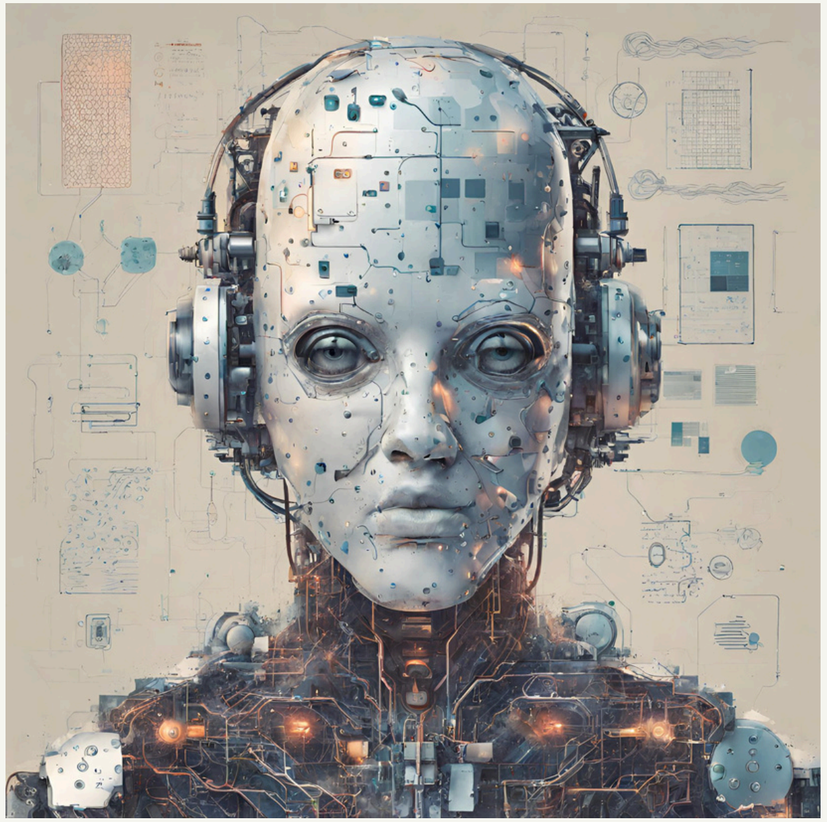
Teaching AI's to reason and code, confidentially



A proposal defense presentation by
Rabimba Karanjai

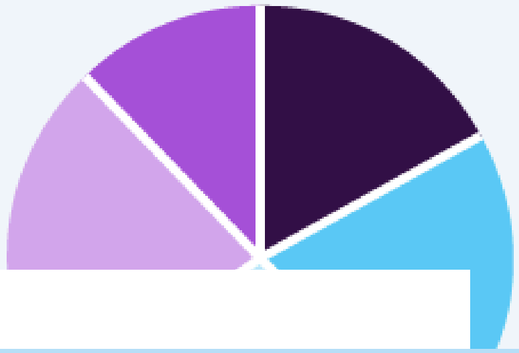
Advisor: Dr. Weidong Shi

U.S. Large Language Model Market

Size, by Application, 2020 - 2030 (USD Million)

Global Large Language Model Market

Share, by Industry Vertical, 2023 (%)



GRAND VIEW RESEARCH

$4.3B

Global Market Size, 2023

COPILOT!!!

Genreate code

generate code snippets & autocomplete

Code l

Documentation

descriptive comments and explanations for code blocks

Optimize

assist in debuggi
errors as well
alterna

AUGUST 2020

GLOBAL STATISTICS

Market Size (2022)	CAGR (2023-2032)	Market Size (2032)
$4.1 BN	>22%	$29.1 BN

SEGMENT STATISTICS

Cloud Segment Market Share (2022)	70%
BFSI Segment Market Share (2022)	24%

REGIONAL STATISTICS

North America

Market Share (2022)

>37%

AI CODE TOOLS MARKET

Global Market Insights

Introduction

PART 01

Research Problem

WHAT I WANT TO SOLVE

- Safety: How can I ensure that LLMs generate code that is free of vulnerabilities and adheres
- to security best practices?.
- Robustness: How can I enhance the resilience of LLMs to adversarial attacks, input pertur-
- Reasoning: How can I improve the ability of LLMs to understand, explain, and justify their code generation decisions?.

Thesis Statement

WHAT I WANT TO PROVE / DISPROVE

- LLMs for Smart Contract Generation
- Can we translate code using LLMs
- Reasoning in LLM Code Generation
- Decentralized Computation for AI

Contributions

DECENTRALIZED SYSTEMS AND BLOCKCHAIN

1. IEEE TNSM
2. ACM SAC 24
3. IEEE ICBC 22
4. Middleware 22

→

ARTIFICIAL INTELLIGENCE AND LLMS

1. CHI (HEAL) 24
2. ICEDEG

→

SMART CONTRACTS AND AI SAFETY

1. BRAINS
2. IEEE ICBC

Smart Contract Generation

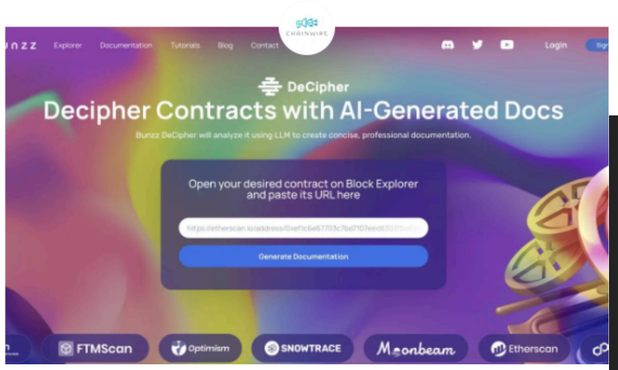
PART 02

Web3×LLM On-Chain Contract Analysis Tool "DeCipher" Sparks Excitement Among Developers and Researchers

Users can create documents from nearly all Smart Contracts existing on each Blockchain with a single click.

By Chainwire

Aug 6, 2023 • 3 min read



CoinDesk

AI Safety for Smart Contracts Is AI Safety for the World

Opinion

AI Safety for Smart Contracts Is AI Safety for the World

Web3 infrastructure can bring new safety and reliability tools to AI, a cycle that will make the intersection of AI and Web3 massively and mutually beneficial, Chainlink scientist Ari Juels and Google AI lead Laurence Moroney write.

By Ari Juels, Laurence Moroney Apr 23, 2024 at 12:04 p.m. CDT

Updated Apr 23, 2024 at 12:07 p.m. CDT CONSENSUS MAGAZINE

Smart Contract Generation

CAN WE USE AI TO GENERATE SMART CONTRACTS?

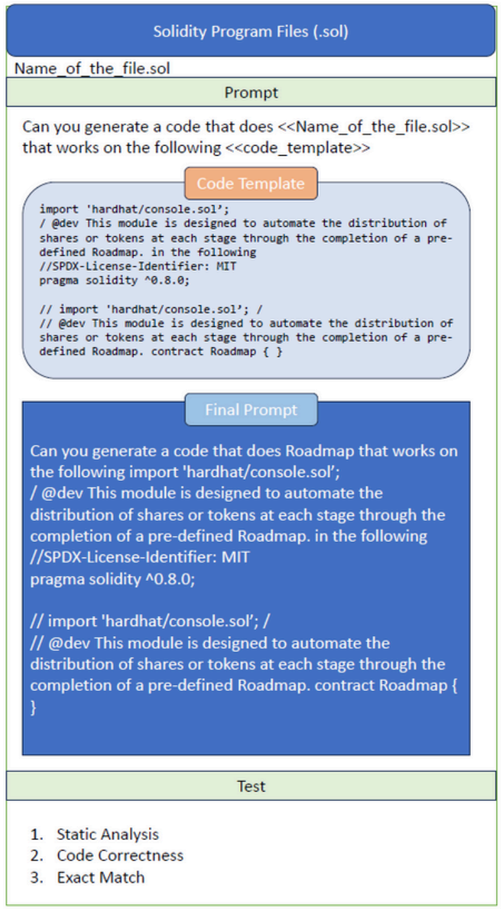
- **RQ1:** What is the quality of the code generated by state of the art LLMs
- **RQ2**: Can I create a system that takes a source smart contract and translates it to a target smart contract in a low resource language and with safety guarantees?

