

# 语言特性分析指导的智能合约测试 科研进展情况

2021/12/18

王子彦

[ziyan-wang.github.io](https://ziyan-wang.github.io)

中山大学计算机学院

InPlusLab



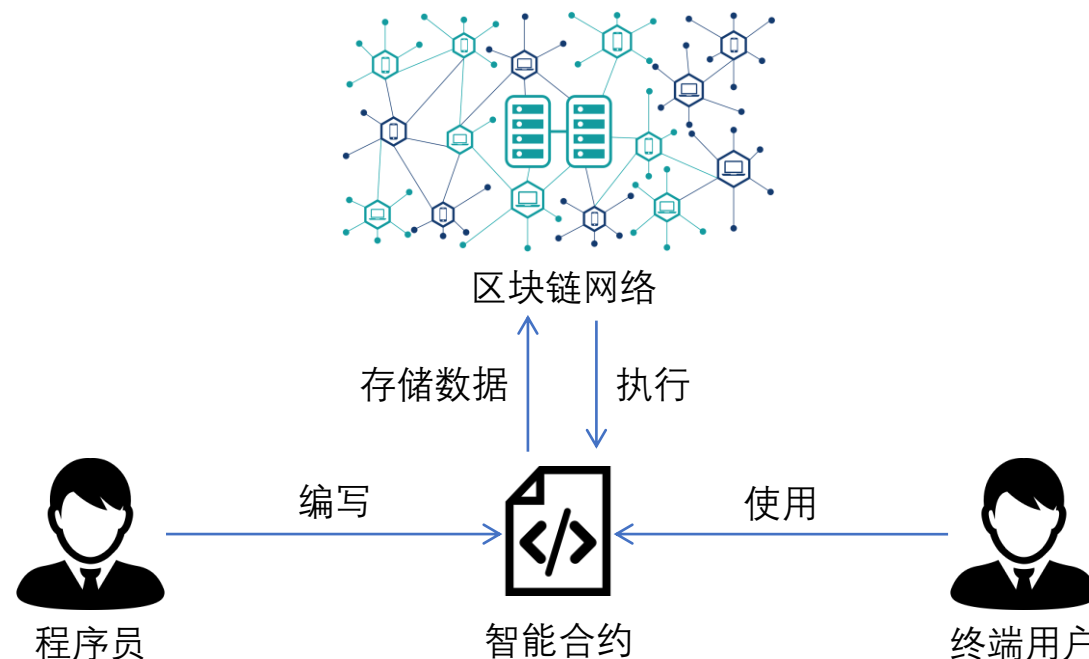
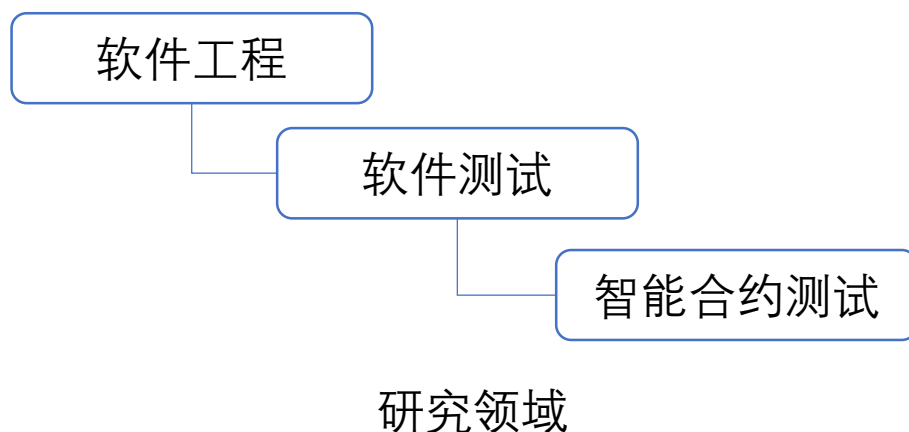


