# Fabric支持RSA的策略和方法

## ——构筑安全可信的区块链网络

**张喜来 双链科技CEO**

# 个人简介

## 双链科技创始人 CEO

前大型电商系统高级架构师

服务过的客户

TOSHIBA Leading Innovation

Lane Crawford

FERGUSON a WOLSELEY company

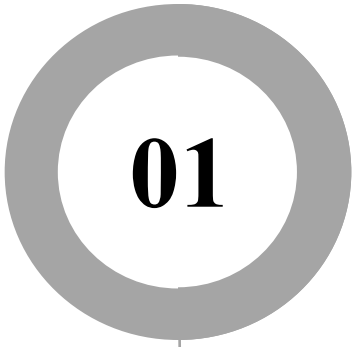
China unicom 中国联通

Guitar Center

SEPHORA

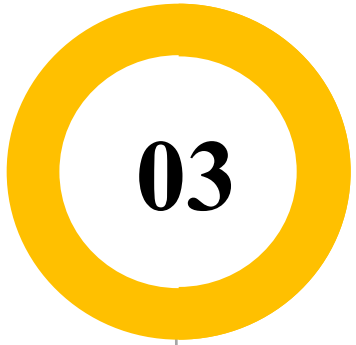
# 大纲

HiBlock 区块链社区

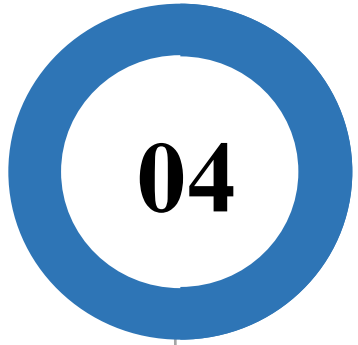



1.Fabric发展现状


2.整体架构

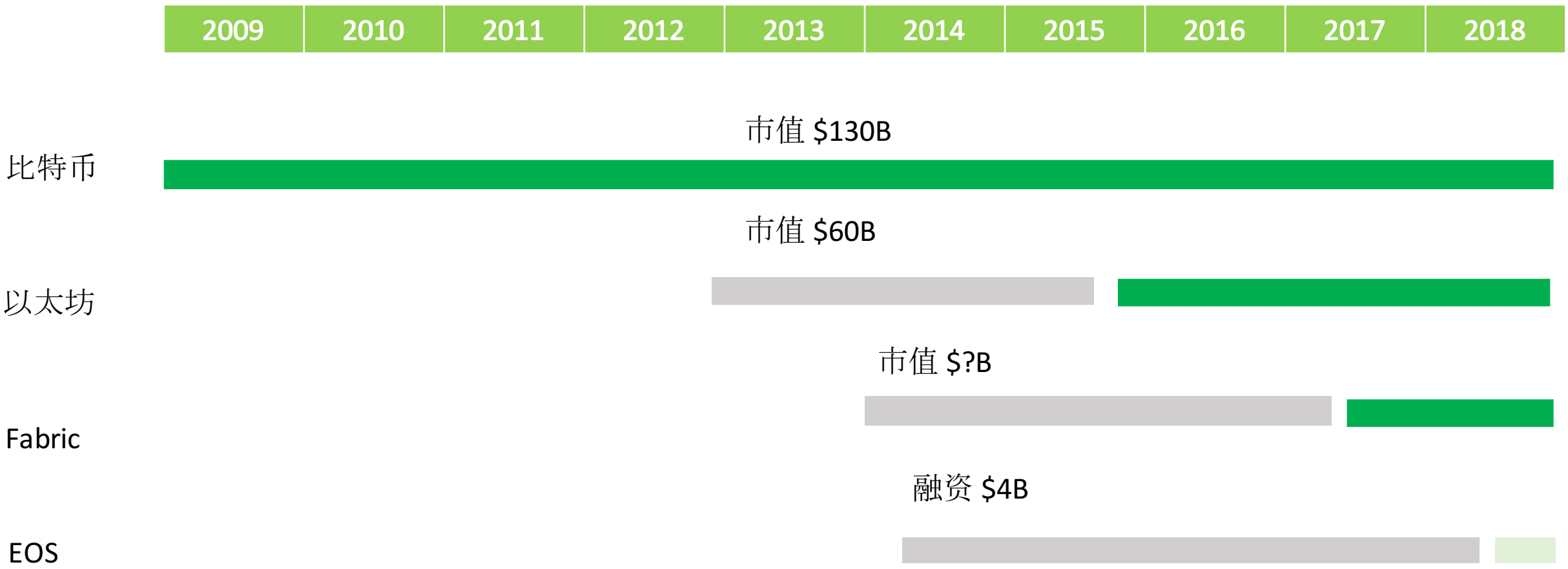



3.FabricMSP模块设计




4.RSA证书支持

# Fabric发展现状


2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
市值 $130B
比特币
市值 $60B
以太坊
市值 $?B
Fabric
融资 $4B
EOS