Smart Contract Generation

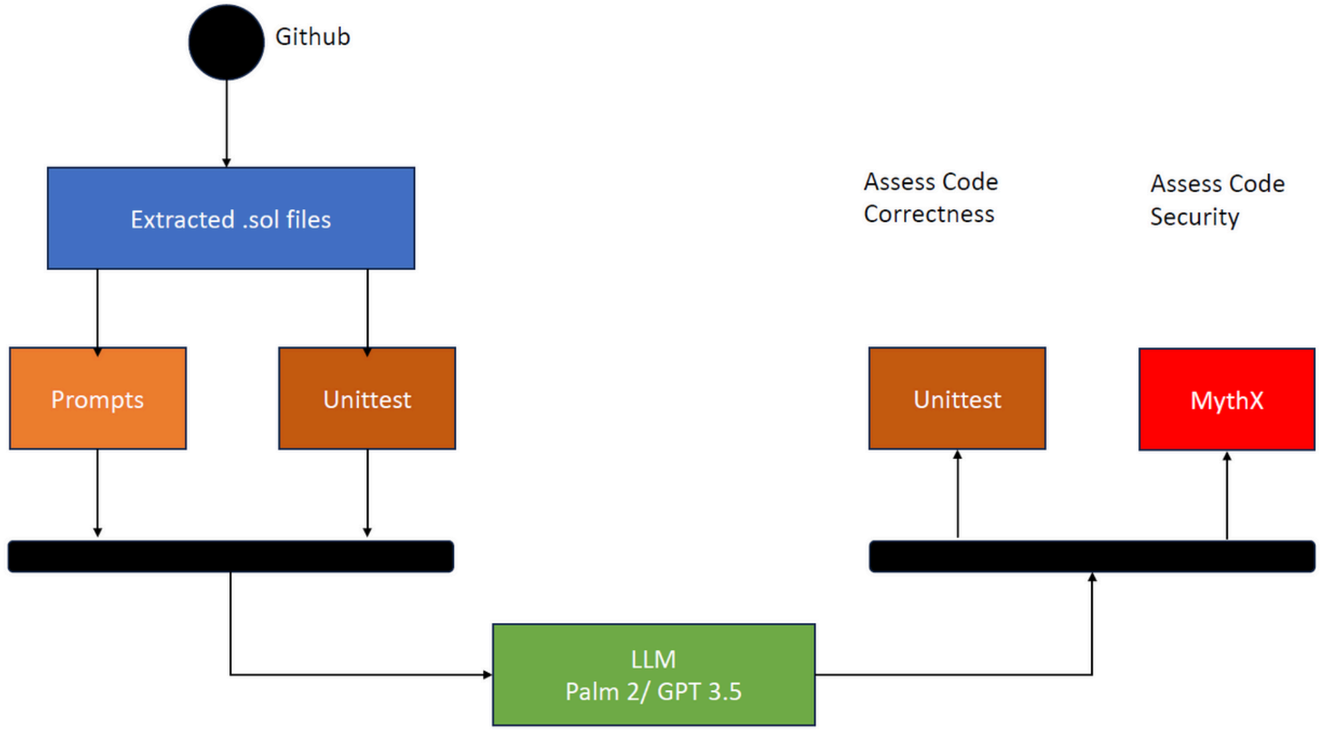
CAN WE USE AI TO GENERATE SMART CONTRACTS?

- **RQ1:** What is the quality of the code generated by state of the art LLMs
- **RQ2**: Can I create a system that takes a source smart contract and translates it to a target smart contract in a low resource language and with safety guarantees?

