基于 Fabric 的存储扩展实践

李冠男

2018年8月

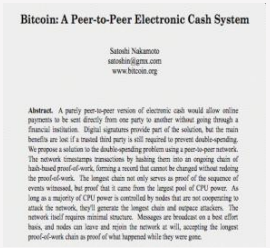
京东金融
JD Finance

京东金融
JD Finance

目 录

Part 1 背景

京东金融
JD Finance


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

A Peer-to-Peer
Electronic Cash System

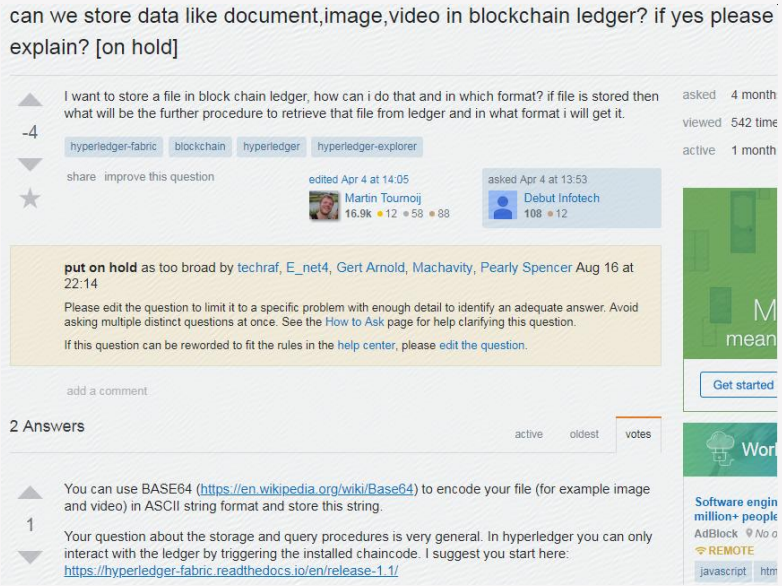
Bitcoin core

Ethereum

京东金融
JD Finance

同时，有些场景也需要区块链具备文件存储能力，如：

- ✓ Tx的附加文档，如：专利文件、版权
- ✓ 特定的大图片文件、视频，如：医学实验或检查结果
- ✓ 法律案件的各类证据
- ✓ 电子合同等……



can we store data like document,image,video in blockchain ledger? if yes please explain? [on hold]

I want to store a file in block chain ledger, how can i do that and in which format? if file is stored then what will be the further procedure to retrieve that file from ledger and in what format i will get it.

asked 4 month
viewed 542 time
active 1 month

-4

hyperledger-fabric | blockchain | hyperledger | hyperledger-explorer

share improve this question

edited Apr 4 at 14:05 Martin Tournoij 16.9k ● 12 ● 58 ● 88

asked Apr 4 at 13:53 Debut Infotech 108 ● 12

put on hold as too broad by techraf, E_net4, Gert Arnold, Machavity, Pearly Spencer Aug 16 at 22:14

Please edit the question to limit it to a specific problem with enough detail to identify an adequate answer. Avoid asking multiple distinct questions at once. See the How to Ask page for help clarifying this question.

If this question can be reworded to fit the rules in the help center, please edit the question.

add a comment

2 Answers active oldest votes

1

You can use BASE64 (https://en.wikipedia.org/wiki/Base64) to encode your file (for example image and video) in ASCII string format and store this string.

Your question about the storage and query procedures is very general. In hyperledger you can only interact with the ledger by triggering the installed chaincode. I suggest you start here: https://hyperledger-fabric.readthedocs.io/en/release-1.1/

Get started

Software engin
million+ people
AdBlock
REMOTE
javascript

找到约 3,250,000 条结果（用时 0.41 秒）

storage - How can I store big files on the blockchain? - Ethereum ...
https://ethereum.stackexchange.com/.../how-can-i-store-big-files-on-the-bloc... ▾ 翻译此页
1 个回答
2016年5月3日 - No, you will have to store your data somewhere else and store the hash of this data ar its location in the blockchain. You should have enough ...

solidity - Store whole document pdf files on ... 1 个回答 2018年7月19日
Document transfer via blockchain? 1 个回答 2017年8月17日
How does data storage on the blockchain work? 2 个回答 2017年2月8日
blocks - Storing document/file in blockchain 3 个回答 2016年8月8日
ethereum.stackexchange.com站内的其它相关信息

Attaching big files to the blockchain – Decentralized – Medium
https://medium.com/...blockchain/attaching-big-files-to-the-blockchain-64e9... ▾ 翻译此页
2017年9月18日 - BigChainDB is a blockchain adapted for the big files. It can store enormous amounts of data and provides really fast transactions. However it ...