# 一、研究问题背景与难点



## ■ 智能合约测试

- 以太坊是一个支持编写图灵完备智能合约的区块链平台，开发者主要使用Solidity编程语言
- 智能合约测试困难，因为其运行环境较复杂，难以在测试环境复现线上的环境
- 如果需要复现线上的环境，则需要依次重放公链上的所有交易，因此有必要设计一个交易重放方法来辅助测试





## 二、国内外研究现状

- 2019年, Hartel等人<sup>1</sup>提出了一个基于Truffle的智能合约历史交易重放脚本生成方法, 但该方法不能保证测试环境和线上环境一致
- 2021年, Kim等人<sup>2</sup>设计了一个离线、高效的智能合约执行环境, 用于合约测试和性能评估, 可保证测试环境和线上一致
- 虽然现有的智能合约交易重放方法可以用于测试环境的构建, 但尚无方法能适用于智能合约合约Gas优化的测试场景

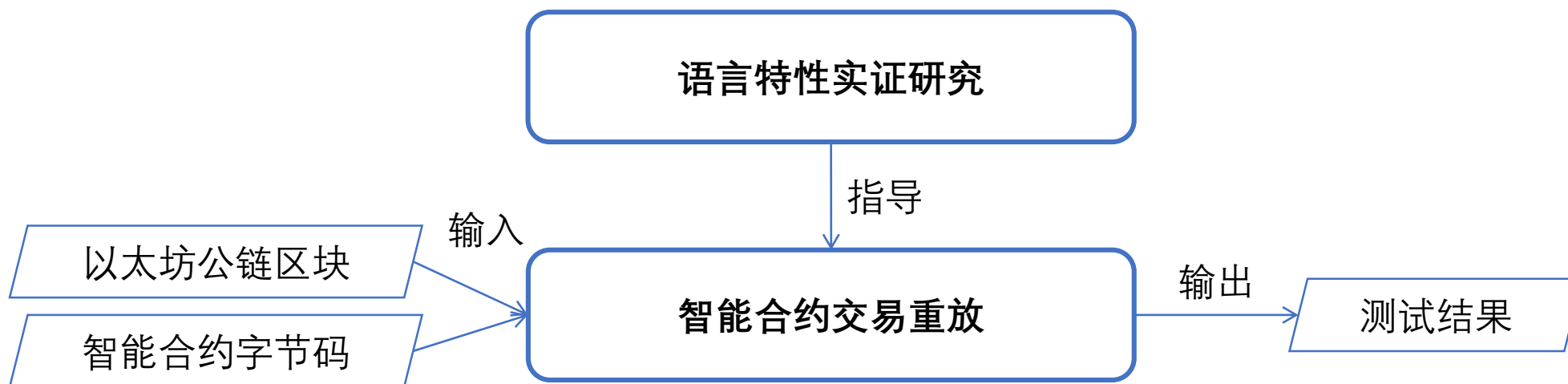
---

<sup>1</sup> Pieter Hartel, & Mark van Staalduinen. (2019). Truffle tests for free – Replaying Ethereum smart contracts for transparency.

<sup>2</sup> Yeonsoo Kim, Seongho Jeong, Kamil Jezek, Bernd Burgstaller, & Bernhard Scholz (2021). An Off-The-Chain Execution Environment for Scalable Testing and Profiling of Smart Contracts. In 2021 USENIX Annual Technical Conference (USENIX ATC 21) (pp. 565–579). USENIX Association.