RQ1



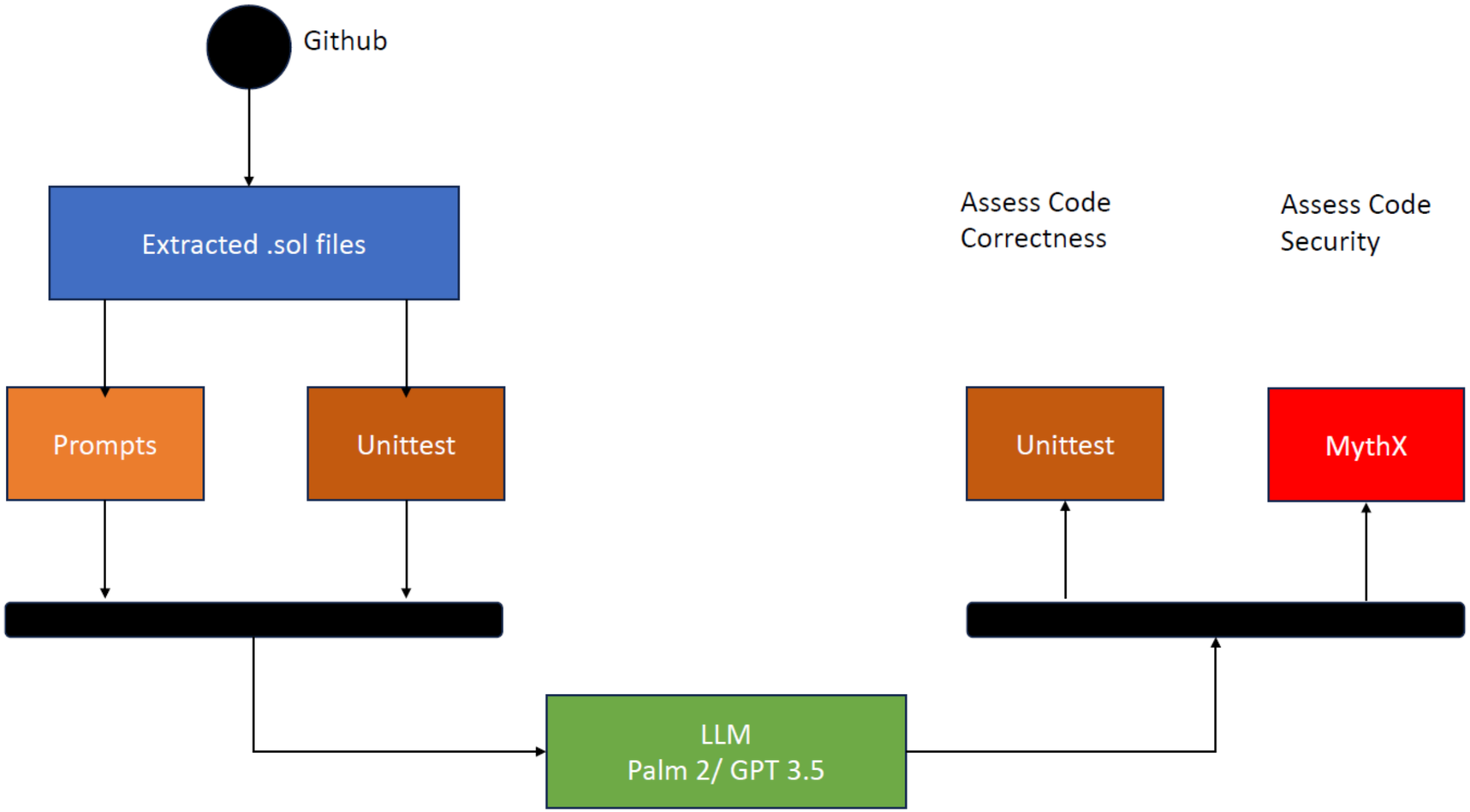
Prompt generation example



A step-by-step illustration of the experiment's workflow

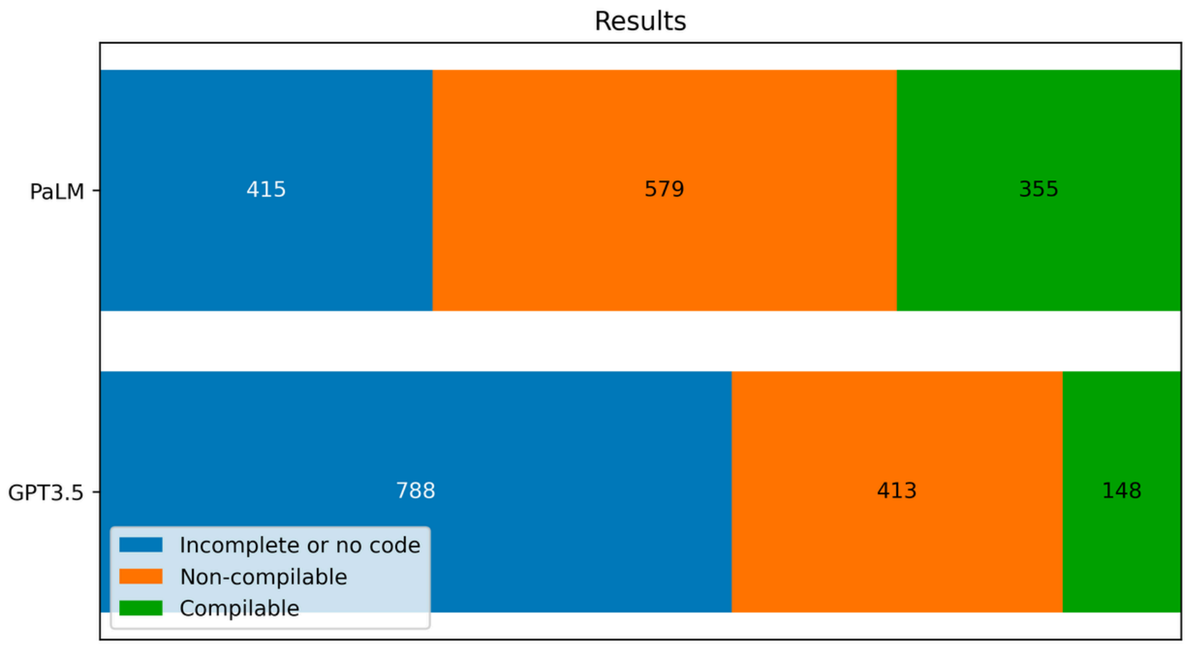
Karanjai, Rabimba, et al. "Who is Smarter? An Empirical Study of AI-Based Smart Contract Creation." 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, 2023.

RQ1

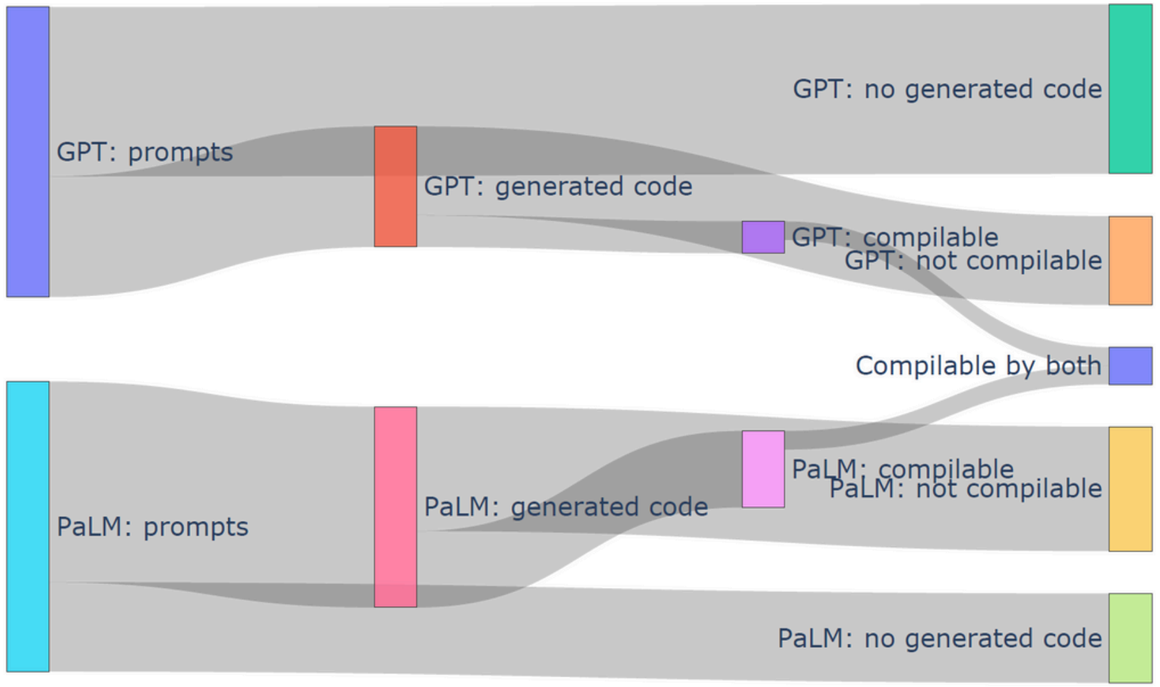


Karanjai, Rabimba, et al. "Who is Smarter? An Empirical Study of AI-Based Smart Contract Creation." 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, 2023.

RQ1



Code compile statistics



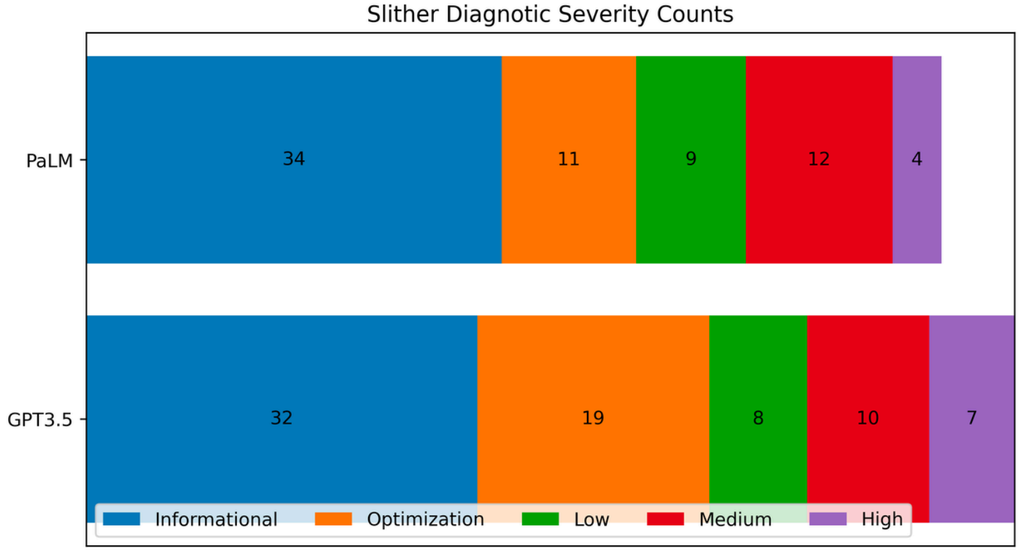
Division of different generated codes based on their correctness

Karanjai, Rabimba, et al. "Who is Smarter? An Empirical Study of AI-Based Smart Contract Creation." 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, 2023.

RQ1

Table 2: Bugs found by Slither

Severity	Lint	GPT3.5	PaLM2
Informational	dead-code	24	27
	similar-names	0	2
	assembly	4	0
	reentrancy-unlimited-gas	1	0
	low-level-calls	1	1
	too-many-digits	1	1
	unused-state	1	3
Optimization	constable-states	7	7
	immutable-states	12	4
Low	reentrancy-benign	1	0
	calls-loop	1	1
	missing-zero-check	2	1
	reentrancy-events	0	1
	timestamp	3	3
	shadowing-local	1	3
Medium	erc20-interface	0	5
	incorrect-equality	5	4
	locked-ether	2	3
	tautology	3	0
High	uninitialized-state	4	0
	weak-prng	3	4



RQ1

RESEARCH QUESTION

RQ1 WHAT IS THE QUALITY OF THE CODE GENERATED BY LLMS LIKE CHATGPT AND GOOGLE PALM2?
- RQ1.1 CODE VALIDITY
- RQ1.2 CODE CORRECTNESS

