Ask questions to @ollie.j	For https://github.com/klaytn/klaytn/issues/1823							
Conclusion	geth/crypto/bls12381 is faster in point arithmetic, but supranational/blst is also usable.							
	supranational/blst is good enough for consensus which involves only a few op/sec.							
Thesis to verfy:	The library's performance is coherent to EVM gas pricing							
Tested by: ollie.j	**geth/crypto/bls12381 v1.11.5**							
Tested at: 2023.04.07	**darwin/arm64, Apple M1 Max 10-core, MacOS 12.6**					**linux/amd64, Xeon E5-2686 16-core, m4.4xlarge**		
EIP-2537 precompiles	bench name	nsec/op	Measured gas	EIP gas pricing		nsec/op	Measured gas	EIP gas pricing
BLS12_G1ADD	BenchmarkG1Add	572	17	500		1,279	38	500
BLS12_G1MUL	BenchmarkG1Mul	152,282	4,568	12,000		503,436	15,103	12,000
BLS12_G1MULTIEXP	-	-	-	(variable)		-	-	(variable)
BLS12_G2ADD	BenchmarkG2Add	1,720	52	800		3,878	116	800
BLS12_G2MUL	BenchmarkG2Mul	478,777	14,363	45,000		1,562,219	46,867	45,000
BLS12_G2MULTIEXP	-	-	-	(variable)		-	-	(variable)
BLS12_PAIRING	BenchmarkPairing (1 pair)	899,459	26,984	108,000		1,947,002	58,410	108,000
BLS12_MAP_FP_TO_G1	BenchmarkG1MapToCurve	81,953	2,459	5,500		186,214	5,586	5,500
BLS12_MAP_FP2_TO_G2	BenchmarkG2SWUMap	1,337,893	40,137	75,000		2,853,158	85,595	75,000
Thesis to verfy:	(1) The library is efficient enough for consensus purpose (2) the library is also useful for EIP-2537 purpose							
Tested by: ollie.j	**supranational/blst/binding/go v0.3.10**							
Tested at: 2023.04.07	**darwin/arm64, Apple M1 Max 10-core, MacOS 12.6**					**linux/amd64, Xeon E5-2686 16-core, m4.4xlarge**		
EIP-2537 precompiles	bench name	ns/op	Measured gas	EIP gas pricing		ns/op	Measured gas	EIP gas pricing
BLS12_G1ADD								
BLS12_G1MUL	BenchmarkMultiScalarP1Once	256,352	7,691	12,000		423,817	12,715	12,000
BLS12_G1MULTIEXP								
BLS12_G2ADD								
BLS12_G2MUL	BenchmarkMultiScalarP2Once	584,176	17,525	45,000		1,060,165	31,805	45,000
BLS12_G2MULTIEXP								
BLS12_PAIRING								
BLS12_MAP_FP_TO_G1								
BLS12_MAP_FP2_TO_G2								
Signature (G1=pub,G2=sig)	bench name	ns/op	**ms/op**	op/sec		ns/op	**ms/op**	op/sec
G2.Sign	BenchmarkCoreSignMinPk	312,855	**0.3**	3,196		537,056	**0.5**	1,862
G2.Verify	BenchmarkCoreVerifyMinPk	696,372	**0.7**	1,436		1,250,972	**1.3**	799
G2.AggSigs; x10	BenchmarkCoreAggregateMinPk/10	202,108	**0.2**	4,948		391,064	**0.4**	2,557
G2.AggSigs; x100	BenchmarkCoreAggregateMinPk/100	1,011,215	**1.0**	989		1,734,007	**1.7**	577
G2.AggSigs; x1000	BenchmarkCoreAggregateMinPk/1000	9,015,656	**9.0**	111		15,185,507	**15.2**	66
G2.AggVerify; same msg; x10	BenchmarkCoreFastVerifyAggregateMinPk/10	694,654	**0.7**	1,440		1,289,785	**1.3**	775
G2.AggVerify; same msg; x100	BenchmarkCoreFastVerifyAggregateMinPk/100	743,987	**0.7**	1,344		1,378,276	**1.4**	726
G2.AggVerify; same msg; x1000	BenchmarkCoreFastVerifyAggregateMinPk/1000	1,265,313	**1.3**	790		1,865,692	**1.9**	536
G2.AggVerify; many msgs; x10	BenchmarkCoreVerifyAggregateMinPk/10	1,104,490	**1.1**	905		2,063,752	**2.1**	485
G2.AggVerify; many msgs; x100	BenchmarkCoreVerifyAggregateMinPk/100	5,067,965	**5.1**	197		8,197,031	**8.2**	122
G2.AggVerify; many msgs; x1000	BenchmarkCoreVerifyAggregateMinPk/1000	41,577,262	**41.6**	24		71,776,914	**71.8**	14
Signature (G1=sig,G2=pub)	bench name	ns/op	**ms/op**	op/sec		ns/op	**ms/op**	op/sec
G1.Sign	BenchmarkCoreSignMinSig	143,730	**0.1**	6,957		215,327	**0.2**	4,644
G1.Verify	BenchmarkCoreVerifyMinSig	578,030	**0.6**	1,730		1,106,987	**1.1**	903
G1.AggSigs; x10	BenchmarkCoreAggregateMinSig/10	164,248	**0.2**	6,088		323,610	**0.3**	3,090
G1.AggSigs; x100	BenchmarkCoreAggregateMinSig/100	782,225	**0.8**	1,278		1,273,525	**1.3**	785
G1.AggSigs; x1000	BenchmarkCoreAggregateMinSig/1000	6,867,378	**6.9**	146		10,851,514	**10.9**	92
G1.AggVerify; same msg; x10	BenchmarkCoreFastVerifyAggregateMinSig/10	592,340	**0.6**	1,688		1,289,785	**1.3**	775
G1.AggVerify; same msg; x100	BenchmarkCoreFastVerifyAggregateMinSig/100	680,527	**0.7**	1,469		1,378,276	**1.4**	726
G1.AggVerify; same msg; x1000	BenchmarkCoreFastVerifyAggregateMinSig/1000	1,396,783	**1.4**	716		1,865,692	**1.9**	536
G1.AggVerify; many msgs; x10	BenchmarkCoreVerifyAggregateMinSig/10	906,087	**0.9**	1,104		1,820,643	**1.8**	549
G1.AggVerify; many msgs; x100	BenchmarkCoreVerifyAggregateMinSig/100	3,939,685	**3.9**	254		6,333,793	**6.3**	158
G1.AggVerify; many msgs; x1000	BenchmarkCoreVerifyAggregateMinSig/1000	29,809,165	**29.8**	34		51,260,395	**51.3**	20