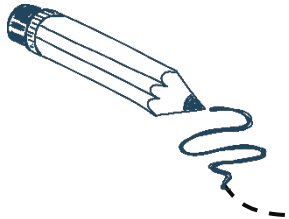
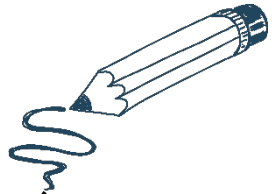
PoRep

—— Proof of Replication in Filecoin

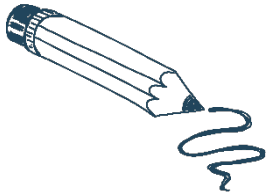
CONTENTS



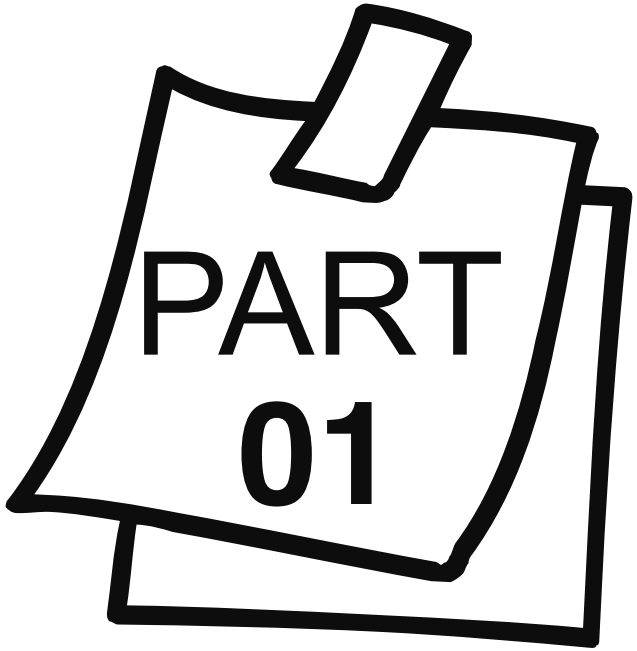
1. What's Filecoin?



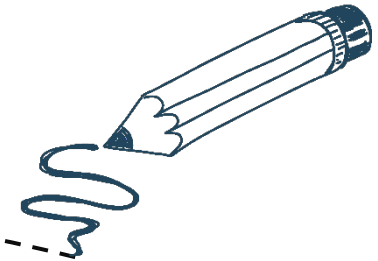
2. Challenges in implementing storage services



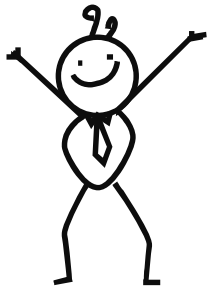
3. How to overcome the challenges? PoRep and PoSt !



What's Filecoin?



What's Filecoin?



Filecoin is a decentralized storage network that turns cloud storage into an algorithmic market!

To encourage participation and facilitate the development of the network,a token also called “filecoin” is used in the market.

What's Filecoin?

To construct a market for storing and retrieving.A marketplace for buying and selling data storage services.

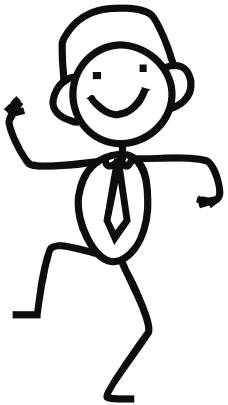
Provide PoRep and PoSt as consensus algorithm.
Ensure system security and fairness.

What's Filecoin?

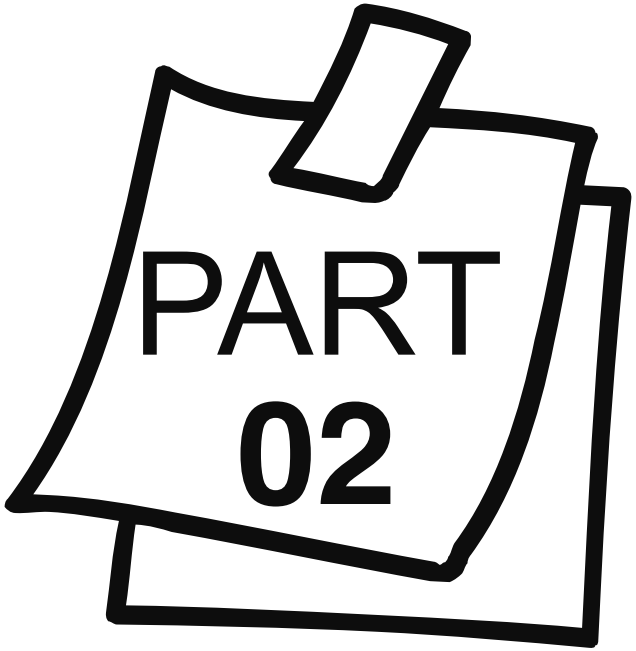
As a blockchain project,
Filecoin has **two main features**:

1. Real-world requirements (data storage) are completed while using distributed ledger.

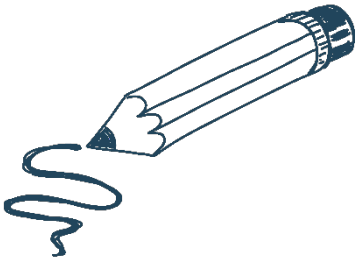
2. Considering PoS as common consensus will save more resources and is also more decentralized than using PoW.



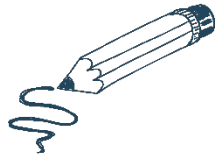
Therefore, Filecoin is safer, more efficient, and less costly than traditional storage services.
The Filecoin project is favored by many people and is considered to be a very promising public chain project.



Challenges in implementing storage services



How to implement storage services?



Actors in Filecoin

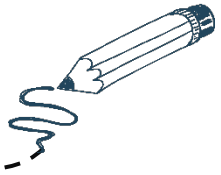
- client
- Store miners
- Retrieve miners
- The network

For example

Customer C has a data D wants to store 5 copies in the network.Store miners S1, S2, S3, S4, S5 through competition, get an opportunity to store D. The network gives each miner the right to record the next block according to the space stored by each miner, and the token is rewarded at the same time. When the customer needs to retrieve the data, the retrieve miner helps him get it back.

Is there any unexpected situation ?

How to implement storage services?
— Problems you may encounter



Is the data of customer c really stored by 5 storage miners? Maybe s1 is stored, but s3 is not. When c requests data from s3, s3 is obtained from s1 and handed over to c.

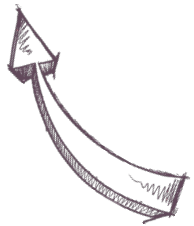
(**outsourcing attack**)

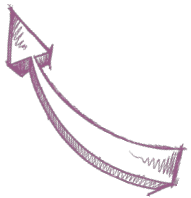
Maybe s1, s2, s3, s4, s5 are the 5 accounts registered by the same person, may only stores one copy.

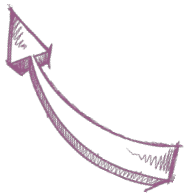
(**sybil attack**)

