8, avoiding version compatibility issues and yielding relatively higher compilation success. However, ERC721 involves more complex logic and dependencies, such as ownership management, authorization controls, and security checks. These features are difficult to capture with simple patterns,

making models prone to logical errors. Moreover, ERC721 typically depends on additional interfaces like ERC165 and IERC721Metadata, increasing generation complexity and negatively affecting functional correctness.

DeFi. In the benchmark, DeFi contracts account for a notable proportion (22.58%). The models show a slight decline in compilation success rates for this category, with a 3.8% decrease in the *Compile@1* metric. This may be due to complex blockchain operations commonly used in DeFi contracts, such as *delegatecall* and *abi.encodePacked*, which can cause syntax or type errors during model generation, resulting in compilation failures. Nevertheless, regarding functional correctness, the models’ performance on DeFi contracts is consistent with the overall level, indicating the models have acquired a reasonable understanding of core logic and common patterns in this category.

For other categories (such as Gaming and Proxy contracts), the number of samples is relatively small, each accounting for less than 10%. As a result, the evaluation results in these categories may exhibit certain randomness.

Conclusion. Standardized tokens like **ERC20** provide unified interfaces and mature implementations that help models generate code with high compilation success and functional correctness. In contrast, non-standard contracts (e.g., DeFi, Gaming) lack consistent patterns and diverse logic, making generation more error-prone and less reliable. This variability remains a key challenge for improving model output quality.

Findings 4: Models excel in generating simple standardized contracts like ERC20, but struggle with complex logic in ERC721 and diverse operations in DeFi contracts, highlighting the challenges of non-standardized code.

C. RQ3: Incorrect Case Analysis

To help developers better leverage LLMs for smart contract code generation, we further analyze the common issues encountered in current models. Specifically, we examine code artifacts from the 124 generation tasks and categorize the identified issues into the following two types for detailed analysis: *compilation errors* and *testing errors*.

1) Compilation Errors: In smart contract development, compilation errors involve not only syntax issues but also potential deficiencies in handling specific risk scenarios. We systematically analyze compilation errors by first identifying the compiler version used in on-chain contracts and compiling corresponding generated contracts with that version, collecting 985 error logs. Using open card sorting [43], we categorize these into 5 major types and 17 subcategories (Table IV). Among the major error types, *ParserError* (37.21%) and *TypeError* (36.43%) dominate, while *DeclarationError* (21.71%) is also frequent, together accounting for over 95% of all errors. These results suggest that current models often fail at basic syntax understanding, type handling, and declaration correctness during contract-level code generation. Further analysis of the subcategory errors reveals the following key issues:

TABLE IV
SYNTAX ERRORS OF LLM-GENERATED CODE.

Category	Proportion
ParserError	37.21%
Event triggering method error	22.48%
Missing parentheses/semicolon	6.20%
Syntax structure error	5.43%
Receive function version issue	3.10%
TypeError	36.43%
Override keyword conflict	8.53%
Contract member unavailable	6.20%
Type conversion error	6.20%
Function parameter count mismatch	5.43%
Function parameter type mismatch	4.65%
Pure/View keyword conflict	2.33%
Storage type conversion error	1.55%
Member access error	1.55%
DeclarationError	21.71%
Undefined identifier	15.50%
Variable redefinition	4.65%
Call to invisible function	1.55%
Other Errors	2.33%
Stack depth limit	2.33%
Incorrect association with function parameter	1.55%
Others	0.78%

Inadequate Adaptation to Compiler Versions: For example, starting from Solidity version 0.4.21, the *emit* keyword is introduced to trigger events, whereas earlier versions do not require it. Similarly, the *receive* function becomes the standard function for receiving Ether in version 0.6.0, replacing the previous *function()* syntax. Errors related to event triggering and the *receive* function together account for 25.58% of all compilation failures, indicating that current models have not sufficiently learned to adapt to syntax changes across different Solidity versions.

Weak Understanding of Type System and Storage Mechanisms: Unlike other general-purpose languages, Solidity employs a state layering mechanism, introducing *storage* and *memory* to represent variable locations, and variable types are limited with less flexible type conversion. The generated code frequently violates these rules, including type conversion errors (6.20%), parameter type mismatches (4.65%), and storage type conversion errors (1.55%), which together account for 12.40% of all compilation errors. These results indicate a weak understanding of Solidity’s type system and storage semantics in current models.