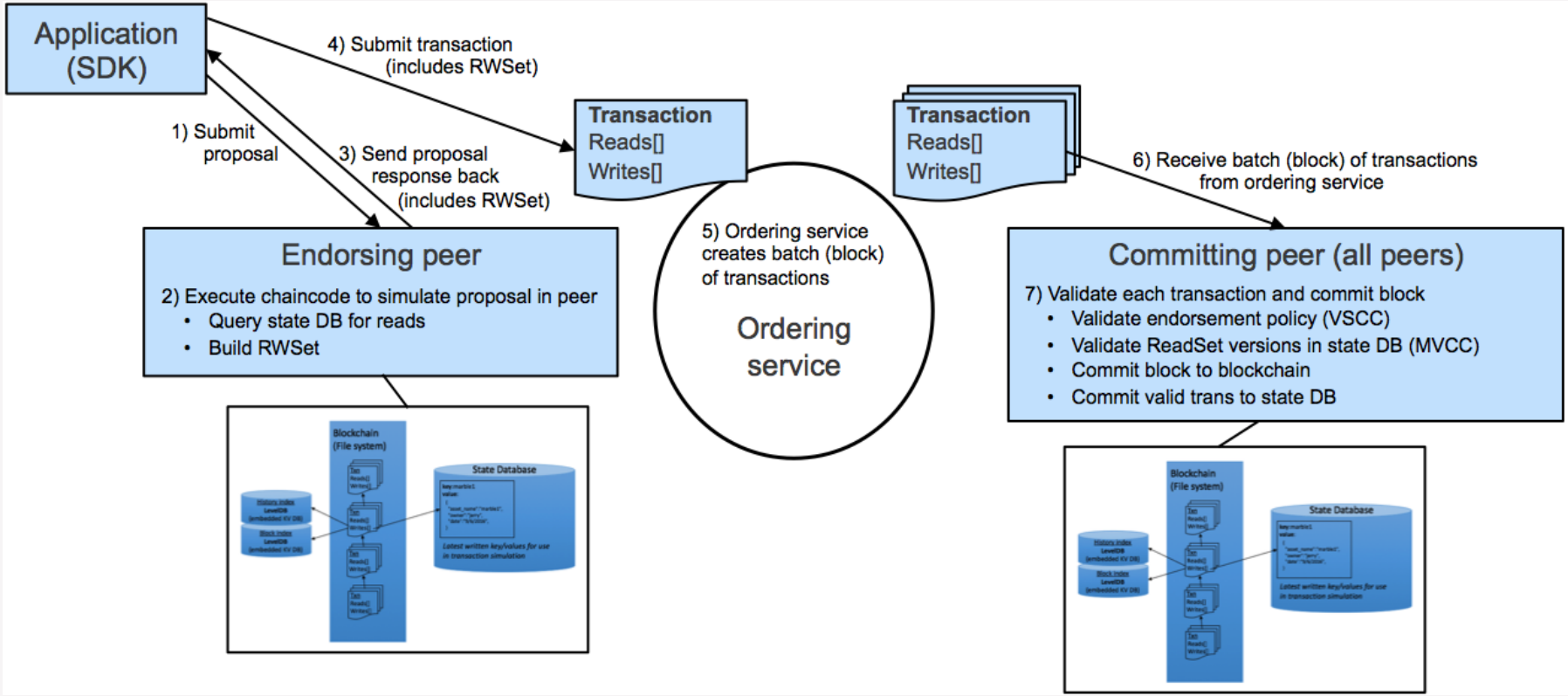
How to store big files on Blockchain - Quora
https://www.quora.com/How-can-I-store-big-files-on-Blockchain - 翻译此页
2018年4月15日 - Blockchain is one of the prevalent cryptocurrencies which may be defined as a digitized, decentralized, public ledger of all cryptocurrency transactions.

What's the best blockchain solution for storing large files in the ... 2018年2月18日
How can the blockchain verify the content of large files? 2017年11月6日
How to store/download a file in the Bitcoin blockchain network if ... 2016年5月16日
Can blockchain be used for file-sharing? 2016年3月30日
www.quora.com站内的其它相关信息

Can large files (over 64MB) be stored in the blockchain employing ...
https://www.multichain.com/.../stored-blockchain-employing-multiple-assoc... ▾ 翻译此页
2018年2月27日 - Yes, you can embed files of any size if you partition them across multiple stream item where each ha

存储文件的需求一直存在！

- 如果直接将文件存储在链上？来看下fabric的工作流程就知道这么做不太明智



京东金融 JD Finance

现　状

- 现阶段的主流区块链对（大）文件存储的支持如何呢？

Bitcoin	Can only store small amounts of Tx metadata
Ethereum	1MB data Costs 3.7628ETH（Gas Price：5 Gwei）
Hyperledger Fabric	< 99MB by default Edit brokerConfig.Producer.MaxMessageBytes (fabric/orderer/kafka/config.go) and rebuild to change.--- Not advisable