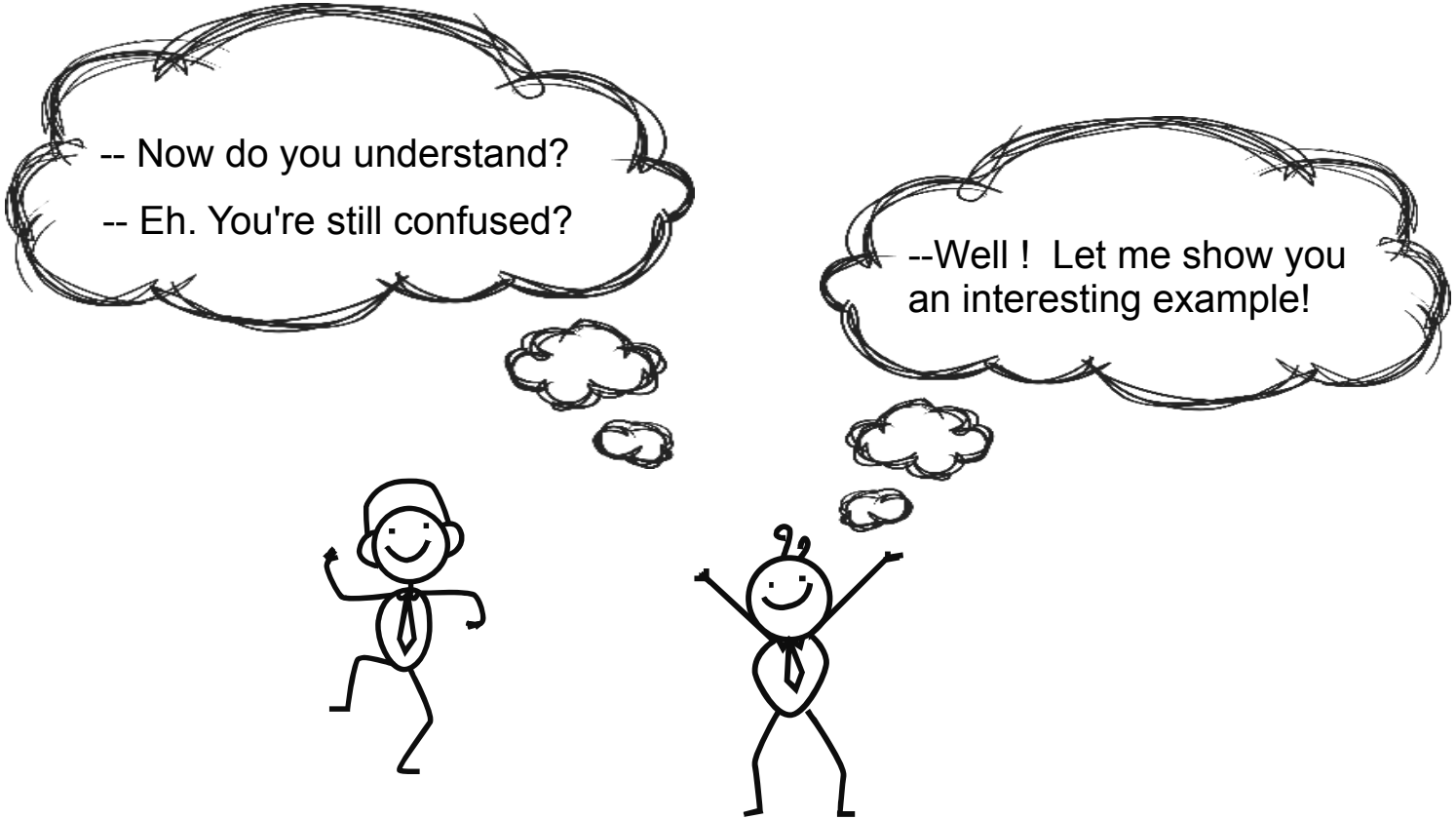
Perhaps customer c and storage miners are also together, and data D of c is generated by a very short D'. This way he only needs to store a small D'.

(**generation attack**)





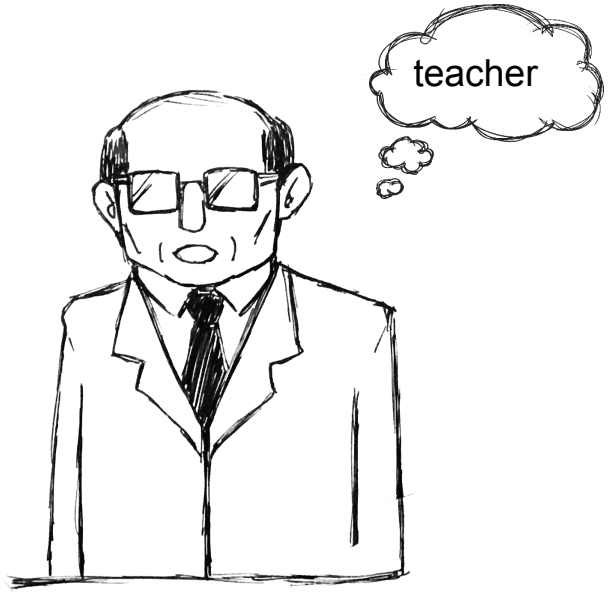



-- Now do you understand?
-- Eh. You're still confused?
--Well ! Let me show you an interesting example!

An interesting example：class notes

A middle school teacher has a habit, he will highlight some key points in each lesson and ask all the students to record in the notebook. So that, the students can review it at any time.

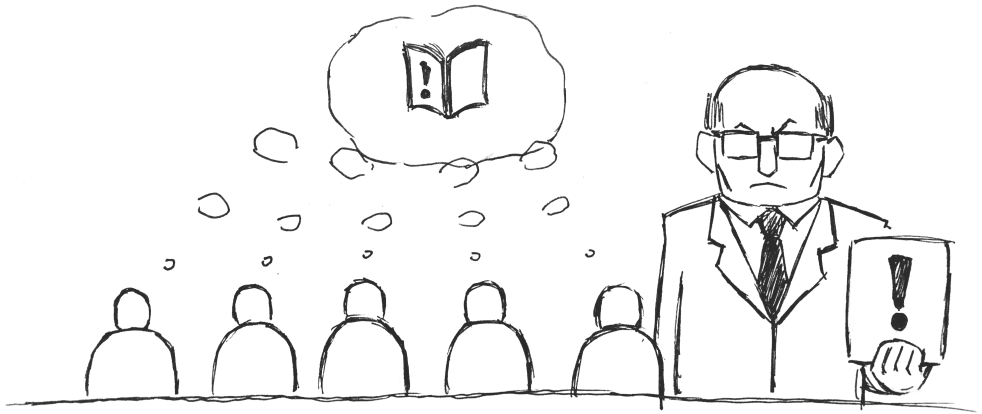
Suppose I hate taking notes or the paperis too expensive, how should I deal with it ?