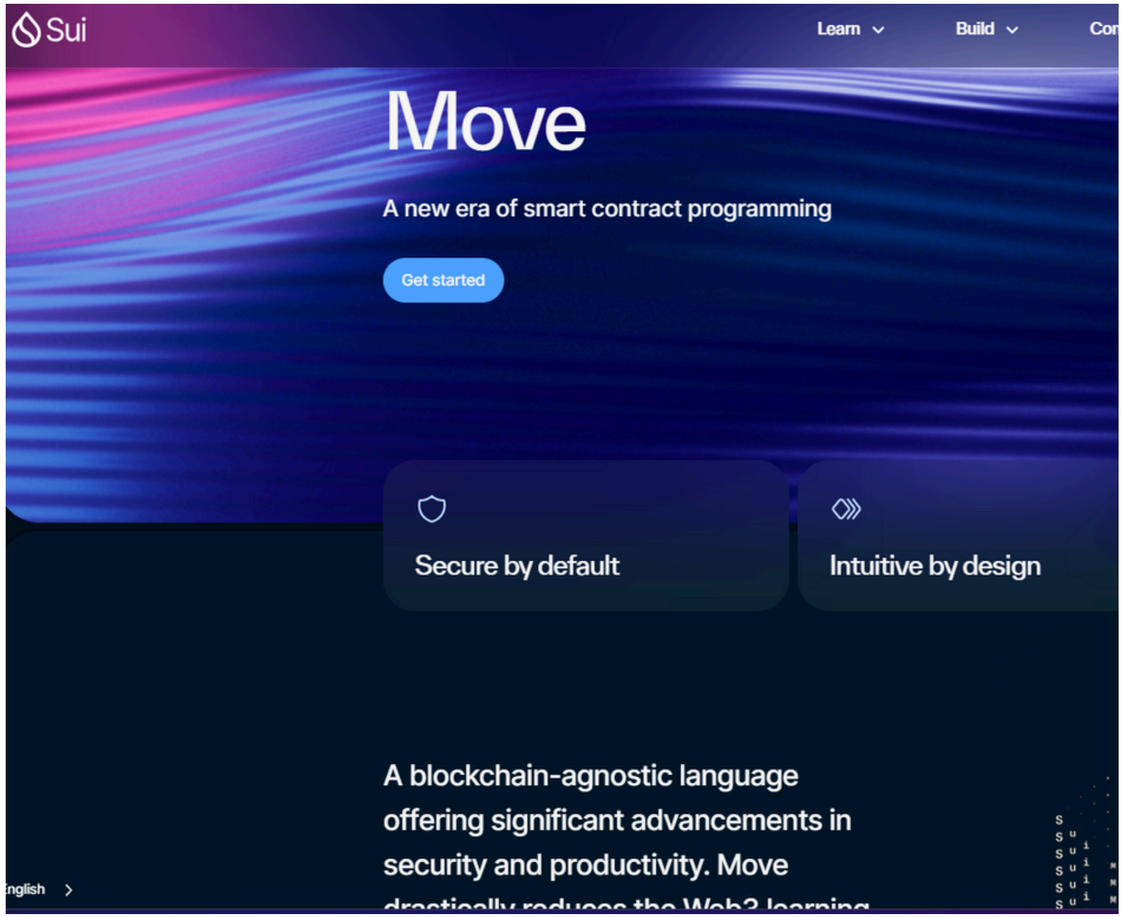
• RQ2 CAN BETTER CODE BE GENERATED USING DIFFERENT PROMPTING TECHNIQUES
• RQ3 ARE THE GENERATED CODES SECURE?

- BUGGY CODE
- LESS THAN 50% CODE COMPILABLE
- IN CONTEXT LEARNING INCREASES PERFOREMANCE, BUT NOT TOO MUCH
- HAS SECURITY ISSUES

Smart Contract Generation

CAN WE USE AI TO GENERATE SMART CONTRACTS?

- **RQ1:** What is the quality of the code generated by state of the art LLMs
- **RQ2**: Can I create a system that takes a source smart contract and translates it to a target smart contract in a low resource language and with safety guarantees?



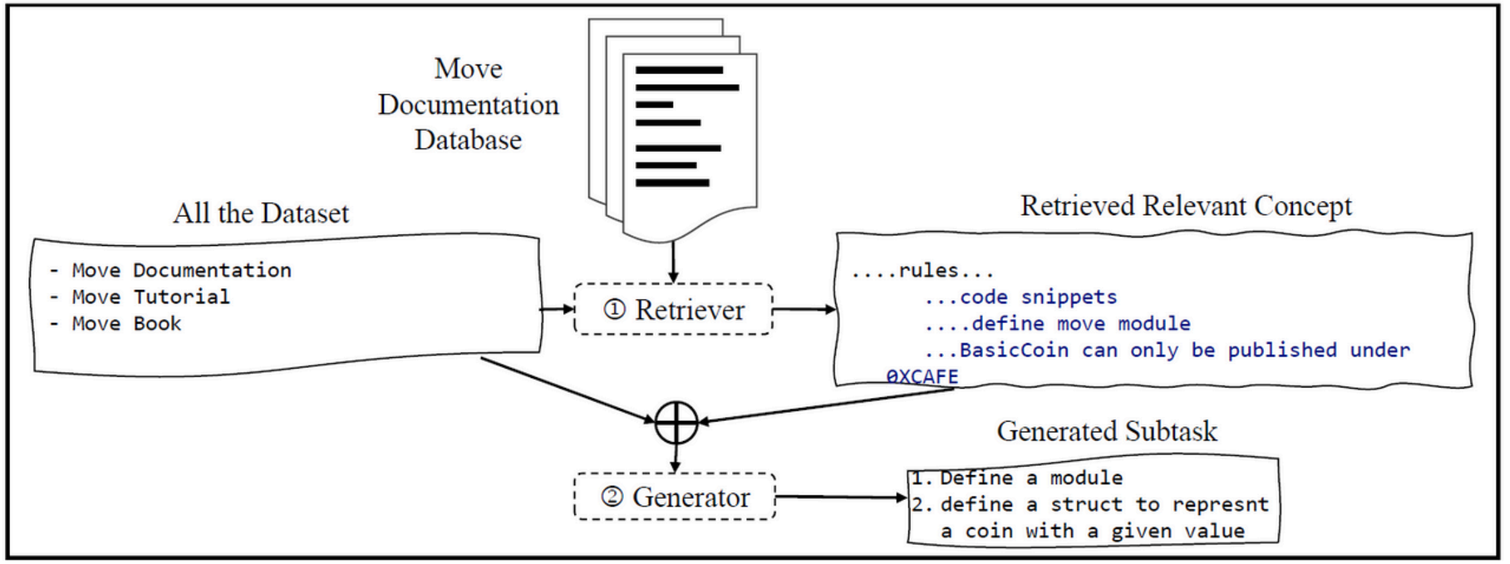
Resources: A Safe Language Abstraction for Money

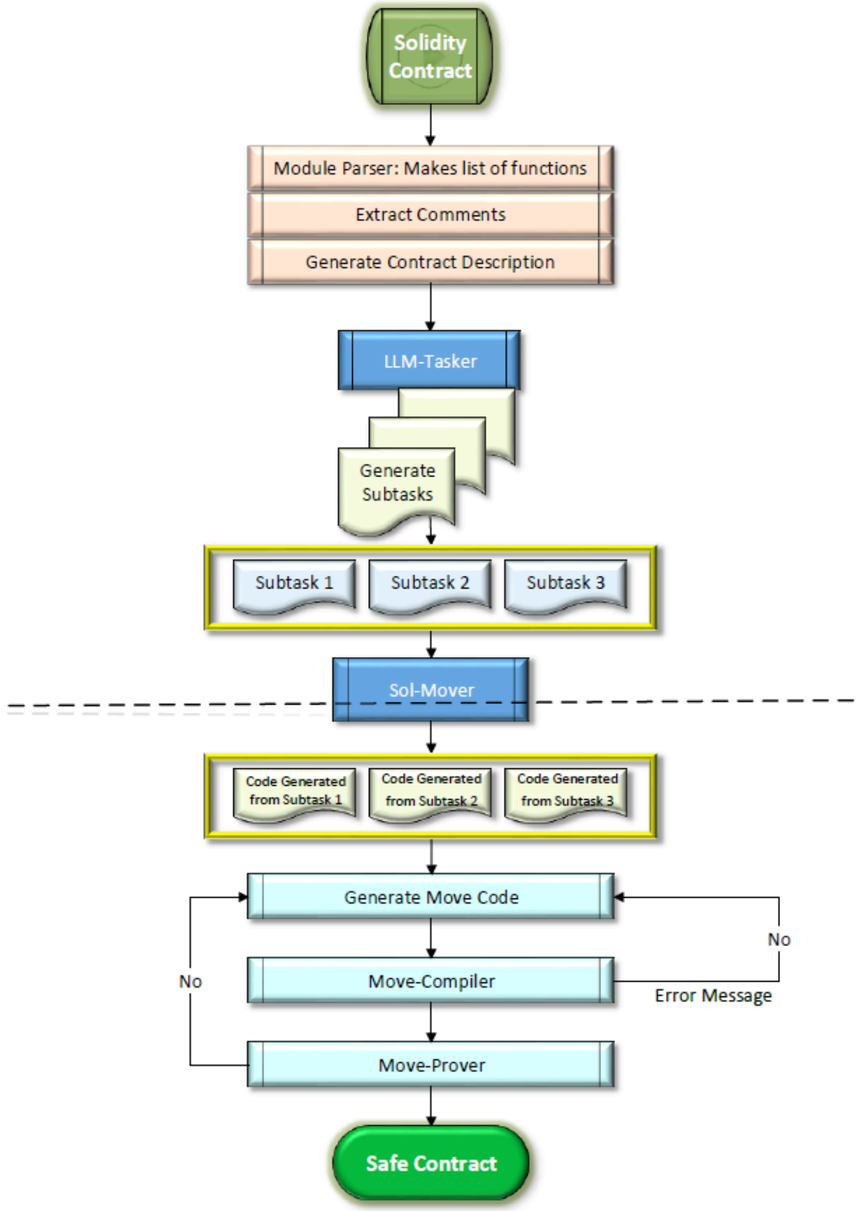
SAM BLACKSHEAR, Novi
DAVID L. DILL, Novi
SHAZ QADEER, Novi
CLARK W. BARRETT, Stanford University
JOHN C. MITCHELL, Stanford University
ODED PADON, Stanford University
YONI ZOHAR, Stanford University