Errors in Syntax Rules and Keyword Usage: Solidity uses the *pure* and *view* keywords to define function visibility and *override* to indicate method overriding. However, the generated code often misuses these keywords, with *pure/view* keyword errors accounting for 2.33% and *override* conflicts for 8.53% of all compilation errors. Additionally, the model exhibits flaws in handling complex Solidity-specific syntax structures, such as *abi.encodePacked*, *abi.encodeWithSignature*, and *delegatecall*. Furthermore, basic syntax errors, such as missing parentheses or semicolons (6.20%) and function parameter count mismatches (5.43%), are also frequent, highlighting the

model’s lack of proficiency in Solidity syntax compared to its performance in general-purpose languages like Python and Java.

Insufficient Context Dependency Handling: For contract-level code generation, understanding contextual dependencies is crucial. However, common compilation errors include duplicate variable declarations and calling undefined identifiers, both of which occur at a rate of 20.15%. This indicates the model’s insufficient grasp of contextual information within the Solidity development environment.

Findings 5: In LLMs generated smart contracts, compilation errors are most commonly seen as *ParseError* and *TypeError*. Among them, errors caused by Solidity-specific features (such as compiler version compatibility and type system) account for 49.61%, while errors due to insufficient context understanding account for 21.71%.

2) Testing Errors: In our test suite, we focus on evaluating the consistency of generated contracts in three aspects: *return values*, *event triggers*, and *storage states*. However, the generated contracts often exhibit various types of inconsistencies in these aspects. Our statistics show that return value inconsistencies have the highest proportion at 45.18%, followed by storage state inconsistencies at 43.05%, and event trigger inconsistencies being the lowest at 11.86%.

These inconsistencies reveal multiple potential deficiencies in the model’s code generation capabilities. *Return value inconsistencies* often result from the model’s failure to accurately understand function logic or generate erroneous code in conditional statements and loops, leading to incorrect results for callers. *Event trigger inconsistencies* indicate the model’s limited understanding of the Solidity event mechanism, which may prevent critical operations from being captured in logs or blockchain explorers, reducing system transparency. *Storage state inconsistencies* expose the model’s shortcomings in variable management, which may cause subsequent transactions to operate on incorrect data or even lead to security vulnerabilities, such as reentrancy attacks or unauthorized access. The following are two typical error cases:

```

/**
 * @notice Allows the admin to mint new tokens to a specified user.
 * @dev Only the admin can call this function. The user must be
 * mintable.
 * @param user The address of the user to receive the new tokens.
 * @param quantity The raw (unadjusted) amount of tokens to mint.
 */
function mintNewDNC(address user, uint256 quantity) public onlyadmin{
    uint256 correctedQuantity = quantity * (10**(decimals-1));
    if(mintable[user] == true) {
        totalSupply = totalSupply.add(correctedQuantity);
        balances[user] = balances[user].add(correctedQuantity);
        Transfer(0, user, correctedQuantity);
        Minted(user, correctedQuantity);
        balances[user] = balances[user].add(quantity);
        totalSupply = totalSupply.add(quantity);
        Minted(user, quantity);
        Transfer(0x0, user, quantity);
    }
}

```

Fig. 6. Example of Misunderstanding Implicit Conditions

Testing Error 1: Misunderstanding Implicit Conditions:

In the `mintNewDNC` function shown in Figure 6, the generated code fails to handle token decimal adjustments. The docstring describes parameter `quantity` as a *raw (unadjusted) amount*, implicitly indicating an adjustment is needed. However, the model uses the parameter directly, missing this requirement.

```
/**
 * @notice Depreciates the mint and mints remaining tokens to
 * the deployer.
 * @dev This function can only be called by the contract owner
 * and depreciates the mint, mints 66 tokens to the deployer, and
 * sets the mint status.
 */
function depreciateMint() external onlyOwner {
  ✓ require(!depreciatedMint, "Mint is already depreciated.");
  depreciatedMint = true;
  publicStatus = false;
  huntlistStatus = false;
  // Mint 66 tokens to the deployer
  for (uint i = 0; i < 66; i++) {
    if (totalSupply < maximumSupply) {
      totalSupply++;
      _mint(msg.sender, totalSupply);
    }
  }
}
```

Fig. 7. Example of Lack of Context Understanding

Testing Error 2: Lack of Context Understanding:

In generating the `depreciateMint` function, the model fails to fully understand the context. It omits the necessary condition check for the `depreciateMint` variable at the beginning of the function, which is explicitly described in comments as a flag to prevent multiple calls. This oversight allows the function to be repeatedly called, leading to functional deviations.