### 三、创新点和个人主要工作





# 三、创新点和个人主要工作

## ■ Solidity语言特性实证研究 SolEngine

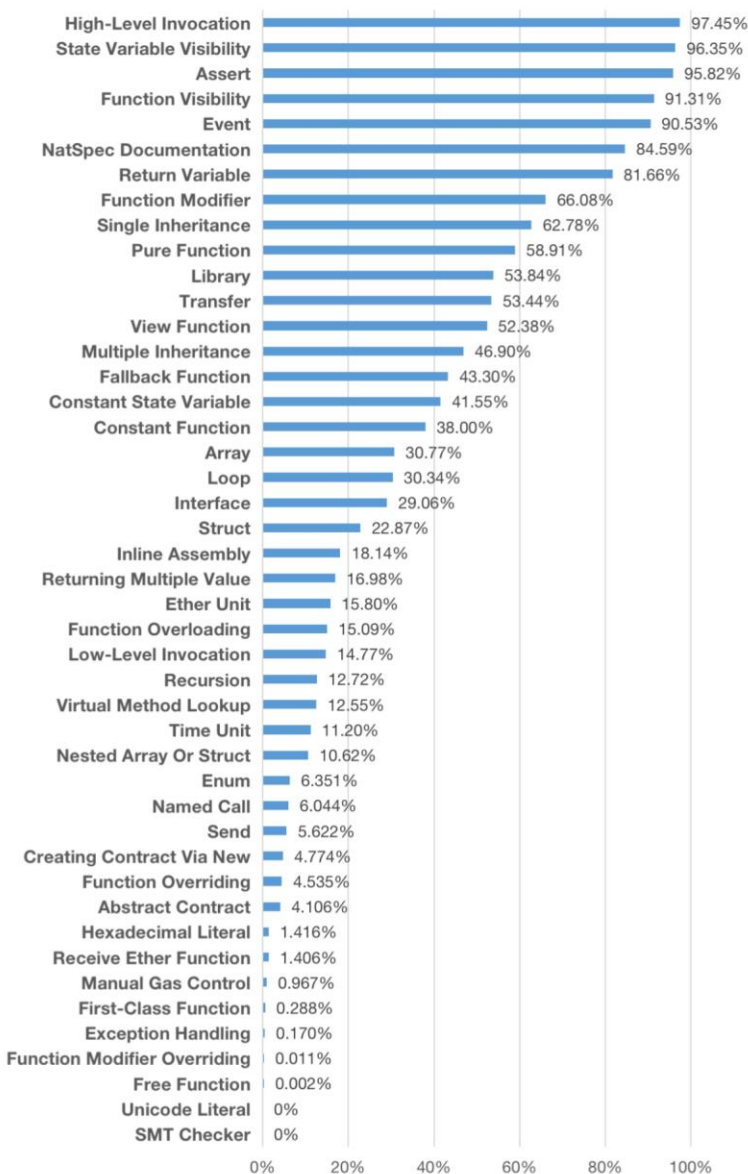
- 编程语言方面，开展了第一个Solidity语言特性的实证研究，总结了6大类41种特性，并设计了一个可扩展的静态特性分析工具，自动、高效地分析41种特性在>17万个开源合约中的分布，然后人工找出特性的使用模式和这些模式造成的bug，并给Solidity社区中的不同群体提供针对性的建议

## ■ 智能合约交易重放方法 EthReplayer

- 运行环境方面，设计了一个智能合约交易重放方法，通过动态替换智能合约的字节码、并监测环境信息来测试合约的正确性，用于多种测试场景，包括Gas优化效果评估、ERC20合约测试等，是第一个支持Gas优化测试场景的方法
- 对于实证研究中发现的容易导致bug的语言特性，使用了这些特性的合约，可使用此方法进行测试