Scenario 1

Every time the teacher checks my notes, I will take the notes of my deskmate to pretend to be mine.
（**outsourcing attack**）

Scenario 2



Although it is claimed that everyone has notes, in fact, there is only one note in the whole class. When the teacher checks who's notes, this note is taken as the person's.

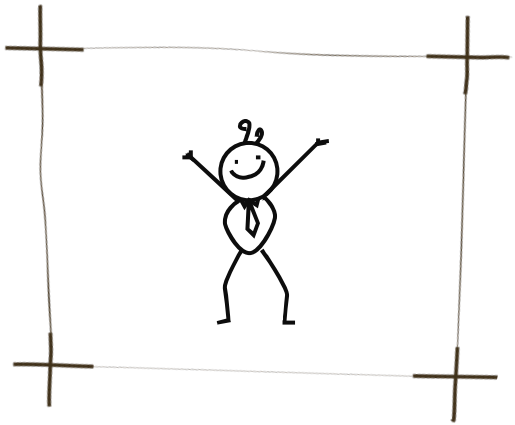
（**sybil attack**）

Scenario 3

Every time, when the teacher tells everyone she will check the notes tomorrow，then I will supplement a note all night.

（**generation attack**）

Negative effect caused by dishonesty



【From the perspective of storage services】

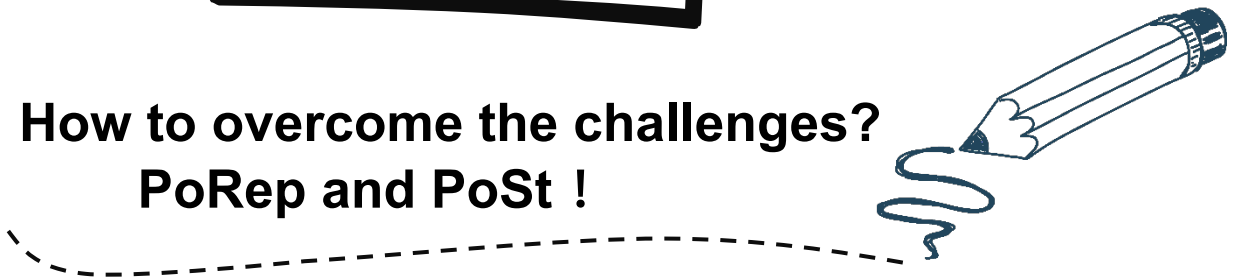
The security that customer redundant backup data expects to achieve is not guaranteed.

【From the perspective of blockchain】

Unsure of the amount of data stored by the miners. Therefore, a fair consensus mechanism cannot be formed.

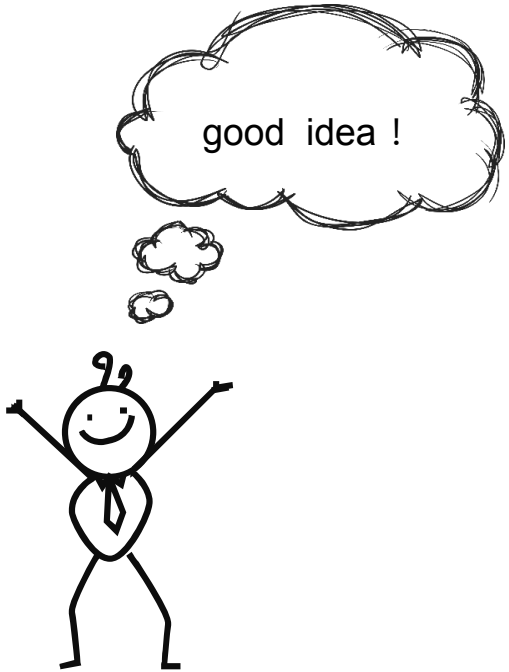
PART 03

How to overcome the challenges?
PoRep and PoSt！



How does the teacher solve the problem of cheating at notes ?