而且也没必要像Tx一样，让百兆千兆的各类文件副本存储在区块链的每一个节点上

所以通常的做法是：

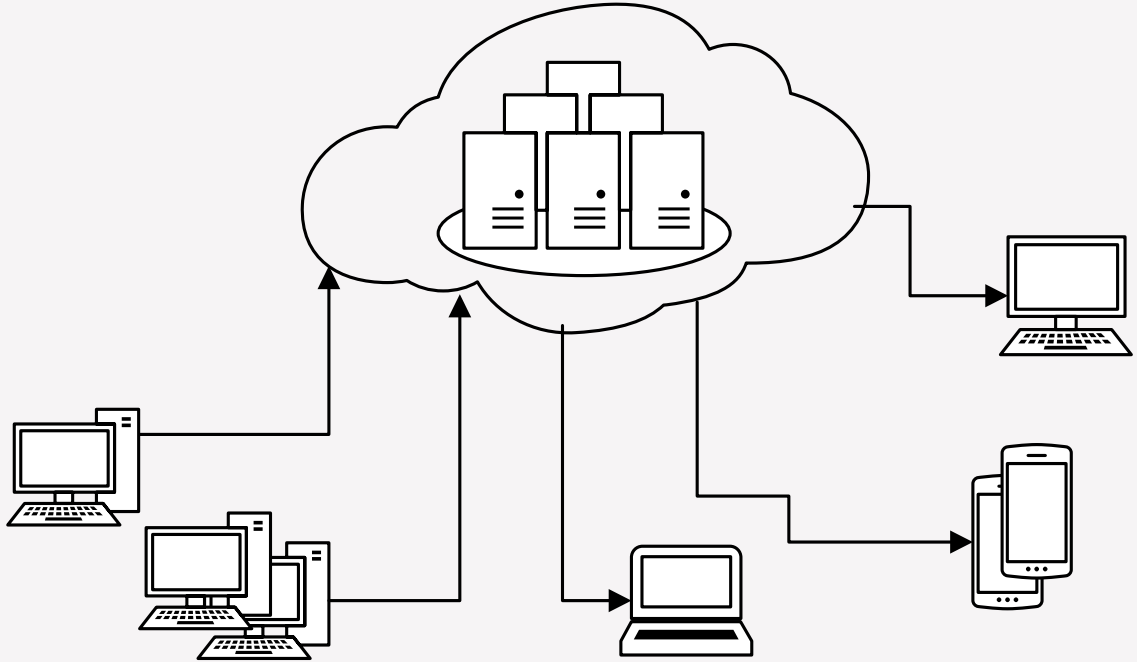
将文件存储在链外，在链上存储文件的hash

这样文件其实依然是中心化存储，比如传统的“云存储“

京东金融
JD Finance

现　状

传统云存储是让用户上传自己的数据到云端，用户上传完毕后，由服务提供商将数据保存在他们的数据中心。这样用户无论何时何地想要访问这些信息的时候，只需要向数据中心发送一条请求，数据中心将数据发给用户。



京东金融
JD Finance

现　状

问题（中心化存储）：

- 数据存储所需的大型服务器需要温控，并且严格维护， 成本高昂
- 会有延迟（通常数据中心与用户不会距离很近）
- CDN？隐私策略等由服务提供商设计，依然有办法访问和分享用户的个人数据，毕竟不透明
- 除开作恶可能，只要有人工牵扯进去，就很可能会有意外的错误产生（员工误删数据库的事件并不罕见，GitLab记忆犹新...）

京东金融
JD Finance

- 解决区块链天然不易存储大文件的问题：区块链+分布式存储网络技术

两者结合，发挥各自的优势

Part 2 相关概念&目标

京东金融 JD Finance

IPFS——What ?

- ✓ IPFS（ InterPlanetary File System ）星际文件系统
- ✓ IPFS是分布式存储网络
- ✓ IPFS是一个点对点的超媒体协议，目的是让现有的网络更快、更安全、更开放
- ✓ IPFS致力于替代HTTP协议，为所有人建造一个更好的网络