Smart contracts are programs that implement potentially sophisticated transactions on modern blockchain platforms. In the rapidly evolving blockchain environment, smart contract programming languages must allow users to write expressive programs that manage and transfer assets, yet provide strong protection against sophisticated attacks. Addressing this need, we present flexible and reliable abstractions for programming with digital currency in the Move language [Blackshear et al. 2019]. Move uses novel linear [Girard 1987] *resource* types with semantics drawing on C++11 [Stroustrup 2013] and Rust [Matsakis and Klock 2014]: when a resource value is assigned to a new memory location, the location previously holding it must be invalidated. In addition, a resource type can only be created or destroyed by procedures inside its declaring module. We present an executable bytecode language with resources and prove that it enjoys *resource safety*, a conservation property for program values that is analogous to conservation of mass in the physical world.

Blackshear, Sam, et al. "Resources: A safe language abstraction for money." arXiv preprint arXiv:2004.05106 (2020).

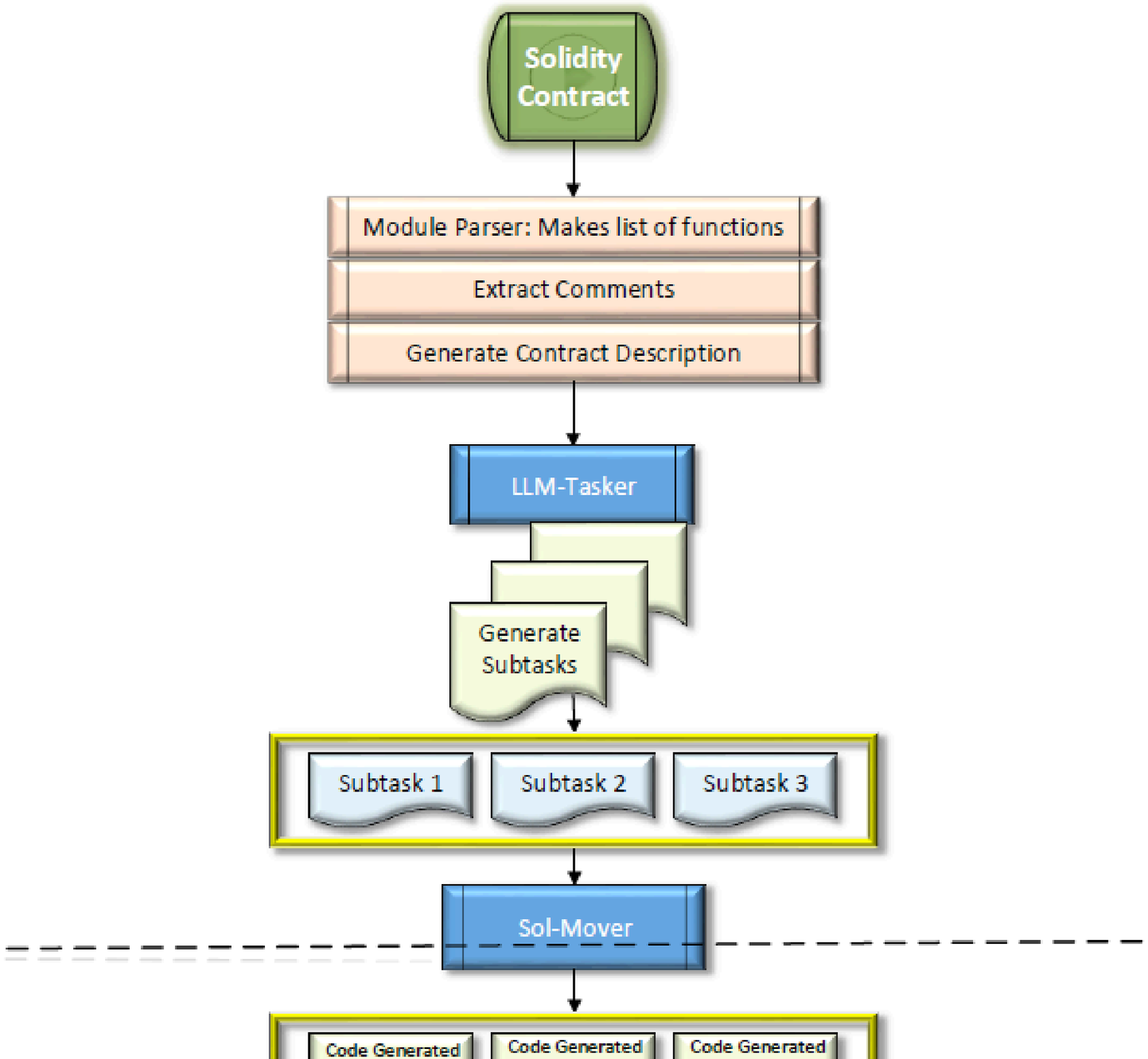
RQ2



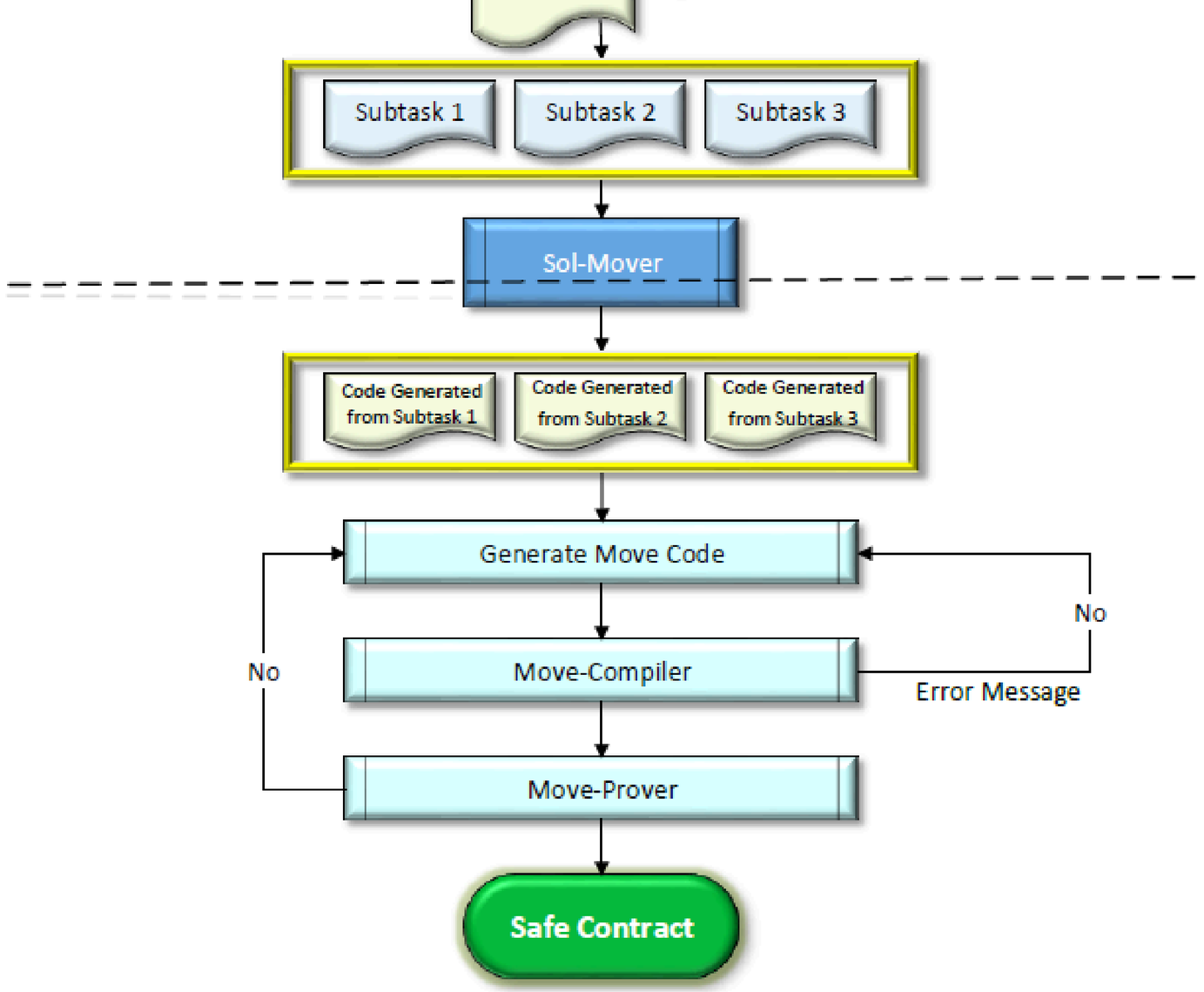