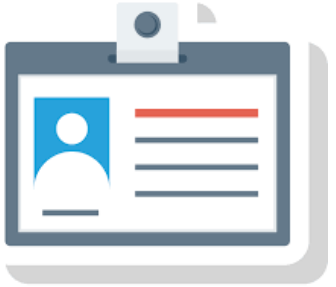
# Fabric特征

不挖矿

没有币


靠权限


靠背书



靠身份

三靠一不一没有

# Fabric特征

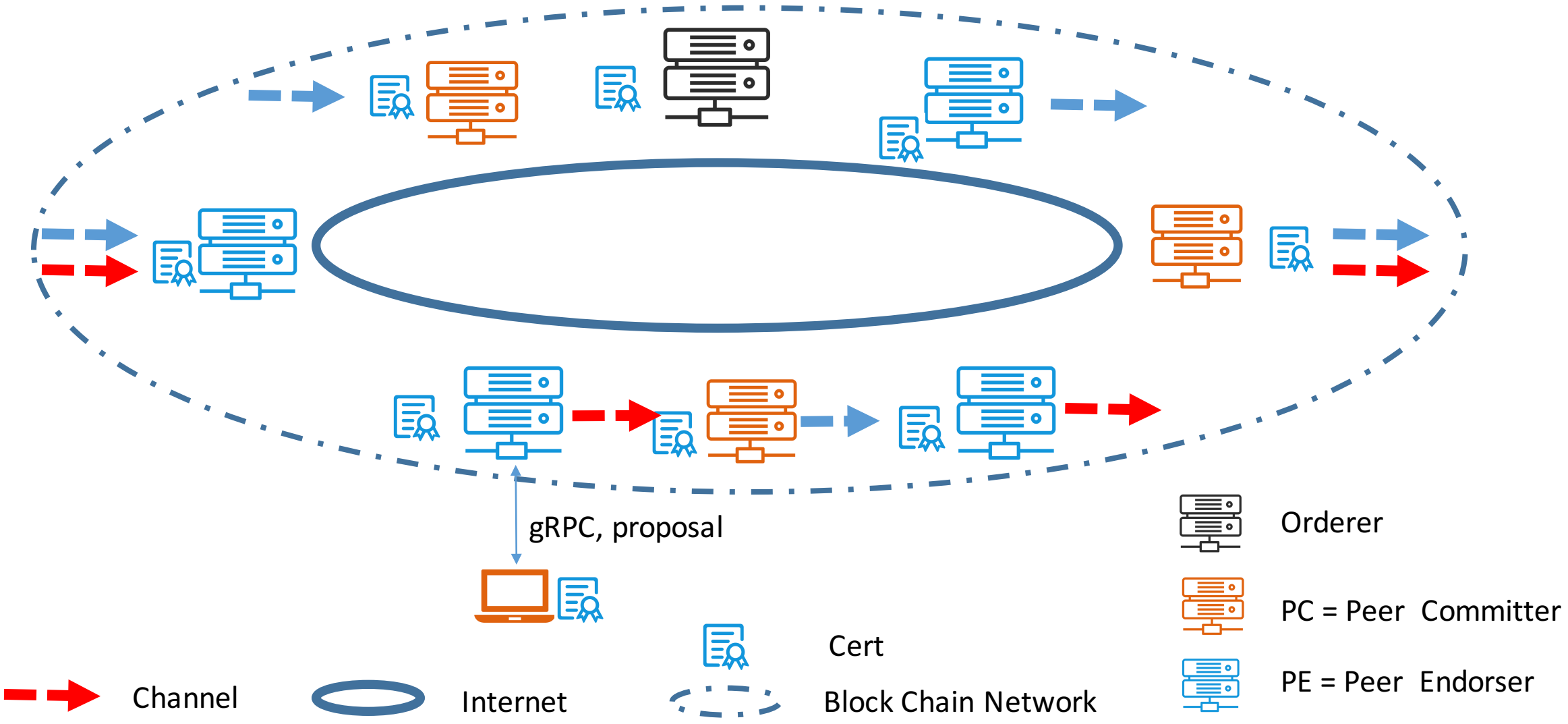
HiBlock 区块链社区

不靠挖矿，就得靠身份