京东金融 JD Finance

IPFS——How？

- 每个文件以及所有的文件块都有独一无二的指纹，是一个加密哈希值

- IPFS可以自动去除网络中的重复文件，可以跟踪每个文件的版本历史

- 每个网络节点只存储自己感兴趣的内容以及一些索引信息，用来找到谁存储了什么

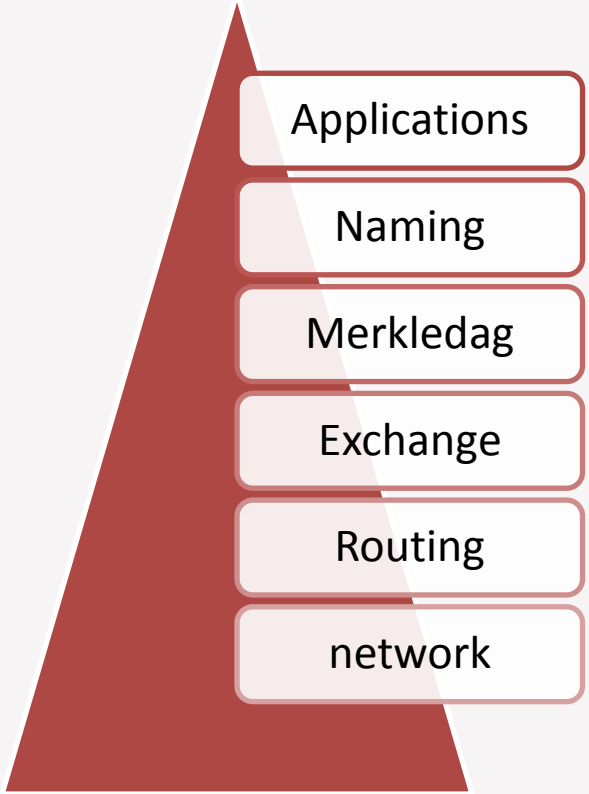
- 查找文件的时候使用Hash询问IPFS网络哪些节点存储了特定的内容

- 每个文件可以通过去中心化的命名系统IPNS获得对人友好的名字（不是一串看花眼的hash）

京东金融 JD Finance

IPFS——Stack

- IPFS包含借鉴了很多成熟的技术，并在其基础上进行了改进和创新



Web

Self-Certifying Filesystem

git

BitTorrent

DHT

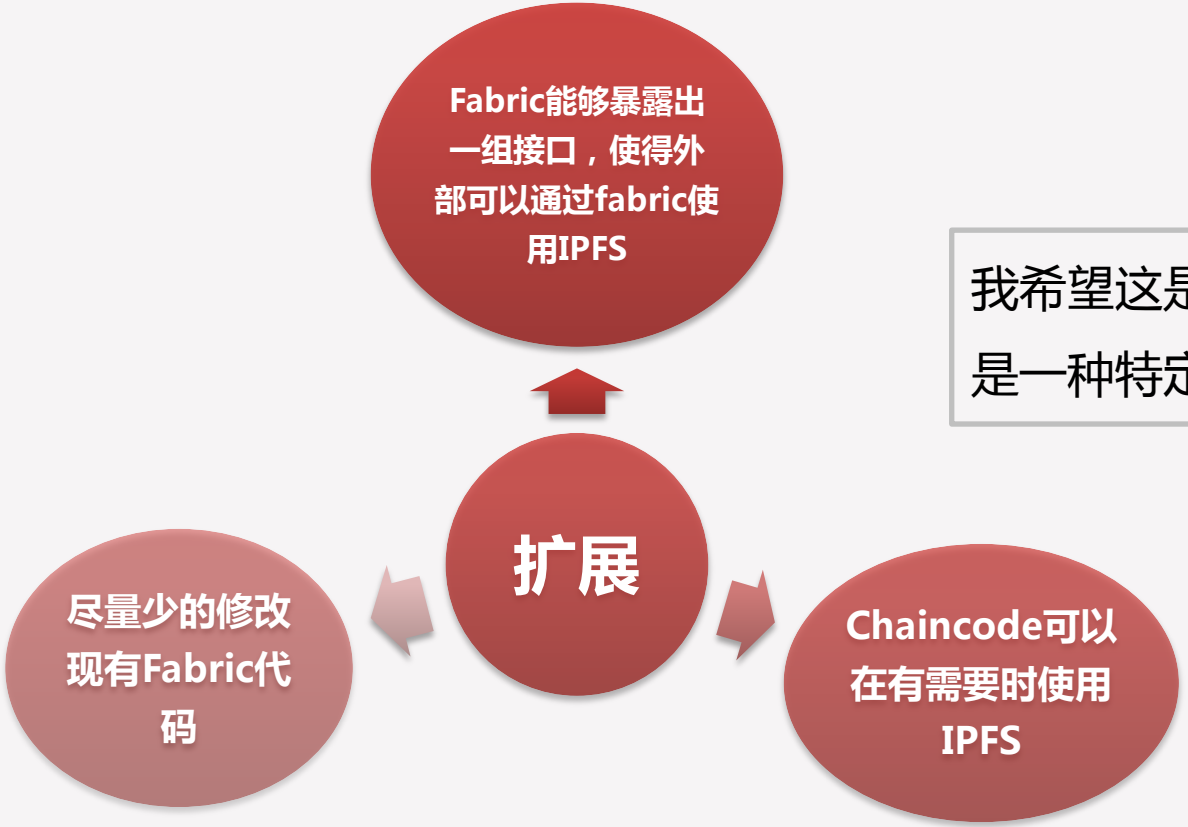
Using the Data

Defining the Data

Moving the Data

京东金融
JD Finance

我希望达成的目标