Karanjai, Rabimba, et al. "SolMover: Feasibility of using LLMs for Translating Smart Contracts" 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2024.

RQ2


Solidity Contract
Module Parser: Makes list of functions
Extract Comments
Generate Contract Description
LLM-Tasker
Generate Subtasks
Subtask 1
Subtask 2
Subtask 3
Sol-Mover
Code Generated
Code Generated
Code Generated

RQ2


Subtask 1
Subtask 2
Subtask 3
Sol-Mover
Code Generated from Subtask 1
Code Generated from Subtask 2
Code Generated from Subtask 3
Generate Move Code
Move-Compiler
Move-Prover
Safe Contract
No
Error Message
No

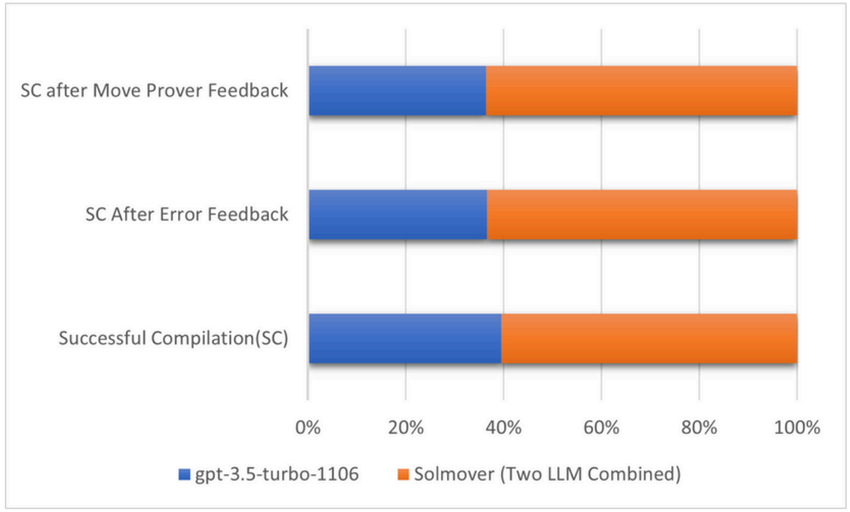
RQ2

LLMs	Compilable Code?	Performance
gpt-3.5-turbo-1106	Y	Mixed
Solmover (Two LLM Combined)	Y	Mixed
Mixtral-8x7B-Instruct	N	Mixes different languages and generate unusable code
LLama2	N	Mixes different languages and generate unusable code
Palm2	N	For Move only generates code snippets and plan

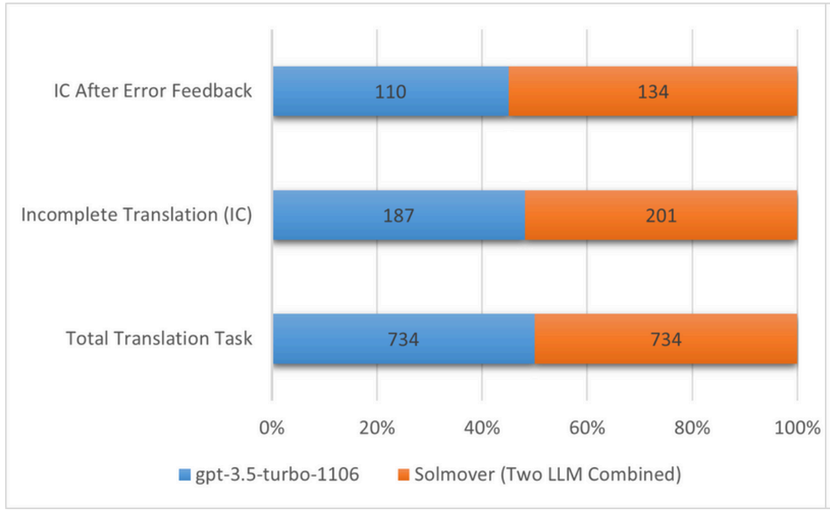
Table 1: Code Translation Capability of Four LLMs.

LLM	Total Translation Task	Successful Compilation(SC)	SC After Error Feedback	SC after Move Prover Feedback
gpt-3.5-turbo-1106	734	204	229	229
Solmover (Two LLM Combined)	734	313	397	401

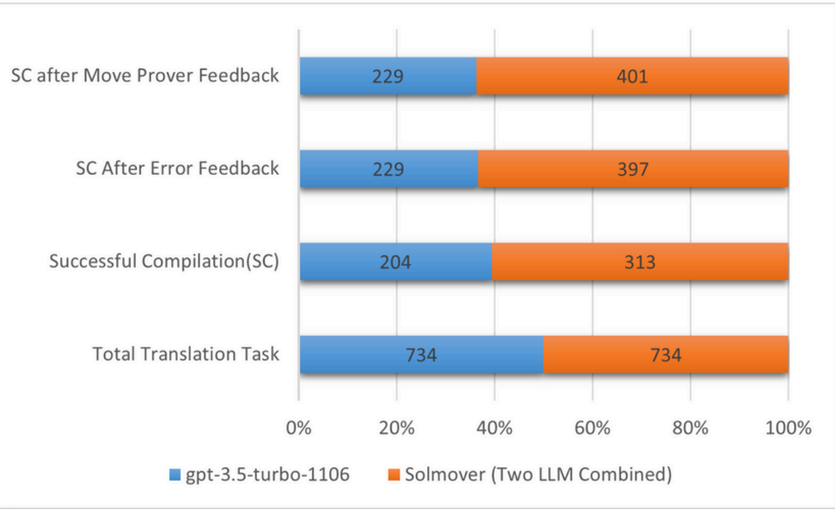
Table 2: Successful Translations.