VI. DISCUSSION

A. Recitation for LLMs

In our evaluation of the Gemini-2.0-Flash-Exp model, we observe a recitation error in 12.54% of the tests. This error occurs when the LLM detects that the generated output significantly overlaps with copyright-protected or highly similar content from the training data [44]. To prevent copyright infringement, the model halts generation and labels the output as “recitation”. This mechanism serves as a safeguard against unauthorized content reproduction.

However, in the context of smart contract code generation, which is inherently highly standardized and repetitive (e.g., the ERC20 token standard), this mechanism can become problematic. Even though we have rewritten comments in our benchmark to mitigate such issues, the recurring structure and standardized nature of smart contracts make it challenging to avoid recitation. The model struggles to distinguish between legitimate reuse of standard code patterns and potential copyright infringement, resulting in false positives.

Addressing this issue is essential for future smart contract development, as it highlights the need for refined mechanisms that can accurately differentiate between valid standard code reuse and inappropriate content reproduction, thereby minimizing the risk of erroneous recitation.

B. Implications

1) *For Model Developers:* Our study shows that current LLMs achieve insufficient performance on Solidity contract-level generation compared to function-level generation, and frequently produce *ParseError* and *TypeError* issues, particularly those stemming from compiler version incompatibilities, type system misuses, and insufficient handling of contextual dependencies (see Findings 2 and 5). These results indicate that existing models struggle to capture Solidity-specific syntax variations and to maintain inter-function consistency. To address these limitations, model developers could incorporate more version-diverse training data, adopt semantics-preserving data augmentation strategies that emphasize inter-function interactions, and apply structure-aware decoding constraints to reduce syntax and type errors. Additionally, introducing compiler version information as explicit control signals during decoding may help mitigate version-related failures.

2) *For Smart Contract Developers:* We find that while models perform well on standardized ERC20 contracts, they struggle with more complex categories such as ERC721 and DeFi, often producing logically inconsistent or incomplete implementations (see Findings 3 and 4). These categories remain challenging for current models, likely due to their intricate logic and heavy inter-contract dependencies. Developers should therefore exercise heightened caution when adopting such code in practice. Specifically, they could conduct thorough manual reviews of dependency handling and state management logic, carefully check for subtle semantic defects such as incorrect event triggers or missing condition checks (see Section V-C), and avoid assuming correctness solely based on successful compilation, given the high prevalence of semantic inconsistencies revealed by our dynamic evaluation.

3) *For Researchers:* We present SolContractEval, addressing the lack of standardized contract-level benchmarks for smart contract generation by providing a reproducible dataset built from real-world contracts with contextual integrity. Our test case construction method is generalizable and can serve as a blueprint for developing future smart contract benchmarks. Building on this foundation, future research could explore fine-grained error attribution, aiming to pinpoint errors at the level of individual components and dependencies within generated contracts, and develop hybrid evaluation approaches that combine static analysis with transaction replay to more accurately assess and localize semantic errors.

C. Threat to Validity

1) *Internal Threats:* In constructing the benchmark dataset, we recognize the potential risk of data leakage between the benchmark data and the model’s training data. To mitigate potential data leakage, two developers with three years of smart contract experience independently rewrite the original comments into structured NatSpec documentation, ensuring semantic accuracy while significantly differing from the source. All annotations are cross-verified to ensure consistency and to minimize subjective bias during manual annotation. We

also conduct a preliminary qualitative comparison with existing benchmarks from other programming domains to provide a rough performance reference (see Section V-A). However, due to inherent differences across programming domains, it is difficult, if not impossible, to control variables such as task design and data distribution to ensure a fully equitable comparison. Thus, our comparison should be interpreted as suggestive rather than as a rigorous quantitative evaluation of task difficulty.

2) *External Threats*: While our evaluation focuses on three widely used smart contract types, which may not capture the full diversity of contract forms in the ecosystem, these types represent common real-world use cases. Moreover, SolContractEval is designed for extensibility, allowing more categories to be incorporated in future work to broaden coverage. Additionally, due to time and cost constraints, this study evaluates six LLMs, so findings may not fully represent all models. Nevertheless, we include representative state-of-the-art models from different families (e.g., GPT, Gemini, Claude) to ensure the reliability of our conclusions.