我希望这是一种系统的能力，而不是一种特定的应用层手段

京东金融 JD Finance

分　析

Fabric能够暴露出一组接口，使得fabric用户可以使用IPFS → Chaincode可以在有需要时使用IPFS → 尽量少的修改现有Fabric代码

以现有的go-sdk作为粘合剂，将fabric和ipfs联合起来，是最直接的方式

想法：对go-sdk进行二次开发，把与ipfs交互的逻辑封装其中，由sdk先请求ipfs得到返回，再将返回结果作为交易内容写入fabric

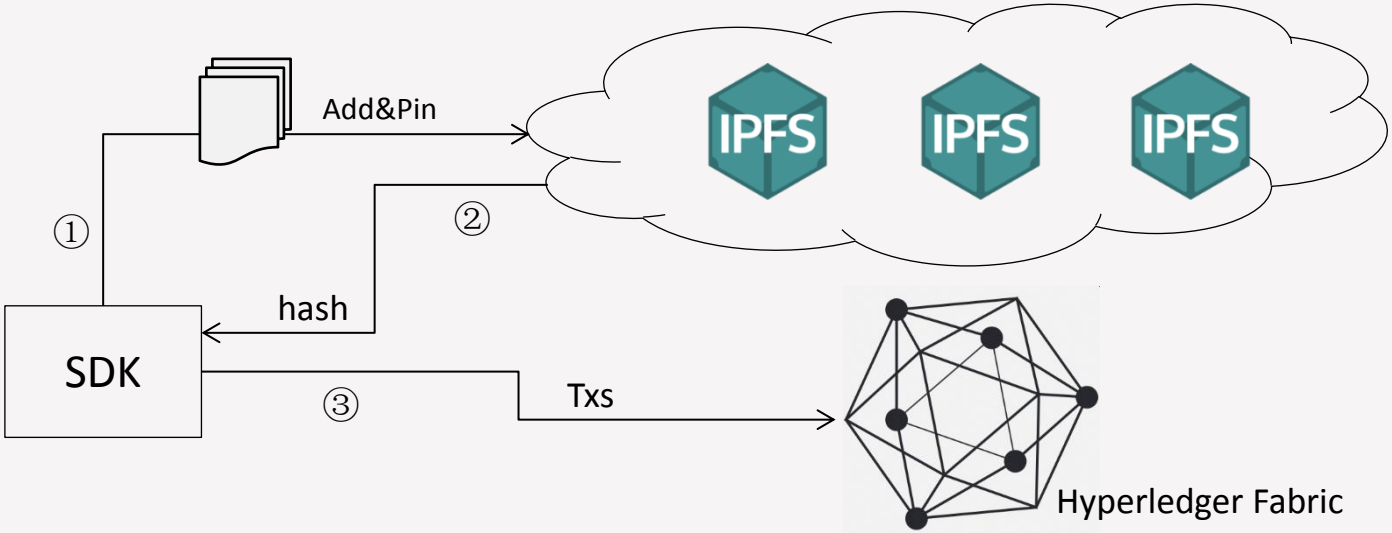
另外IPFS有几个特点需要注意：

- 有垃圾回收机制，写入某个节点的数据，只有经过称为“pin”的操作才能保证不被回收掉
- 不同节点之间不会自动备份同步数据，除非主动发起请求

Part 3 设计方案

京东金融 JD Finance

方案一



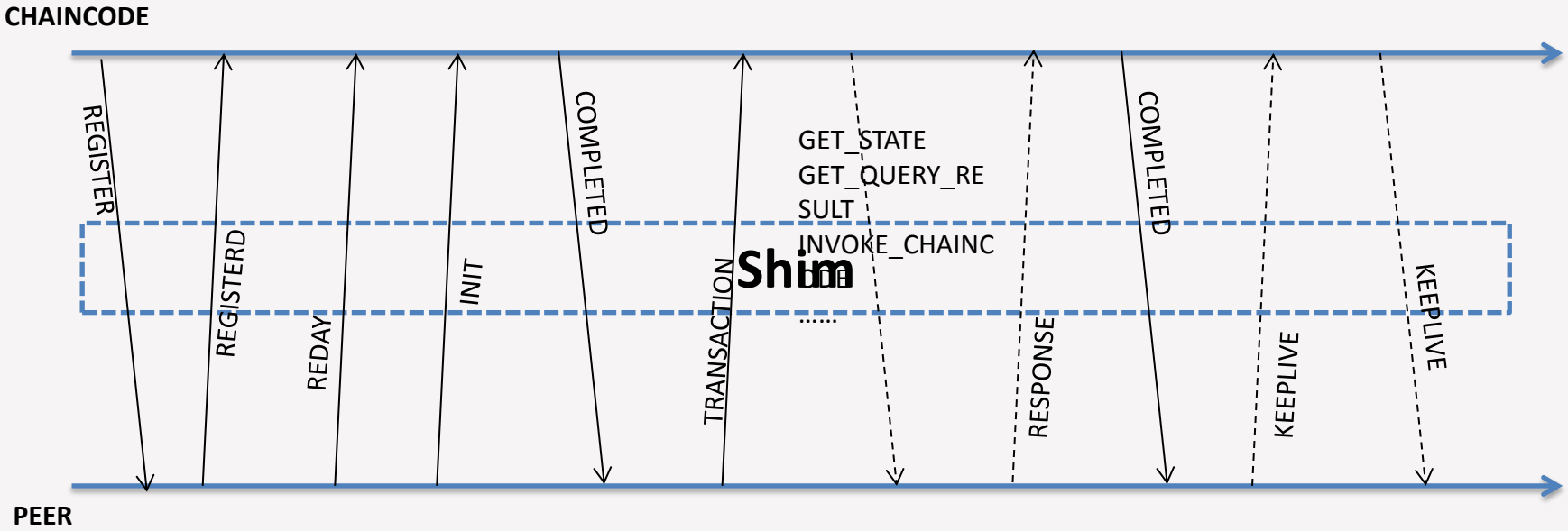
特点	缺点
ipfs与fabric相互独立	Chaincode无法使用ipfs
ipfs作为外部系统由sdk调用	
完全不用修改fabric的代码和内部流程	