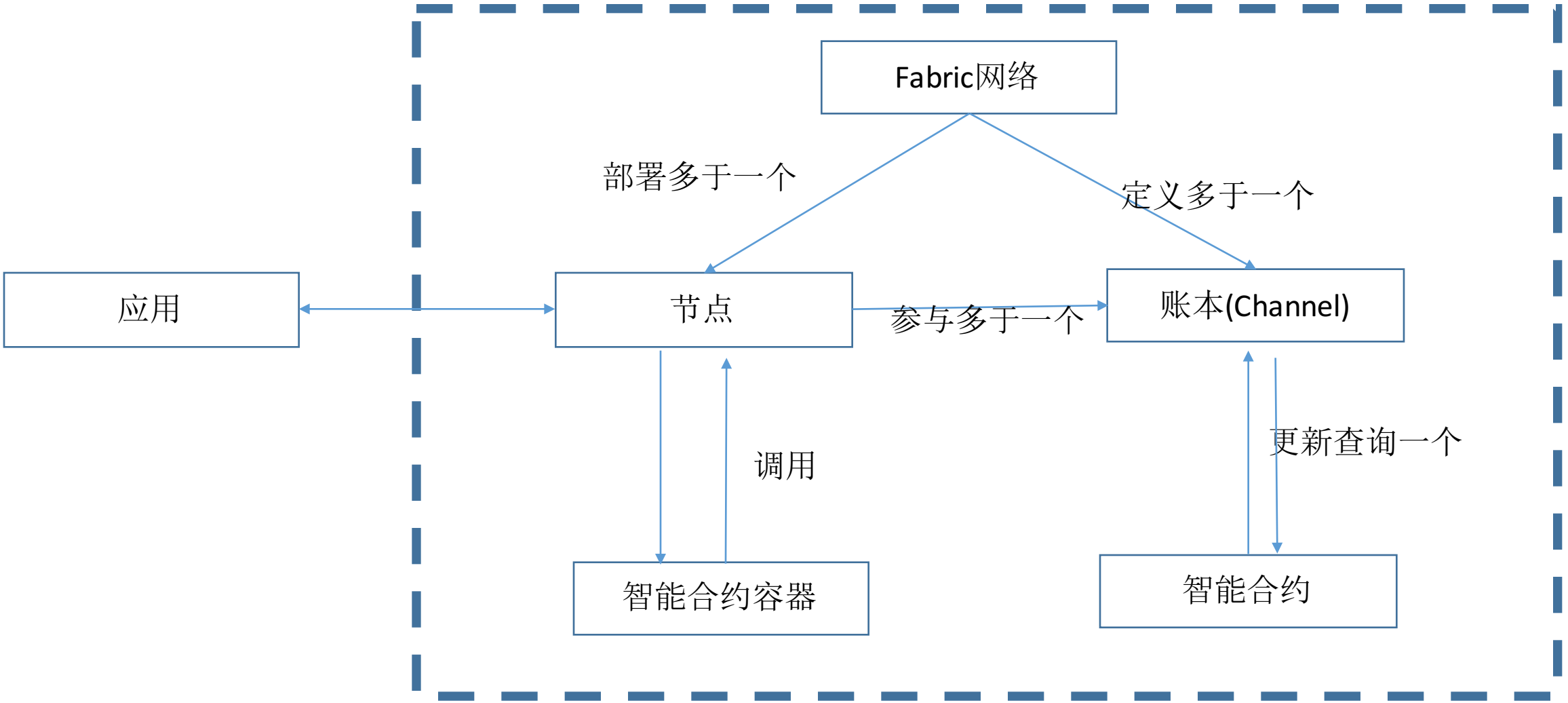
# Fabric整体架构 – 从一个故事说起

简单来说，是这样

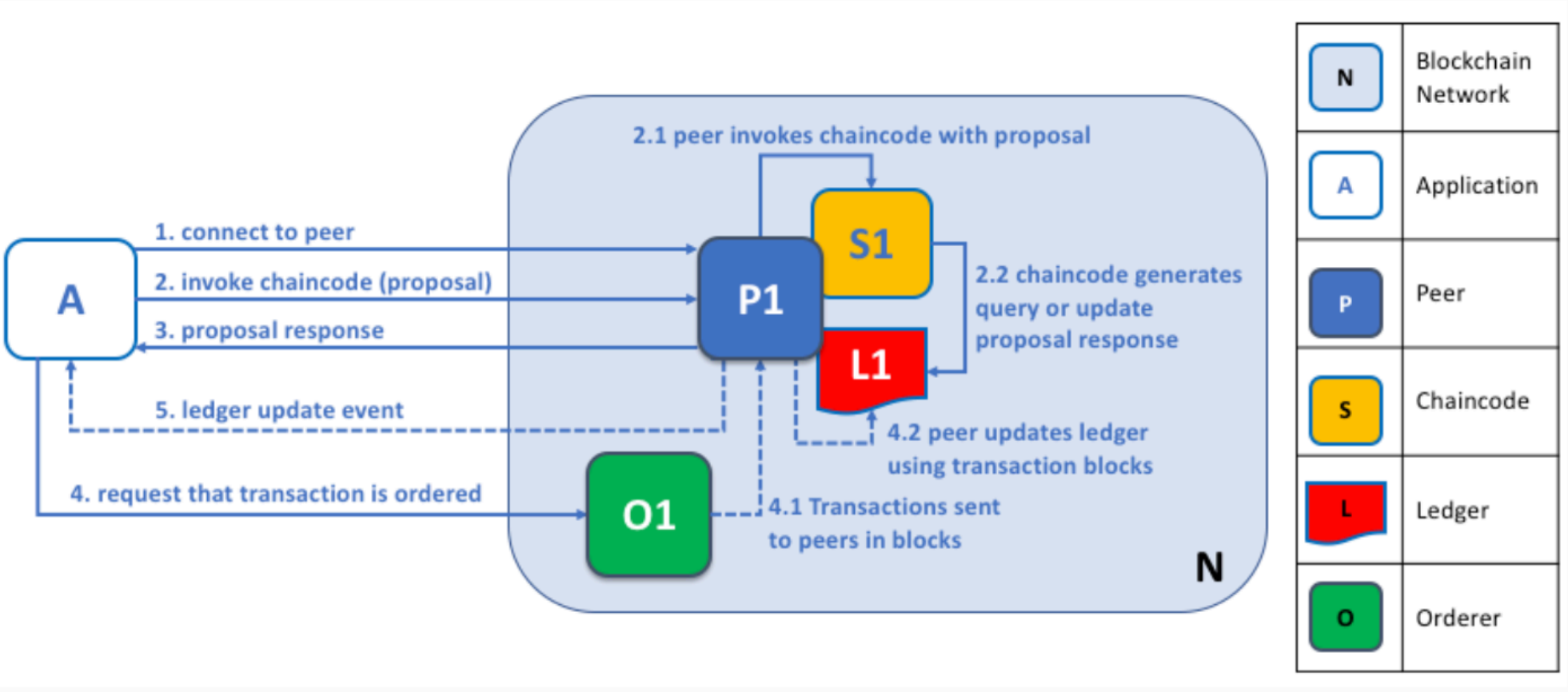
# Fabric运行时架构



# Fabric 语义模型


Fabric网络
部署多于一个
定义多于一个
应用
节点
参与多于一个
账本(Channel)