# 四、部分实验结果

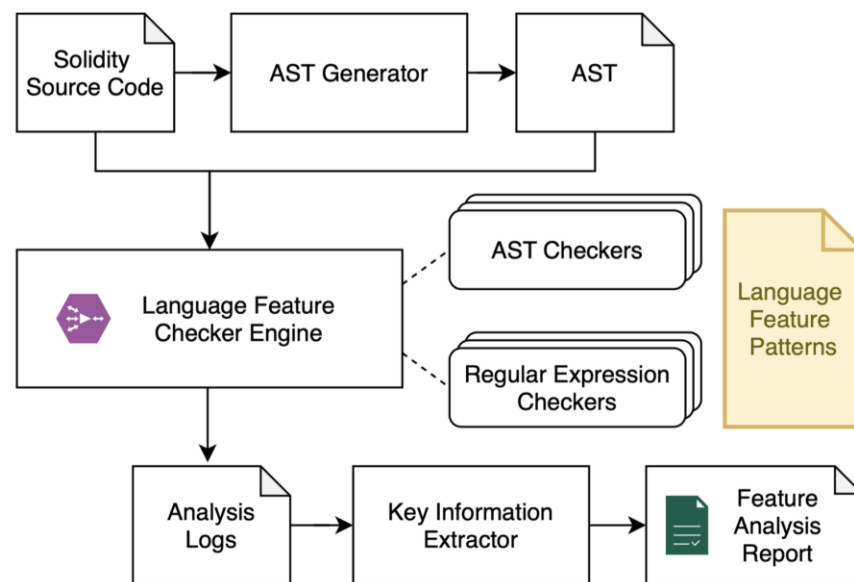


特性使用情况分布

## ■ Solidity语言特性实证研究



- 设计静态特性分析工具自动分析源代码，获得41种特性的使用情况分布数据，并总结出5个研究结论



静态特性分析工具架构图

- 结论1：高级跨合约函数调用、可见性、断言、事件和NatSpec文档是最受欢迎的特性，而SMT检查器、Unicode字符串、自由函数和函数修饰符覆盖是最不受欢迎的特性
- 结论2：随着时间的推移，开发人员倾向于使用构建大型复杂合约所需的特性，例如接口和库，并避免fallback函数等容易出错的特性
- 结论3：可见性、事件和断言等特性提供了智能合约的基本功能，几乎被所有合约使用
- 结论4：编写开源智能合约的开发人员愿意使用NatSpec格式在他们的代码中编写文档
- 结论5：低级函数调用和多重继承等不安全和复杂的特性不如安全和易于使用的特性受欢迎