京东金融 JD Finance

分 析

Chaincode运行在docker容器中

- 通过gRPC与 peer 通信
- 通过shim组件进行交互



京东金融 JD Finance

分 析

Shim中的chaincodeStubInterface定义了在chaincode中可以使用的功能。

于是想到，如果希望chaincode使用ipfs，可以对shim进行扩展来实现。

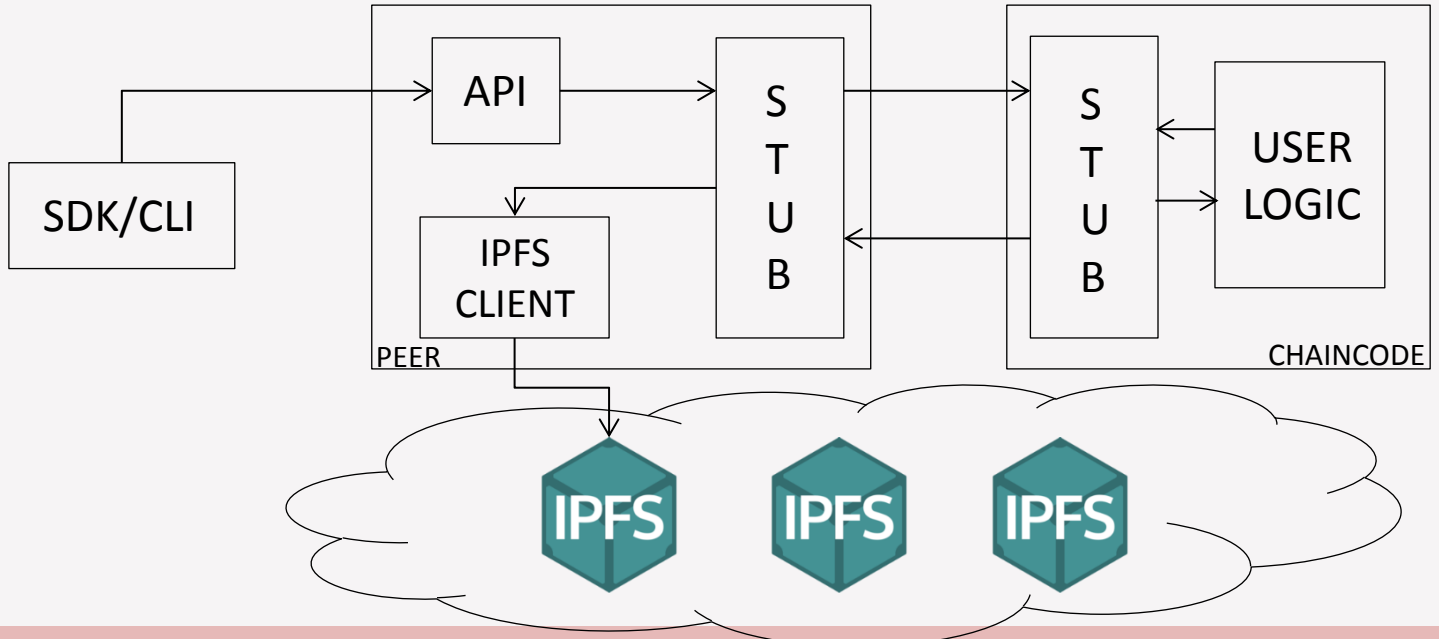
```
type ChaincodeStubInterface interface {
    GetArgs() [][]byte
    GetStringArgs() []string
    GetFunctionAndParameters() (string, []string)
    GetArgsSlice() ([]byte, error)
    GetTxID() string
    GetChannelID() string
    InvokeChaincode(chaincodeName string, args [][]byte, channel string) pb.Response
    GetState(key string) ([]byte, error)
    PutState(key string, value []byte) error
    DelState(key string) error
    GetStateByRange(startKey, endKey string) (StateQueryIteratorInterface, error)
    GetStateByPartialCompositeKey(objectType string, keys []string) (StateQueryIteratorInterface, error)
    CreateCompositeKey(objectType string, attributes []string) (string, error)
    SplitCompositeKey(compositeKey string) (string, []string, error)
    GetQueryResult(query string) (StateQueryIteratorInterface, error)
    GetHistoryForKey(key string) (HistoryQueryIteratorInterface, error)
    GetPrivateData(collection, key string) ([]byte, error)
    PutPrivateData(collection string, key string, value []byte) error
    DelPrivateData(collection, key string) error
    GetPrivateDataByRange(collection, startKey, endKey string) (StateQueryIteratorInterface, error)
    GetPrivateDataByPartialCompositeKey(collection, objectType string, keys []string) (StateQueryIteratorInterface, error)
    GetPrivateDataQueryResult(collection, query string) (StateQueryIteratorInterface, error)
    GetCreator() ([]byte, error)
    GetTransient() (map[string][]byte, error)
    GetBinding() ([]byte, error)
    GetDecorations() map[string][]byte
    GetSignedProposal() (*pb.SignedProposal, error)
    GetTxTimestamp() (*timestamp.Timestamp, error)
    SetEvent(name string, payload []byte) error
}
```