Successful Translations

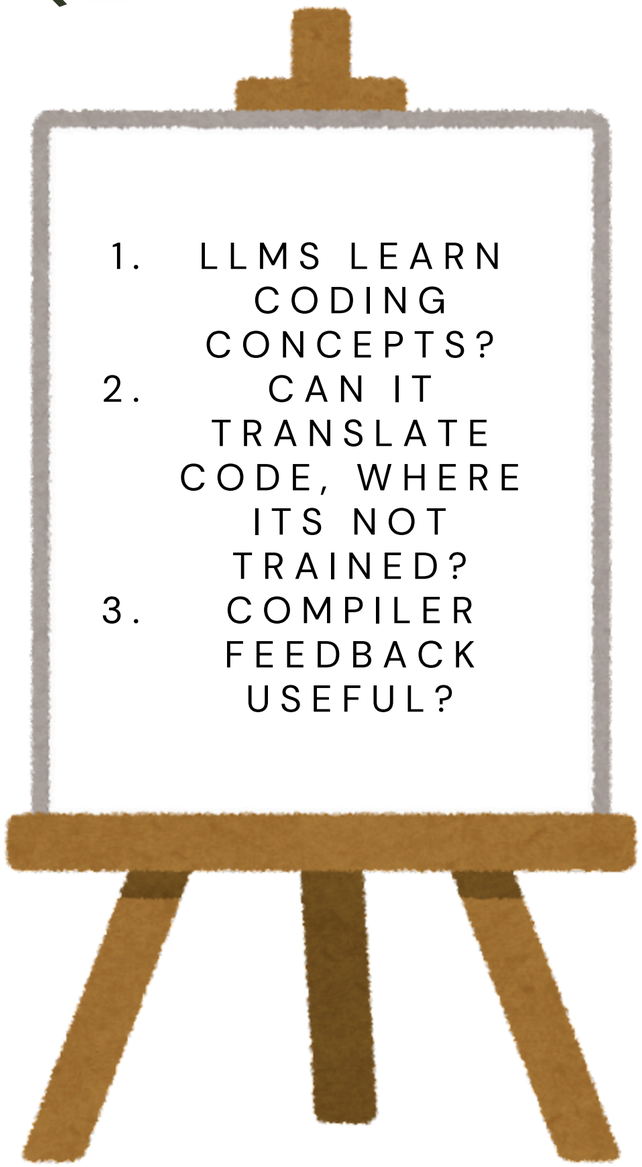


Bug Mitigation



Contract Correctness

RQ2



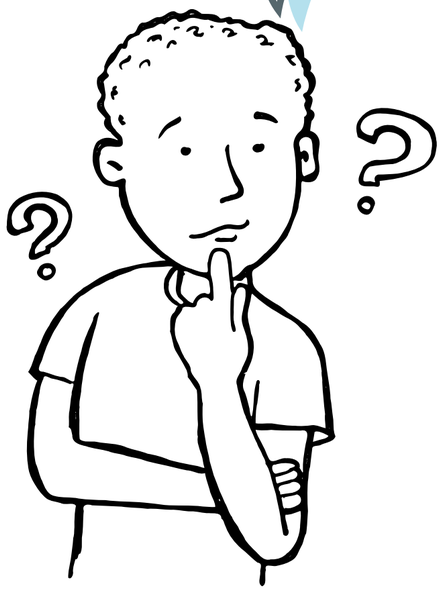
1. LLMS ARE CAPABLE OF ENCODING ASSOCIATIONS THAT **RESEMBLE** CONCEPTS
2. YES. TO SOME DEGREE
3. YES.

Submitted Work

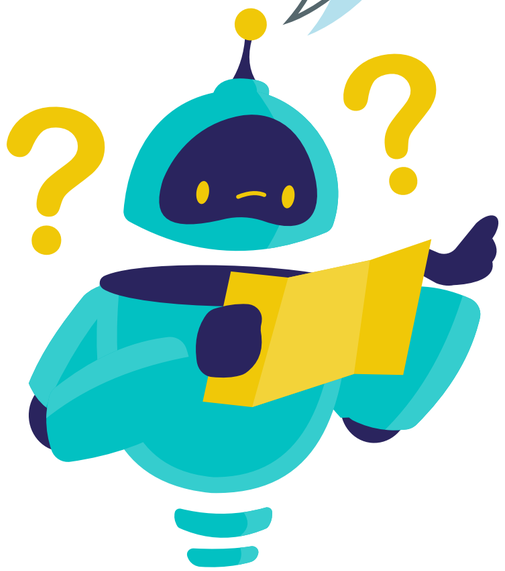
PART 03

Can we understand and generate unit tests for High Performance Computing code libraries?

ICPP 2024



What about security of those codes?



- Can we teach AI world planning?
- Can those reasoning be transferred to coding?

AIWare 2024

Future Work

PART 04

Future Work Timeline

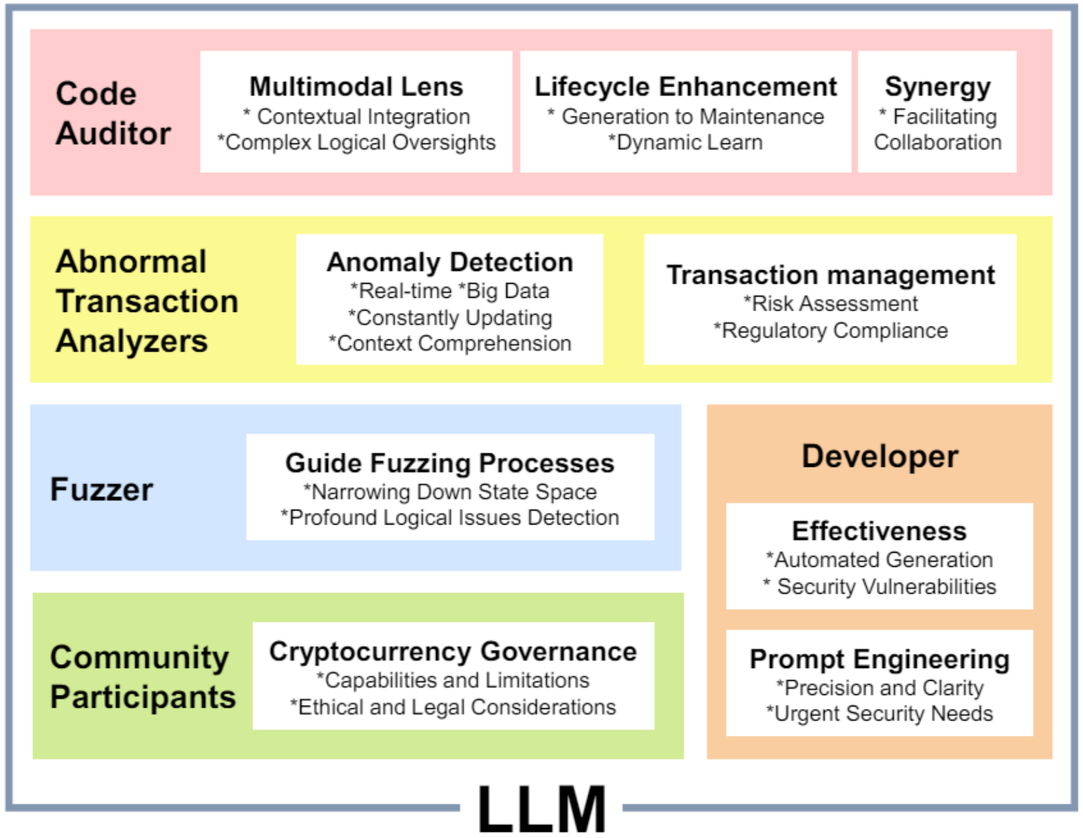
- SolMover Improvement
- MoveGen Work Start
- Comprehensive Work on Low Resource code augmentation

April - June

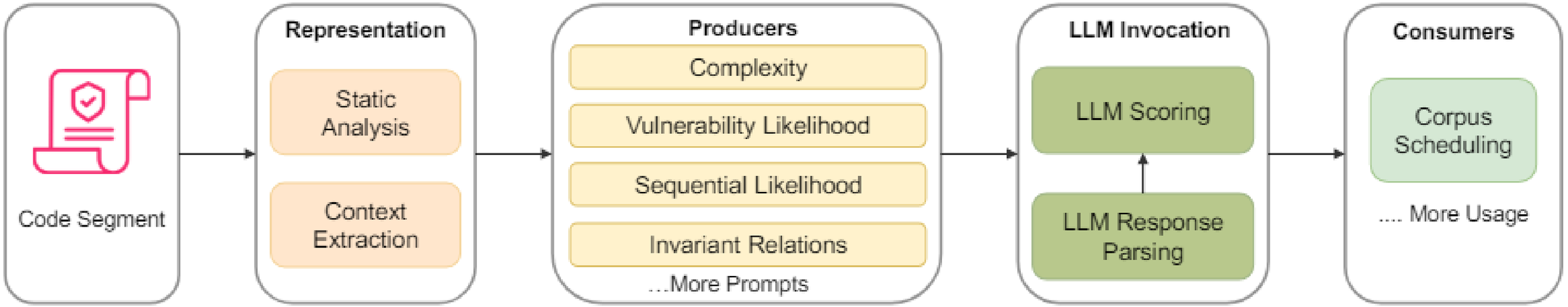
- Work on extending SolMover to support compiler guided code correction
- Start working on direct generation of low resource code (Move)

Can we generate
automated fuzzing
for smart contract?