调用
更新查询一个
智能合约容器
智能合约

# Fabric MSP设计




Ledger = Channel

# 只多说一句

# 上面每个步骤都要用证书
# 谁玩都的要证书

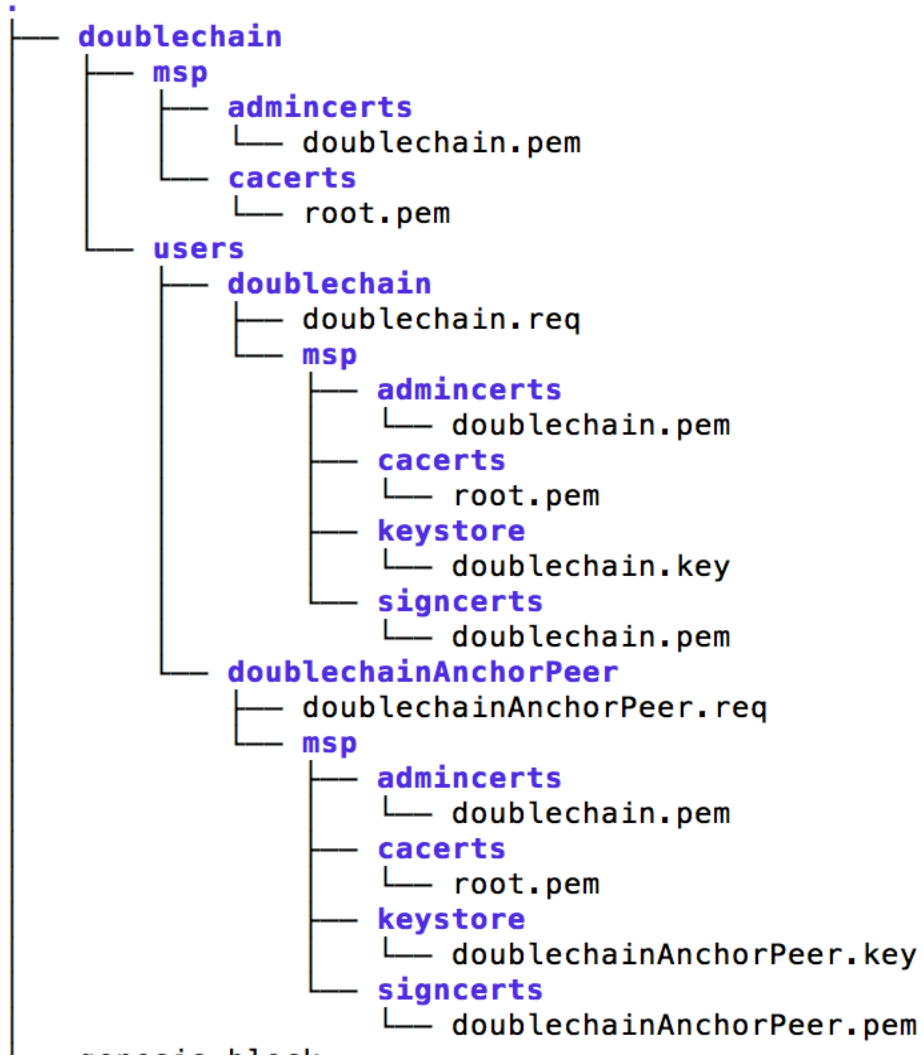
# Fabric 谁都要证，要各种证



- Orderer节点
- Peer节点
- 组织
