

Plutus V3 Cost-Model Functions/Parameters

Links/Resources

- [Chris Moreton's Plutus Pioneer Program Notes](#)
- [Cardano Docs - Plutus](#)
- [Cardano Developer Resources - Smart Contracts](#)
- [Plutus User Guide - IOHK](#)
- [Plutus Repo - IntersectMBO](#)
- [Cost Model | Plutus Documentation - Intersect MBO](#)
- [See also notes.md](#)

Plutus V3 Cost Model Links (External, IntersectMBO):

- [Overview of Plutus Core Cost Model - PDF](#)
- [Plutus Cost Model](#)
- [Plutus Cost Model Data](#)
- [93 References to "costModel" in Intersect Plutus Repo](#)
- [Plutus Core Readme.md](#)
- [Plutus Cost Model Overview \(line 389\) - DOES NOT MATCH conway-genesis.json - Appears truncated](#)
- [Plutus Cost Model Generation](#)
- [Plutus Core Specification \(as of 28 Dec 2024\)](#)
- [Plutus Builtin Cost Model](#)
- [Mainnet Conway Genesis JSON](#)

Making Sense of Plutus Data from Conway Genesis JSON

- There are issues with the data provided by Intersect, further research is being performed
- **Numbers** 76-88 below **ARE NOT** reflected, or cross-referenced, in both **source** docs. These discrepancies are being researched.
 - JSON Lines = Plutus builtinCostModelC - [here](#) - copy
 - JSON Ouput Lines = mainnet-conway-genesis.json - [here](#) - copy
 - where arg = argument
 - where icept = intercept

No.	JSON Lines	JSON Output Lines	Function	cpu.arg.icept OR arg.1	cpu.arg.sl
1.	2 - 17	29 - 32	addInteger	100788	420
2.	18 - 33	33 - 36	appendByteString	1000	173
3.	34 - 49	37 - 40	appendString	1000	59957
4.	50 - 59	41 - 42	bData	1183	--
5.	60 - 72	267 - 269	blake2b_224	207616	8310

No.	JSON Lines	JSON Output Lines	Function	cpu.arg.icept	OR arg.1	cpu.arg.sl
6.	73 - 85	43 - 45	blake2b_256	201305		8356
7.	86 - 95	226 - 227	bls12_381_G1_add	962335		--
8.	96 - 105	228 - 229	bls12_381_G1_compress	2780678		--
9.	106 - 115	230 - 231	bls12_381_G1_equal	442008		--
10.	116 - 128	232 - 234	bls12_381_G1_hashToGroup	52538055		3756
11.	129 - 138	235 - 236	bls12_381_G1_neg	267929		--
12.	139 - 151	237 - 239	bls12_381_G1_scalarMul	76433006		8868
13.	152 - 161	240 - 241	bls12_381_G1_uncompress	52948122		--
14.	162 - 171	242 - 243	bls12_381_G2_add	1995836		--
15.	172 - 181	244 - 245	bls12_381_G2_compress	3227919		--
16.	182 - 191	246 - 247	bls12_381_G2_equal	901022		--
17.	192 - 204	248 - 250	bls12_381_G2_hashToGroup	166917843		4307
18.	205 - 214	251 - 252	bls12_381_G2_neg	284546		--
19.	215 - 227	253 - 255	bls12_381_G2_scalarMul	158221314		26549
20.	228 - 237	256 - 257	bls12_381_G2_uncompress	74698472		--
21.	238 - 247	258 - 259	bls12_381_finalVerify	333849714		--
22.	248 - 257	260 - 261	bls12_381_millerLoop	254006273		--
23.	258 - 267	262 - 263	bls12_381_mulMIResult	2174038		--
24.	268 - 284	275 - 279	byteStringToInteger	c0: 1006041		c1: 43623
25.	285 - 294	62 - 63	chooseData	94375		--