VII. RELATED WORK

A. Code Generation Benchmark

Most existing benchmarks focus on general-purpose languages [8], [40], [41], [45], [46]. For instance, HumanEval [8] includes 164 tasks on language comprehension and algorithms, while MBPP [45] offers 974 beginner-level Python functions. In more complex settings, CoderEval [41] proposes a repository-level benchmark with 460 Python/Java tasks from open-source projects, and ClassEval [40] introduces a class-level benchmark with 100 Python class tasks validated by test suites. Despite rapid progress in benchmarking for general-purpose languages, benchmarks tailored to Solidity remain scarce.

BenchSol [13] is the first to evaluate LLMs on Solidity, providing 15 manually designed tasks with Hardhat tests. SolEval [11] extends this to a repository-level benchmark of 1,125 real-world contracts from GitHub for multi-dimensional assessment. SolBench [12] further emphasizes function-level generation, collecting 4,178 functions from on-chain contracts for functional testing. These benchmarks have several limitations: 1) they primarily focus on function-level generation or overly simplistic contracts, failing to capture the complexity of real-world scenarios; 2) functional testing is often conducted using manually constructed cases or fuzzing, which makes it hard to capture issues that may arise in real applications.

In contrast, our *SolContractEval* is the first contract-level benchmark for Solidity code generation, differing from prior work in both task design and evaluation. Built from real deployed contracts, it requires models to generate full contracts with contextual dependencies such as inheritance and inter-function interactions. To assess functional correctness, SolContractEval replays historical on-chain transactions and analyzes runtime behavior from multiple perspectives.

B. Code Generation in Smart Contract

Dade et al. [47] proposed MazzumaGPT, an optimized LLM for Web3 smart contract generation, enhancing efficiency while preserving functional correctness. Wang et al. [48] introduced CodeBC, which uses a three-stage fine-tuning strategy to optimize CodeLlama. By leveraging a security tag mechanism to guide generation, it mitigates security risks without manual vulnerability labels. Napoli et al. [49] developed a contract generation system based on the CO-STAR prompt optimization framework, integrating tools like Slither to form a comprehensive quality assurance pipeline. These works remain in the exploratory stage, facing challenges such as inconsistent evaluation standards and limited testing scenarios. Our work complements them by providing a comprehensive and objective benchmark through systematic test case design and multi-dimensional evaluation metrics.

VIII. CONCLUSION

In this paper, we propose *SolContractEval*, a contract-level benchmark for Solidity code generation, addressing the current lack of evaluation tools for LLMs in real-world Solidity development scenarios. We conduct the first empirical study on contract-level code generation using six state-of-the-art LLMs. Our results show that Claude-3.7-Sonnet and o4-mini lead in contract-level Solidity generation performance. Second, LLMs underperform compared to class-level generation in general-purpose tasks. Notably, ERC20 contracts, the most widely used category, also yield the most stable generation results. Furthermore, Solidity's inherent characteristics, such as its strict type system, compiler version dependencies, and layered storage model, pose major challenges for accurate contract generation.

ACKNOWLEDGMENT

This research/project was supported by the National Natural Science Foundation of China (No.62202420), Zhejiang Provincial Natural Science Foundation of China (No.LZ25F020003), the National Natural Science Foundation of China (No.62372398 and No.72342025), and the Fundamental Research Funds for the Central Universities (No.226-2025-00067).

DATA AVAILABILITY

All code and data for this study are publicly available at <https://github.com/ZJU-CTAG/SolContractEval>.

REFERENCES

- [1] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.
- [2] DeFillama, "Total value locked in defi," 2025, <https://defillama.com/>.
- [3] etherscan, 2025, <https://etherscan.io/>.
- [4] J. Wang and Y. Chen, "A review on code generation with llms: Application and evaluation," in *2023 IEEE International Conference on Medical Artificial Intelligence (MedAI)*, 2023, pp. 284–289.
- [5] J. Jiang, F. Wang, J. Shen, S. Kim, and S. Kim, "A survey on large language models for code generation," *arXiv preprint arXiv:2406.00515*, 2024.

