

Filecoin-some understanding of AMA

FileCoin (<https://learnblockchain.cn/tags/FileCoin>)

The format of the AMA is quite formal. Questions raised by the community will be deleted and confirmed. Juan, the founder of Filecoin, answered almost 100 questions. The evolution of the code also reflects the thinking of the filecoin team. The processing of the entire sector is more modular and more reasonable. What's more happy is that the filecoin team is also actively optimizing the part of Bellman's zero-knowledge proof.

On Friday morning, I took a look at Filecoin AMA (Ask Me Anything). The format of the AMA is quite formal. Questions raised by the community will be deleted and confirmed. Juan, the founder of Filecoin, answered almost 100 questions. After reading most of the questions and answers, let's summarize:

- Filecoin attaches great importance to security, first of all to ensure that it is safe to go online.
- The network is no accident, it will be online in June/July, but if there is a serious bug, the network may be reset.
- AMD's CPU has an advantage over Intel's CPU. Mainly an extension of **sha**.
- The GPU mainly uses Nvidia's graphics cards, and AMD's graphics cards are not considered for the time being.
- The network may outsourcing the calculation of zk-SNARK in the future.
- There is no reward for the second phase of the testnet.
- Cooperating with third parties to develop wallets.
- Home machines, mining is definitely not good.
- The tape drive is not working now, and the random read capability is not working.
- Filecoin does not support smart contracts.

Looking at the latest lotus and rust-fil-proofs code, there are a few more interesting points.

1. Will the GPU be used when the main network is online?

Many people care about whether the mainnet is online, do I need a GPU? In fact, if you have a deep understanding of the purpose of GPU, the answer is quite obvious. GPU is now mainly used to do three parts: seal commit, epost and post. In general, GPUs are currently used to accelerate zero-knowledge proofs. For the seal commit of the V20 version, the normal server CPU took more than 2 hours. A 2080ti GPU compresses the time to less than 1 hour. Because epost and post processes participate in consensus and require time, using a faster method is obviously beneficial to the entire network. At present, the more reliable solution for zero-knowledge proof acceleration is GPU acceleration. Of course, the CPU also has an acceleration scheme.

The above discussion is only based on the function of the entire network. Whether the mining machine is equipped with GPU or not, the filecoin team is also thinking about this issue. Judging from the answer to the question, the filecoin team is planning to turn the calculation part of the zero-knowledge proof into a service. In other words, the miner can use other zero-knowledge proof services to generate the proof without its own GPU. Those with GPU resources can provide such services.

2. Why does AMD's CPU have an advantage?



Magik6k 2:25 AM


Precommit1 ran for 8h23min, which gives about 1.08MiB/s; Precommit2 52min, 10.5MiB/s on TR3970x



1 reply 8 days ago



Magik6k 2:27 AM

The good news is that commit1 can just run on the same machine as Precommit2 as it only takes a few ms  星想法

As shown in the figure above, the precommit1 stage of the latest code on TR3970x only takes 8.5 hours. Maybe you think this time is too long. You know, on a general Intel server CPU, precommit1 may take more than 20 hours. This is the sector processing time after the algorithm is changed from window SDR to SDR.

If you are familiar with the precommit1 processing algorithm, you find that the current precommit1 process uses a large number of sha256 algorithms. TR3970x has sha extension, which is a more important reason.

By the way, from window SDR to SDR, the processing flow has also changed a little: precommit and commit are divided into two stages.

Now the code is getting more and more interesting, and the evolution of the code also reflects the thinking of the filecoin team. The processing of the entire sector is more modular and more reasonable. What's more happy is that the filecoin team is also actively optimizing the part of Bellman's zero-knowledge proof.

This article participates in the DingChain community writing incentive plan (<https://learnblockchain.cn/site/coins>) , good articles are good for profit, and you are welcome to join as well.

🕒 Published on 2020-03-09 20:17 Reading (789) Credits (3)

Category: FileCoin (<https://learnblockchain.cn/categories/FileCoin>)

0 likes

Favorites

Articles you may be interested in

Why is NFT different? How does Filecoin's distributed storage solution empower NFT?

(<https://learnblockchain.cn/article/2495>) 21 views

IPFS Weekly 132 | The next gathering will showcase the cooperation between IPFS and NFT

(<https://learnblockchain.cn/article/2418>) 69 views

IPFS helps expand ETH, Filecoin and DeFi to create the future together, and analyzes the powerful combination of IPFS and ETH (<https://learnblockchain.cn/article/2390>) 66 views

The Web3.0 China Summit came to a successful conclusion, Hu Feng, COO of Time Cloud: Filecoin needs long-termism! (<https://learnblockchain.cn/article/2375>) 94 views

Web 3.0 is coming, distributed storage plays an important role|Space Cloud invites you to participate in the Web3.0 China Summit and Distributed Storage Industry Conference (<https://learnblockchain.cn/article/2349>) 132 views

People's Daily Online: "Distributed storage opens up a market of 100 billion yuan", IPFS welcomes the new digital era! (<https://learnblockchain.cn/article/2320>) 186 views

Related questions

Which RPC interfaces are the three interface calls in the figure below the filecoin block explorer? ? ?

(<https://learnblockchain.cn/question/1505>) 1 answer

What is the current progress of Filecoin? (<https://learnblockchain.cn/question/4>) 1 answer

0 comments

Please log in (<https://learnblockchain.cn/login>) to comment