No.	JSON Lines	JSON Output Lines	Function	cpu.arg.icept	OR arg.1	cpu.arg.sl
26.	295 - 304	64 - 65	chooseList	132994		--
27.	305 - 314	66 - 67	chooseUnit	61462		--
28.	315 - 330	68 - 71	consByteString	72010		178
29.	331 - 340	72 - 73	constrData	22151		--
30.	341 - 356	74 - 77	decodeUtf8	91189		769
31.	357 - 384	78 - 88	divideInteger	85848		c00: 12320
32.	385 - 400	89 - 92	encodeUtf8	1000		42921
33.	401 - 414	93 - 96	equalsByteString	constant: 24548		intercept: 29
34.	415 - 427	97 - 99	equalsData	898148		27279
35.	428 - 440	100 - 103	equalsInteger	51775		558
36.	441 - 454	103 - 106	equalsString	constant: 39184		intercept: 10
37.	455 - 464	107 - 108	fstPair	141895		--
38.	465 - 474	109 - 110	headList	83150		--
39.	475 - 484	111 - 112	iData	15299		--
40.	485 - 494	113 - 114	ifThenElse	76049		--
41.	495 - 504	115 - 116	indexByteString	13169		--
42.	505 - 521	270 - 274	integerToByteString	c0: 1293828		c1: 28716
43.	522 - 534	264 - 266	keccak_256	2261318		64571
44.	535 - 544	117 - 118	lengthOfByteString	22100		--
45.	545 - 557	119 - 121	lessThanByteString	28999		74

No.	JSON Lines	JSON Output Lines	Function	cpu.arg.icept	OR arg.1	cpu.arg.sl
46.	558 - 570	122 - 124	lessThanEqualsByteString	28999		74
47.	571 - 583	125 - 127	lessThanEqualsInteger	43285		552
48.	584 - 596	128 - 130	lessThanInteger	44749		541
49.	597 - 606	131 - 132	listData	33852		--
50.	607 - 616	133 - 134	mapData	68246		--
51.	617 - 626	135 - 136	mkCons	72362		--
52.	627 - 636	137 - 138	mkNilData	7243		--
53.	637 - 646	139 - 140	mkNilPairData	7391		--
54.	647 - 656	141 - 142	mkPairData	11546		--
55.	657 - 683	143 - 152	modInteger	85848		c00: 12320
56.	684 - 699	153 - 156	multiplyInteger	90434		519
57.	700 - 709	157 - 158	nullList	74433		--
58.	710 - 737	159 - 169	quotientInteger	85848		c00: 12320
59.	738 - 764	170 - 179	remainderInteger	85848		c00: 12320
60.	765 - 780	180 - 183	serialiseData	955506		213312
61.	781 - 793	184 - 186	sha2_256	270652		22588
62.	794 - 806	187 - 189	sha3_256	1457325		64566
63.	807 - 822	190 - 193	sliceByteString	20467		1
64.	823 - 832	194 - 195	sndPair	141992		--
65.	833 - 848	196 - 199	subtractInteger	100788		420

No.	JSON Lines	JSON Output Lines	Function	cpu.arg.icept	OR arg.1	cpu.arg.sl
66.	849 - 858	200 - 201	tailList	81663		--
67.	859 - 868	202 - 203	trace	59498		--
68.	869 - 878	204 - 205	unBData	20142		--
69.	879 - 888	206 - 207	unConstrData	24588		--
70.	889 - 898	208 - 209	unIData	20744		--
71.	899 - 908	210 - 211	unListData	25933		--
72.	909 - 918	212 - 213	unMapData	24623		--
73.	919 - 928	214 - 215	verifyEcdsaSecp256k1Signature	43053543		--
74.	929 - 941	216 - 218	verifyEd25519Signature	53384111		14333
75.	942 - 954	219 - 221	verifySchnorrSecp256k1Signature	43574283		26308
76.	955 - 971	--	andByteString	intercept: 100181		slope1: 726
77.	972 - 988	--	orByteString	intercept: 100181		slope1: 726
78.	989 - 1005	--	xorByteString	intercept: 100181		slope1: 726
79.	1006 - 1021	--	complementByteString	107878		680
80.	1022 - 1031	--	readBit	95336		--
81.	1032 - 1047	--	writeBits	281145		18848
82.	1048 - 1063	--	replicateByte	180194		159
83.	1064 - 1079	--	shiftByteString	158519		8942

No.	JSON Lines	JSON Output Lines	Function	cpu.arg.icept	OR arg.1	cpu.arg.sl
84.	1080 - 1095	--	rotateByteString	159378		8813
85.	1096 - 1108	--	countSetBits	107490		3298
86.	1109 - 1121	--	findFirstSetBit	106057		655
87.	1122 - 1134	--	ripemd_160	1964219		24520
88.	1135 - 1145	--	expModInteger	1000000000000		--