# 四、部分实验结果

## 智能合约交易重放方法



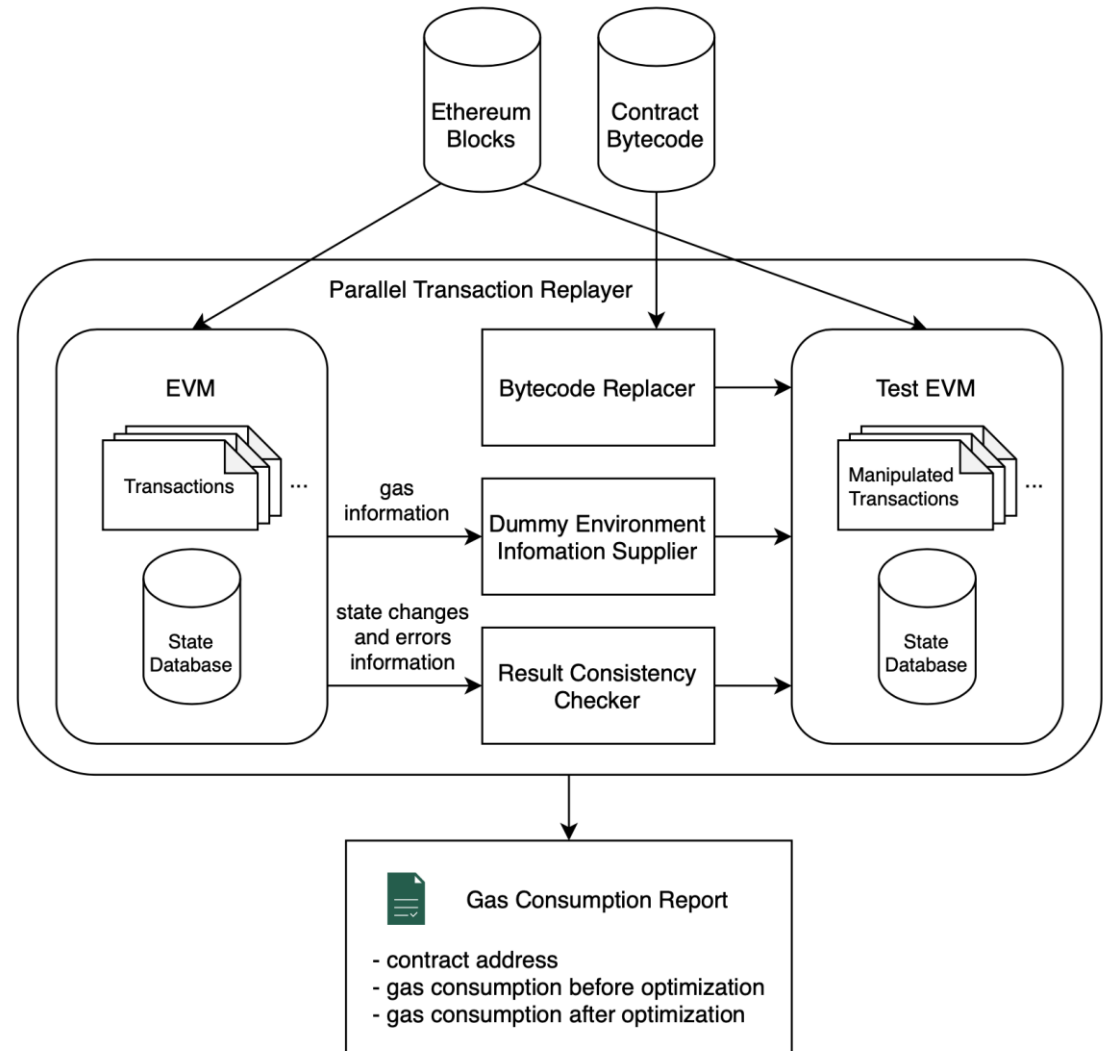
### 系统主要模块

- 以太坊虚拟机 (2个)
- 字节码替换器
- 虚拟环境信息提供者
- 结果一致性验证器

Table 3. Gas Saving of six Gas-inefficient Patterns

Pattern	# c	# t	# saving gas	
			deploy	invoke
P1	11,657	286,696	80,494,110	12,174,283
P2	8,810	229,995	79,077,573	749,724
P3	2,149	59,146	12,262,199	8,860,627
P4	1,898	69,621	-22,030,761	23,219,821
P5	7,442	189,270	348,897	4,850,887
P6	3,216	109,215	29,664,663	23,636,855

Gas优化效果评估实验结果



系统架构图



## 五、学位论文工作计划安排

- 12/01-12/20 开题
- 12/20-01/31 完成Solidity语言特性实证研究的写作
- 02/01-02/28 完成智能合约交易重放方法的代码开发和实验
- 03/01-03/31 完成智能合约交易重放方法的写作





# 六、目前论文和专利成果

## ■ 已发表的论文

**QRS 2021**


The 21st IEEE International Conference on  
Software Quality, Reliability, and Security  
December 6-10, 2021 • Hainan Island, China



Journal of  
Computer Science & Technology

- Ziyan Wang et al., An Empirical Study of Solidity Language Features, The 21st IEEE International Conference on Software Quality, Reliability, and Security Workshop (EI, 第一作者, 与语言特性实证研究相关)
- Queping Kong, Ziyan Wang et al., Characterizing and Detecting Gas-Inefficient Patterns in Smart Contracts, Journal of Computer Science and Technology (CCF-B, 第二作者, 与交易重放方法相关)

## ■ 已公开的专利

-  (老师), 王子彦等: 一种基于源代码的智能合约优化方法及装置, 申请号: 202110013879.3 (第二发明人, 与交易重放方法相关)

# 参考文献



- [1] Z. Zheng, S. Xie, H. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, “An overview on smart contracts: Challenges, advances and platforms,” *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020.
- [2] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
- [3] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, (New York, NY, USA), p. 254–269, Association for Computing Machinery, 2016.