

Contents

Introduction	1
1. Ethereum & Gas Costs	3
1.1. Blockchains	3
1.2. Ethereum & Solidity	4
1.3. The Gas System	6
1.4. Gas Estimations	6
1.4.1. Static Opcode Analysis	7
1.4.2. GASTAP	8
2. Estimating Gas Costs	9
2.1. Fuzz Testing	9
2.2. Argument Generation	9
2.3. Transaction Execution	10
2.4. Symbolic Analysis	11
2.5. Implementation Design	12
2.6. Contracts and Experiment Execution	15
3. Results	16
3.1. Blueprints	16
3.2. Cost trend	17
3.3. Classification	18
3.4. Quantitative analysis	19
Conclusion	22
Bibliography	23
Appendices	25
Appendix A. Example Ballot Contract	25
Appendix B. Fuzzer Procedures for Solidity Types	29
B.1. Fixed Size Types	29
B.1.1. Booleans	29
B.1.2. Integers	29

B.1.3. Addresses	29
B.1.4. Fixed-Point Numbers	29
B.1.5. Characters	30
B.1.6. Fixed-size Byte Arrays	30
B.1.7. Function Pointers	30
B.1.8. Fixed-size Arrays	30
B.2. Dynamic Size Types	30

Appendix C. Contract Composition **31**

Table Index

1.1. Resulting estimations from a sample contract	8
---	---

Figure Index

1.1. Basic structure of a blockchain.	3
2.1. Frequency of each kind of operation found within require statements	11
2.2. Frequency of each operator used within binary operations	12
2.3. Architecture of the developed tool.	13
2.4. Structure used to store fuzzers in the fuzzing layer.	14
2.5. Class hierarchy defined by all the implemented fuzzers.	15
3.1. Gas cost of a service in the less than, constant, category	17
3.2. Gas cost of a service in the less than, constant, category	18
3.3. Heatmap indicating the obtained classifications	19
3.4. Gas cost of the service transferOwnership	21
3.5. Heatmap displaying the results of the experiment with symbolic analysis. . .	21
C.1. Frequency of solidity versions used in the contract database.	31