Olivier Bégassat, Alexandre Belling, Théodore Chapuis-Chkaiban, Franklin Delehelle, Blazej Kolad, Nicolas Liochon

Hi all,

Here is an updated version of the specification we shared last yeararithmetization of a ZK-EVM, and that we will present at devCon (on the 13th, at 11am, please come

).

This is a type 2 ZK-EVM in Vitalik's categorization: it natively supports EVM bytecode, keeping opcodes, including those handling smart contract calls, error management and gas management, as is, but the internal state is represented differently.

The specification covers the stack, the RAM, opcode executing modules such as binary, word comparison, arithmetic, storage. It is still a work in progress. Precompiles & selfdestruct will be added later. When tested against the reference EVM test suite, it runs successfully for 91% of the tests. The implementation will be shared soon.

Here's the document: ZK-EVM_spec.pdf (2.6 MB) and here it is with a white background

ZK-EVM_spec_white_background.pdf (2.6 MB)

Here is the decomposition of the tests. We split the tests in 3 parts:

- : traces are generated and constraints are satisfied;
- : tests that do not pass (i.e.

the implementation or the specification has a bug);

- not implemented

: tests that rely on one or more opcode not yet implemented (e.g.

precompiles).

Total

not implemented

TOTAL

17387

15904

43

1440

91.47%

0.25%

8.28%

stArgsZeroOneBalance

96

84

0

12

stAttackTest

2

0

0

2

stBadOpcode

4251

4165

1

85

stBugs

9

5

2

2

stCallCodes

86

66

0

20

stCallCreateCallCodeTest

55

44

0

11

stCallDelegateCodesCallCodeHomestead

58

41

0

17

stCallDelegateCodesHomestead

58

41

0

17

stChainId

2

2

0

0

stCodeCopyTest

2

2

0

0

stCodeSizeLimit

9

9

0

0

stCreate2

178

158

9

11

stCreateTest

175

164

0

11

stDelegatecallTestHomestead

31

31

0

0

stEIP150singleCodeGasPrices

339

330

0

9

stEIP150Specific

13

11

0

2

stEIP1559

1844

1844

0

0

stEIP158Specific

7

4

0

3

stEIP2930

140

140

0

0

stEIP3607

12

12

0

0

stExample

38

38

0

0

stExtCodeHash

65

41

0

24

stHomesteadSpecific

5

4

0

1

stInitCodeTest

22

20

0

2

stLogTests

46

46

0

0

stMemExpandingEIP150Calls

10

10

0

0

stMemoryStressTest

82

82

0

0

stMemoryTest

578

577

0

1

stNonZeroCallsTest

24

20

0

4

stPreCompiledContracts2

203

0

0

203

stRandom2

226

209

0

17

stRecursiveCreate

2

2

0

0

stRefundTest

26

15

2

9

stReturnDataTest

273

266

0

7

stRevertTest

271

157

0

114

stSelfBalance

42

42

0

0

stShift

42

34

8

0

stSLoadTest

1

1

0

0

stSolidityTest

23

18

0

5

stSpecialTest

14

12

0

2

stSStoreTest

475

475

0

0

stStackTests

375

294

0

81

stStaticCall

478

260

0

218

stStaticFlagEnabled

34

25

0

9

stSystemOperationsTest

69

54

1

14

stTimeConsuming

5190

5187

0

3

stTransactionTest

167

159

0

8

stTransitionTest

6

6

0

0

stWalletTest

46

42

19

-15

stZeroCallsRevert

16

12

0

4

stZeroCallsTest

24

20

0

4

stZeroKnowledge2

519

0

0

519

VMTests_vmArithmeticTest

219

217

1

1

VMTests_vmBitwiseLogicOperation

57

57

0

0

VMTests_vmIOandFlowOperations

170

170

0

0

VMTests_vmLogTest

46

46

0

0

VMTests_vmTests

136

133

0

3