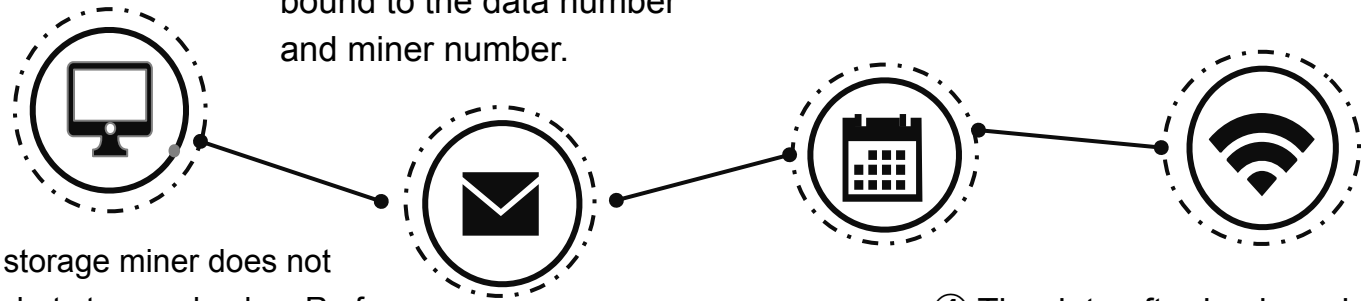
- Teacher needs to know the handwriting of everyone, each person's handwriting is different, so a note can only belong to one classmate.
- Teacher will tell the classmates an hour before checking the notes and ask them to be prepared.
- Now,as a classmate who wants to be lazy or want to save space on your notebook, do you have any way else to cheat?



How to solve ? PoRep !

② The backup method is bound to the data number and miner number.

③ The backup process is slow.



① The storage miner does not store D, but stores a backup R of D.（R is a transformation of D with same lenghth and invertible）.

④ The data after backup should meet the following requirements: even if a part is deleted, the missing part is still slow to generate.

【Result】

Each miner stores a backup R of the same length as the data D, and each backup R is different.

How to copy ?

【Main tools used】

Hash function：Make backup results and operation process results cannot be predicted in advance, close to random.

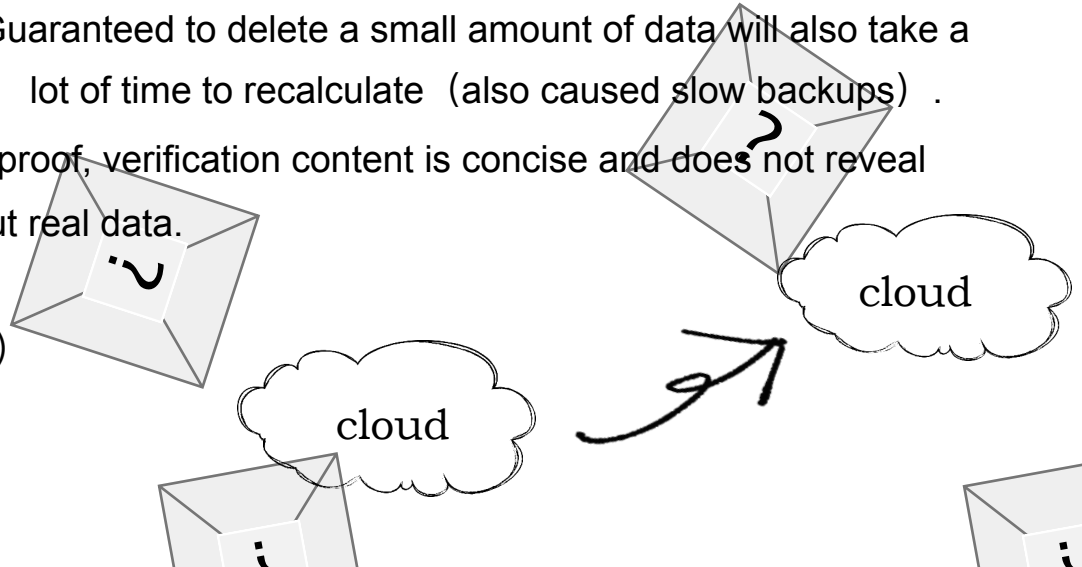
VC(Vector comment)：Used to promise and reveal promise.

DRG(Depth robust graph): Guaranteed to delete a small amount of data will also take a lot of time to recalculate（also caused slow backups）.

ZK-SNARK：Ensure that the proof, verification content is concise and does not reveal information about real data.

【Alternative tool】

VDE（Increase backup delay）



PoRep's brief steps

1. **R**eplication
   A replica is generated based on filecoin's replication parameters, data ID, miner ID, and source data.

2. **PoRep**
   The Proof of Replication is given according to the proof parameters given by Filecoin.

Thanks For Watching !