- [6] L. Deng, X. Ren, C. Ni, M. Liang, D. Lo, and Z. Liu, "Enhancing project-specific code completion by inferring internal api information," *IEEE Transactions on Software Engineering*, 2025.
- [7] "OpenAI o1 Hub | OpenAI," <https://openai.com/o1/>.
- [8] M. Chen, J. Tjokrek, H. Jun, Q. Yuan, H. P. D. O. Pinto, J. Kaplan, H. Edwards, Y. Burda, N. Joseph, G. Brockman *et al.*, "Evaluating large language models trained on code," *arXiv preprint arXiv:2107.03374*, 2021.
- [9] solidity, 2025, <https://soliditylang.org/>.
- [10] A. Lozhkov, R. Li, L. B. Allal, F. Cassano, J. Lamy-Poirier, N. Tazi, A. Tang, D. Pykhtar, J. Liu, Y. Wei *et al.*, "Starcode 2 and the stack v2: The next generation," *arXiv preprint arXiv:2402.19173*, 2024.
- [11] Z. Peng, X. Yin, R. Qian, P. Lin, Y. Liu, C. Ying, and Y. Luo, "Soleval: Benchmarking large language models for repository-level solidity code generation," *arXiv preprint arXiv:2502.18793*, 2025.
- [12] Z. Chen, H. Qin, N. Chen, X. Zhao, L. Xue, X. Luo, and X.-M. Wu, "Solbench: A dataset and benchmark for evaluating functional correctness in solidity code completion and repair," *arXiv preprint arXiv:2503.01098*, 2025.
- [13] E. Daspe, M. Durand, J. Hatin, and S. Bradai, "Benchmarking large language models for ethereum smart contract development," in *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2024, pp. 1–4.
- [14] J. R. Jensen, V. von Wachter, and O. Ross, "An introduction to decentralized finance (defi)," *Complex Systems Informatics and Modeling Quarterly*, no. 26, pp. 46–54, 2021.
- [15] J. Proelss, S. Sévigny, and D. Schweizer, "Gamefi: The perfect symbiosis of blockchain, tokens, defi, and nfts?" *International Review of Financial Analysis*, vol. 90, p. 102916, 2023.
- [16] C. Santana and L. Albareda, "Blockchain and the emergence of decentralized autonomous organizations (daos): An integrative model and research agenda," *Technological Forecasting and Social Change*, vol. 182, p. 121806, 2022.
- [17] Anthropic, "Claude 3.7 sonnet," 2025, <https://www.anthropic.com/claude/sonnet>.
- [18] OpenAI, "Introducing openai o3 and o4-mini," 2025, <https://openai.com/index/introducing-o3-and-o4-mini/>.
- [19] —, "Gpt-4o," 2024, <https://platform.openai.com/docs/models/gpt-4o>.
- [20] D. Guo, D. Yang, H. Zhang, J. Song, R. Zhang, R. Xu, Q. Zhu, S. Ma, P. Wang, X. Bi *et al.*, "Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning," *arXiv preprint arXiv:2501.12948*, 2025.
- [21] B. Hui, J. Yang, Z. Cui, J. Yang, D. Liu, L. Zhang, T. Liu, J. Zhang, B. Yu, K. Lu *et al.*, "Qwen2. 5-coder technical report," *arXiv preprint arXiv:2409.12186*, 2024.
- [22] solidity, "Introduction to smart contracts," 2025, <https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html>.
- [23] Y. Huang, R. Wang, X. Chen, and Z. Zheng, "Ethereum transaction replay platform based on state-wise account input data," *IEEE Transactions on Services Computing*, vol. 17, no. 5, pp. 2404–2416, 2024.
- [24] L. Li, Y. Liang, Z. Liu, and Z. Yu, "Understanding solidity event logging practices in the wild," in *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 2023, pp. 300–312.
- [25] "NatSpec Format — Solidity 0.8.30 documentation," <https://docs.soliditylang.org/en/v0.8.30/natspec-format.html>.
- [26] Z. Wang, X. Chen, X. Zhou, Y. Huang, Z. Zheng, and J. Wu, "An empirical study of solidity language features," in *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2021, pp. 698–707.
- [27] D. Zan, B. Chen, F. Zhang, D. Lu, B. Wu, B. Guan, Y. Wang, and J.-G. Lou, "Large language models meet nl2code: A survey," *arXiv preprint arXiv:2212.09420*, 2022.
- [28] M. Chen, Z. Liu, H. Tao, Y. Hong, D. Lo, X. Xia, and J. Sun, "B4: Towards optimal assessment of plausible code solutions with plausible tests," in *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering*, 2024, pp. 1693–1705.