京东金融 JD Finance

方案二

想法：

- 扩展shim.ChaincodeStubInterface，添加实现相应的功能函数
- 在Fabric内开辟一个模块，专门用来处理ipfs相关的请求



这样就可以像调用GetState/PutState一样调用类似GetFile/PutFile的函数来获取/存储文件了。

京东金融 JD Finance

分 析

怎么办？

Fabric能够暴露出一组接口，使得fabric用户可以使用IPFS

Chaincode可以在有需要时使用IPFS

尽量少的修改现有Fabric代码

方案二与方案一相比实现了**目标2**，可以让chaincode使用ipfs。虽然有诸多缺点，但看上去方向是对的。

fabric pluggable scc：

- Fabric的系统链码会在每个新创建的channel自动部署一套
- 不同的channel之间实现了隔离

跳出来看，让chaincode使用ipfs，也即让chaincode调用外部的途径都有什么呢？

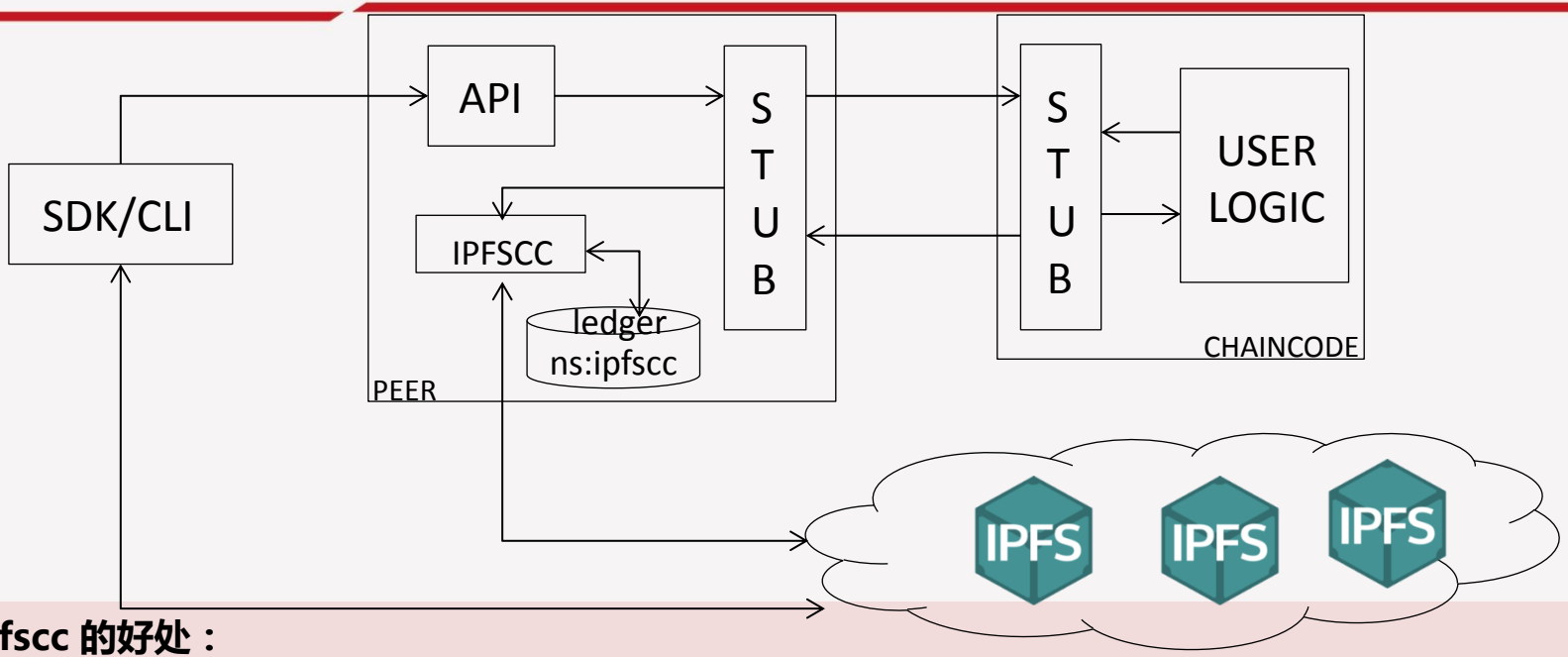
京东金融 JD Finance

分 析

```
type ChaincodeStubInterface interface {
    GetArgs() [][]byte
    GetStringArgs() []string
    GetFunctionAndParameters() (string, []string)
    GetArgsSlice() ([]byte, error)
    GetTxID() string
    GetChannelID() string
    InvokeChaincode(chaincodeName string, args [][]byte, channel string) pb.Response
    GetState(key string) ([]byte, error)
    PutState(key string, value []byte) error
    DelState(key string) error
    GetStateByRange(startKey, endKey string) (StateQueryIteratorInterface, error)
    GetStateByPartialCompositeKey(objectType string, keys []string) (StateQueryIteratorInterface, error)
    CreateCompositeKey(objectType string, attributes []string) (string, error)
    SplitCompositeKey(compositeKey string) (string, []string, error)
    GetQueryResult(query string) (StateQueryIteratorInterface, error)
