24.04.30 Cost Discussion

Xun Zhang Bingsheng Zhang
Zhejiang University, CHN
22221024@zju.edu.cn bingsheng@zju.edu.cn

April 30 2024

1 BLS cost(unfinished part from last week)

We also estimated the cost of various operations(mainly signature scheme) on the Cardano.

The aggregate BLS signature schemes have two versions(or examples). Single key version has the same key and different messages, with public key over G1. This function returns a list of 10 messages {'msg_1', ..., 'msg_10'}, a public key 'pk', and an aggregate signature 'aggr_sig'.

Multi key version has same message, with public key over G2. This function returns a message 'msg', ten public keys '{pk_1,...,pk_10}', and an aggregate signature 'aggr_sig'.

Operation	Script size	CPU usage	memory usage
BLS Verification(G1)	332	1,463,720,946	5754
BLS Verification(G2)	380	1,342,066,427	5754
AggSig Verification(single key)	777	3,336,910,422	71202
AggSig Verification(multi key)	1704	3,676,891,887	430586
Schnorr Verification(G1)	370	248,136,411	13796
Schnorr Verification(G2)	514	493,212,089	13964

Table 1: Cost of signature verification on BLS12-381

and the cost of verifying a single BLS signature can be computed as follow(Note that there may be slight differences between the calculated results and the actual running results):

Funtion	Single BLS Verification
bls12_381_G1_uncompress	1
bls12_381_G2_uncompress	1
bls12_381_G2_hashToCurve	1
bls12_381_GT_millerLoop	2
bls12_381_GT_mul	0
bls12_381_GT_finalVerify	1
Total	1,417,919,846

Table 2: BLS Verification Cost(over G1)

2 Verification cost

review the cost of Groth16 proof verification and ATMS verification.

Funtion	Groth16 Verification	ATMS Verification
bls12_381_G1_uncompress	4	N
bls12_381_G2_uncompress	4	0
bls12_381_G1_mul	1	0
bls12_381_G1_add	1	$N+1$
bls12_381_GT_millerLoop	4	2
bls12_381_GT_mul	2	0
bls12_381_GT_finalVerify	1	1
blake2b_256	0	$\log_2 M * N$
Total	2,299,066,153	1,914,978,116 $(M = 100, N = 34)$

Table 3: Verification Cost

and we also use the data from Kenneth, to see how expensive to verify a original Plonk proof over Cardano. The number of operations required for a vanilla plonk verifier are (the numbering refers to each step of the verifier as in the original paper):

Funtion	Plonk Verification
bls12_381_G1_uncompress	16
bls12_381_G2_uncompress	2
bls12_381_G1_mul	17
bls12_381_G1_add	20
bls12_381_GT_millerLoop	4
bls12_381_GT_mul	2
bls12_381_GT_finalVerify	1
blake2b_256	6
modular exponantiation	1
multiplyInteger	42
divideInteger	1
addInteger	14
modInteger	2
Total	3,255,167,757

Table 4: Plonk Verification Cost

And this version of Plonk is based on KZG polynomial commitment, which is also used in Halo2 proof system(to reduce the verification cost).

In conclusion, verifying the cost of Plonk proof is about 40% higher than verifying a Groth16 proof over Cardano.

Combine the zero knowledge proofs with signature scheme. Imagine a sufficiently simple (but not practical) scenario: using Halo2/Groth16 to prove the correctness of aggregation and straightly verify BLS signature. And we show the cost of various possible approaches:

	Plonk(Halo2)	Plonk(Halo2) + BLS	Plonk(Halo2) + Groth16	Plonk(Halo2) + Groth16 + BLS
CPU cost	3255M	4672M	2299M	3716M

Table 5: Bridge Scheme Verification Cost

Note that the results are calculated by hand, which may differ from the actual situation.