WIP: Automated Smart Contract Fuzzing



WIP: Automated Smart Contract Fuzzing



Future Work Timeline

APRIL – JUNE

- SolMover Improvement
- MoveGen Work Start
- Comprehensive Work on Low Resource code augmentation

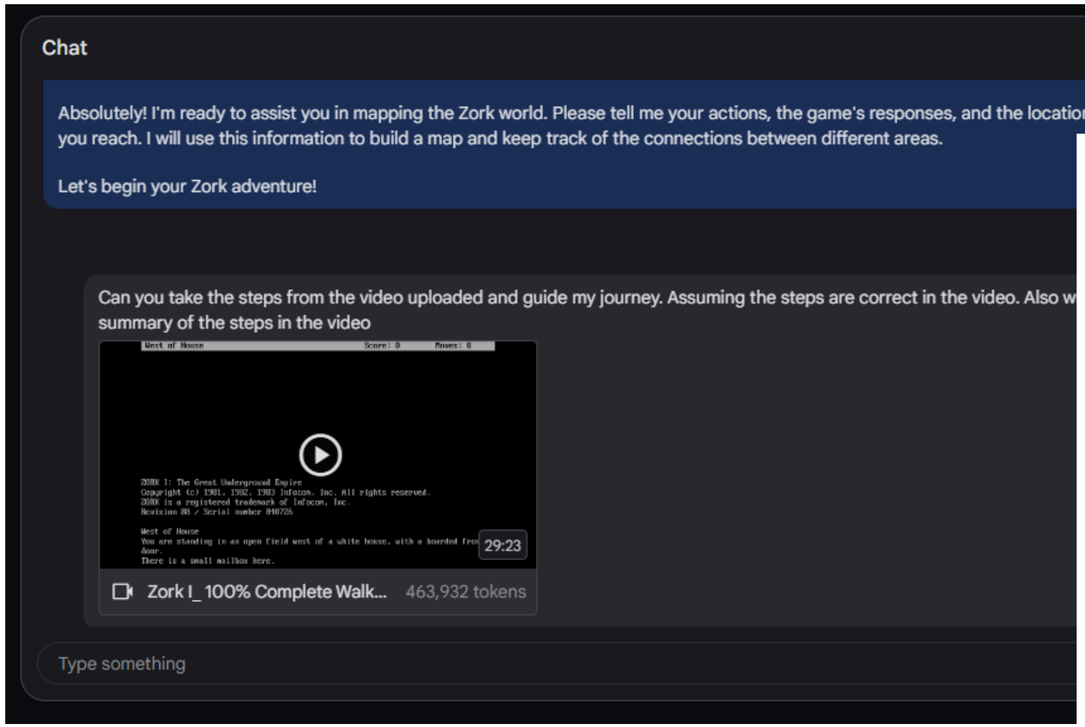
JULY – SEPTEMBER

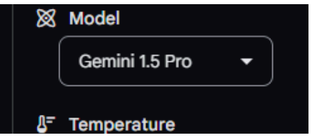
- Submit paper for the improved SolMover extended work
- Work on publishing HPC Code Exploration paper
- Work on attacking LLMs with randomness
- Finish email phishing work

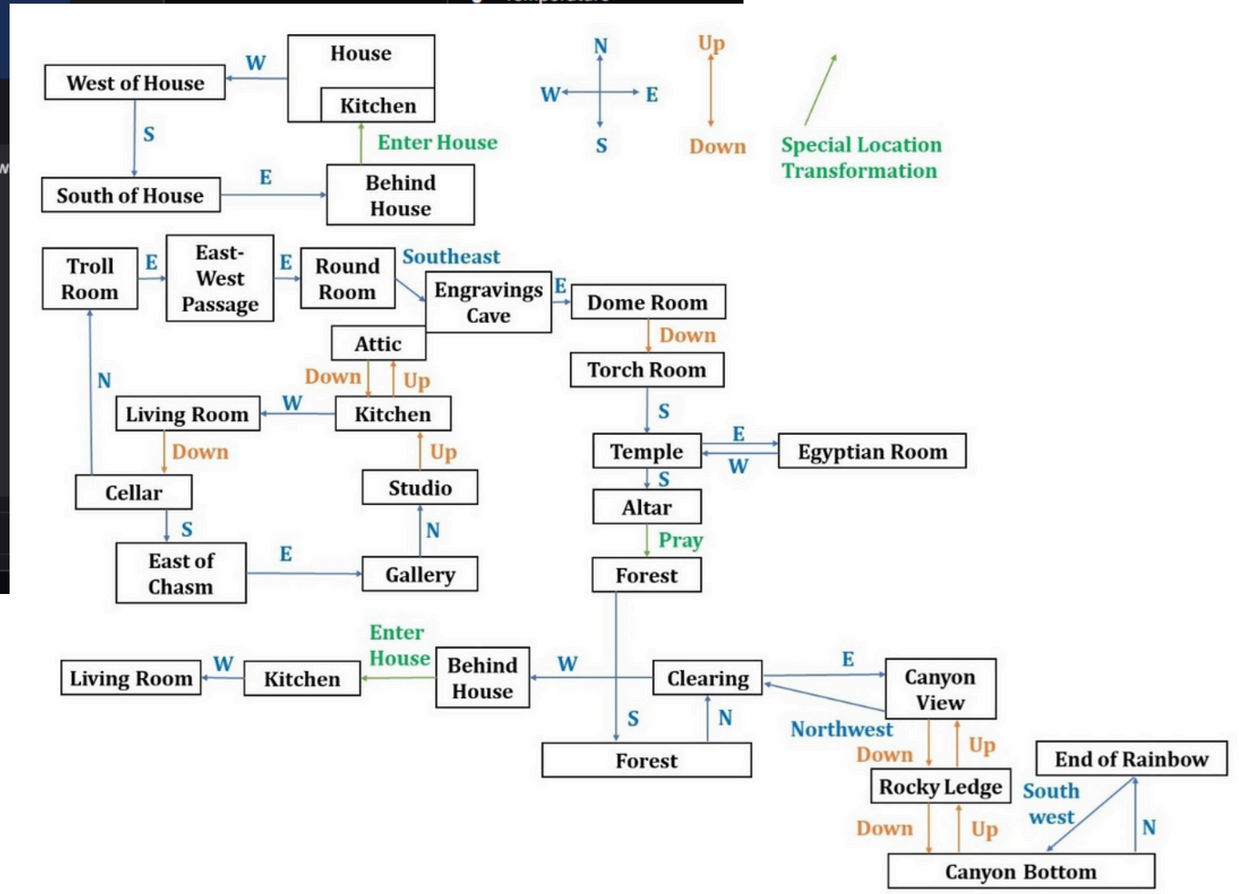
OCTOBER–DECEMBER

EARLY 2025

WIP: World Planning from Multimodal Data







Future Work Timeline

APRIL - JUNE

- SolMover Improvement
- MoveGen Work Start
- Comprehensive Work on Low Resource code augmentation

JULY - SEPTEMBER

- Submit paper for the improved SolMover extended work
- Work on publishing HPC Code Exploration paper
- Work on attacking LLMs with randomness
- Finish email phishing work

OCTOBER-DECEMBER

- Train and evaluate multilingual AI models for both high-resource and low-resource languages
- Begin investigating techniques for enhancing AI reasoning and explainability.

EARLY 2025

- Work on Dissertation
- Work on CV for Job

Conclusion

PART 05

Selected Contributions

DECENTRALIZATION

- Re-Imagining Decentralized Infrastructure As Code using Blockchain (IEEE TNSM'23)
- Decentralized Translator of Trust: Supporting Heterogeneous TEE for Critical Infrastructure Protection (ACM BSCI'23)
- Decentralized FaaS over Multi-Clouds with Blockchain based Management for Supporting Emerging Applications (ACM SAC'24)
- Decentralized Application Infrastructures as Smart Contract Codes (IEEE ICBC'22)
- Privacy preserving event based transaction system in a decentralized environment (ACM MIddleware'22)

AI

- SolMover: Feasibility of using LLMs for Translating Smart Contracts (IEEE ICBC'24)
- Who is Smarter? An Empirical Study of AI-based Smart Contract Creation (BRAINS'23)
- Comparing Rationality Between Large Language Models and Humans: Insights and Open Questions (CHI'24)
- All We Need is Voter Feedback (ICEDEG'24)

Implications of the research

AI SAFETY AND ROBUSTNESS FOR SMART CONTRACTS

Areas of improvement

- REASONING
- CODE CORRECTNESS
- CONFIDNETIAL COMPUTE
- DECENTRALIZED COMPUTE

Thank You!

April 2024