    GetHistoryForKey(key string) (HistoryQueryIteratorInterface, error)
    GetPrivateData(collection, key string) ([]byte, error)
    PutPrivateData(collection string, key string, value []byte) error
    DelPrivateData(collection, key string) error
    GetPrivateDataByRange(collection, startKey, endKey string) (StateQueryIteratorInterface, error)
    GetPrivateDataByPartialCompositeKey(collection, objectType string, keys []string) (StateQueryIteratorInterface, error)
    GetPrivateDataQueryResult(collection, query string) (StateQueryIteratorInterface, error)
    GetCreator() ([]byte, error)
    GetTransient() (map[string][]byte, error)
    GetBinding() ([]byte, error)
    GetDecorations() map[string][]byte
    GetSignedProposal() (*pb.SignedProposal, error)
    GetTxTimestamp() (*timestamp.Timestamp, error)
    SetEvent(name string, payload []byte) error
}
```

京东金融 JD Finance

方案三



实现为 ipfscc 的好处：

- ✓ 可以单独维护，修改和升级更方便
- ✓ User Chaincode可以通过ChaincodeStubInterface.InvokeChaincode调用ipfscc来使用ipfs
- ✓ 不用修改代码
- ✓ 可以将文件索引存储在ipfscc namespace中，这样由系统实现文件状态监控也可行了，至于如何监控，是另外的故事

京东金融 JD Finance

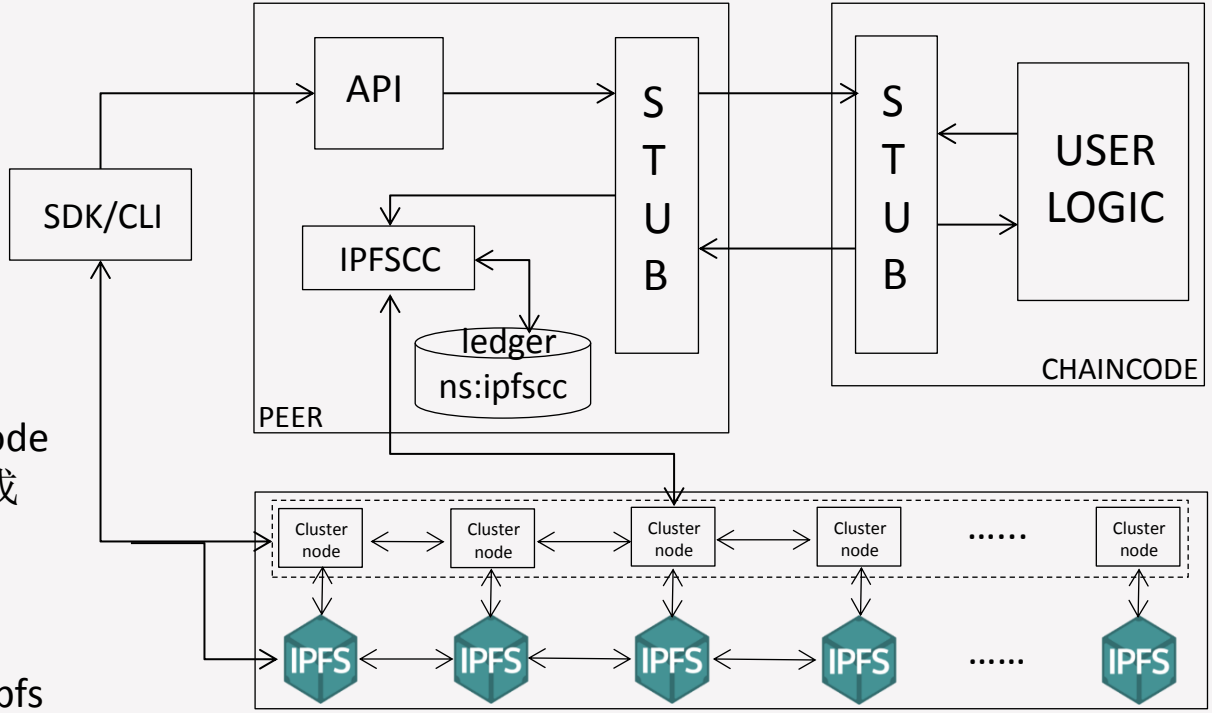
方案三

最后：

- 通过ipfs-cluster提供共识自动备份ipfs网络中的文件，并可以灵活配置备份数量

流程：

- Sdk/CLI上传文件/由chaincode根据需要在peer端临时生成文件并上载ipfs网络
- 得到返回hash，通过ipfs-cluster pin 文件
- 成功后将文件信息及相关ipfs索引信息写入ipfscc的ledger



谢谢