- [29] B. Roziere, J. Gehring, F. Gloeckle, S. Sootla, I. Gat, X. E. Tan, Y. Adi, J. Liu, R. Sauvestre, T. Remez *et al.*, "Code llama: Open foundation models for code," *arXiv preprint arXiv:2308.12950*, 2023.
- [30] M. Chen, H. Tian, Z. Liu, X. Ren, and J. Sun, "Jumpcoder: Go beyond autoregressive coder via online modification," in *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, 2024, pp. 11 500–11 520.
- [31] "Ethereum.org: The complete guide to Ethereum," <https://ethereum.org/en/>.
- [32] T. E. Ajibola, O. T. Adeniran, and P. Taiwo, "Smartpattern: A machine learning framework for detecting reentrancy vulnerabilities in blockchain smart contracts," in *2025 59th Annual Conference on Information Sciences and Systems (CISS)*, 2025, pp. 1–6.
- [33] J. Zhang, J. Chen, J. Grundy, J. Gao, Y. Wang, T. Chen, Z. Guan, and Z. Chen, "Automated test generation for smart contracts via on-chain test case augmentation and migration," in *2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE)*, 2025, pp. 633–633.
- [34] "SimHash," Wikipedia, Nov. 2024.
- [35] J. Feist, G. Grieco, and A. Groce, "Slither: a static analysis framework for smart contracts," in *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, 2019, pp. 8–15.
- [36] "Hardhat | Ethereum development environment for professionals by Nomic Foundation," <https://hardhat.org>.
- [37] S. Quan, J. Yang, B. Yu, B. Zheng, D. Liu, A. Yang, X. Ren, B. Gao, Y. Miao, Y. Feng *et al.*, "Codeelo: Benchmarking competition-level code generation of llms with human-comparable elo ratings," *arXiv preprint arXiv:2501.01257*, 2025.
- [38] X. Li, W. Chen, Q. Chu, H. Li, Z. Sun, R. Li, C. Qian, Y. Wei, C. Shi, Z. Liu *et al.*, "Can large language models analyze graphs like professionals? a benchmark, datasets and models," *Advances in Neural Information Processing Systems*, vol. 37, pp. 141 045–141 070, 2024.
- [39] Google, "Gemini 2.0 flash," 2024, <https://ai.google.dev/gemini-api/docs/models/gemini-v2?hl=zh-cn>.
- [40] X. Du, M. Liu, K. Wang, H. Wang, J. Liu, Y. Chen, J. Feng, C. Sha, X. Peng, and Y. Lou, "Classeval: A manually-crafted benchmark for evaluating llms on class-level code generation," *arXiv preprint arXiv:2308.01861*, 2023.
- [41] H. Yu, B. Shen, D. Ran, J. Zhang, Q. Zhang, Y. Ma, G. Liang, Y. Li, Q. Wang, and T. Xie, "Codereval: A benchmark of pragmatic code generation with generative pre-trained models," in *Proceedings of the 46th IEEE/ACM International Conference on Software Engineering*, 2024, pp. 1–12.
- [42] "Introducing ChatGPT," <https://openai.com/index/chatgpt/>, Mar. 2024.
- [43] K. M. Lewis and P. Hepburn, "Open card sorting and factor analysis: a usability case study," *The electronic library*, vol. 28, no. 3, pp. 401–416, 2010.
- [44] "Gemini API : The recitation problem is annoying · Issue #257 · google/generative-ai-docs," <https://github.com/google/generative-ai-docs/issues/257>.
- [45] J. Austin, A. Odena, M. Nye, M. Bosma, H. Michalewski, D. Dohan, E. Jiang, C. Cai, M. Terry, Q. Le *et al.*, "Program synthesis with large language models," *arXiv preprint arXiv:2108.07732*, 2021.
- [46] L. Deng, Z. Jiang, J. Cao, M. Pradel, and Z. Liu, "Nocode-bench: A benchmark for evaluating natural language-driven feature addition," *arXiv preprint arXiv:2507.18130*, 2025.
- [47] N. O. O. Dade, M. Lartey-Quaye, E. T.-K. Odonkor, and P. Ammah, "Optimizing large language models to expedite the development of smart contracts," *arXiv preprint arXiv:2310.05178*, 2023.
- [48] H. Zhang, Q. Zhang, Z. Wang, H. Zheng, J. Dong, Z. Zheng *et al.*, "Codebc: A more secure large language model for smart contract code generation in blockchain," *arXiv preprint arXiv:2504.21043*, 2025.
- [49] E. A. Napoli, F. Barbàra, V. Gatteschi, and C. Schifanella, "Leveraging large language models for automatic smart contract generation," in *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2024, pp. 701–710.