- 个人
- 应用服务器

- CA证书，根证书，中级证书
- 私钥
- 通信证tcert
- …

# Fabric 我们的实验网的例子



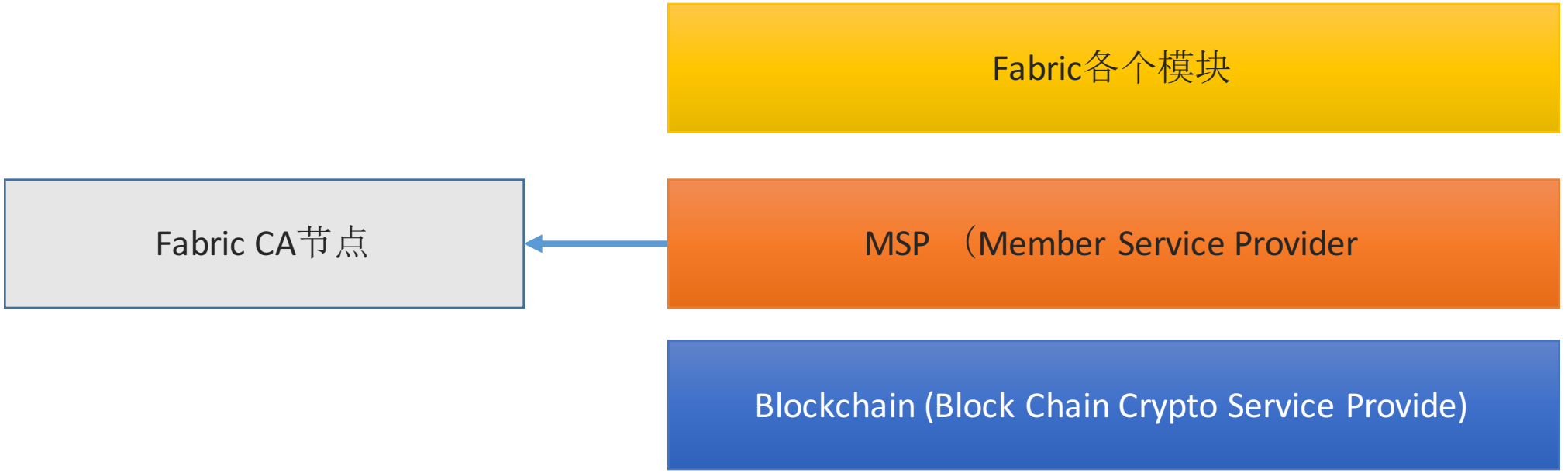

自从知道玩FARBIC之前

还得解PKI体系

整个人都不好了

然而，上面只是一个机构的

# Fabric MSP 模块设计

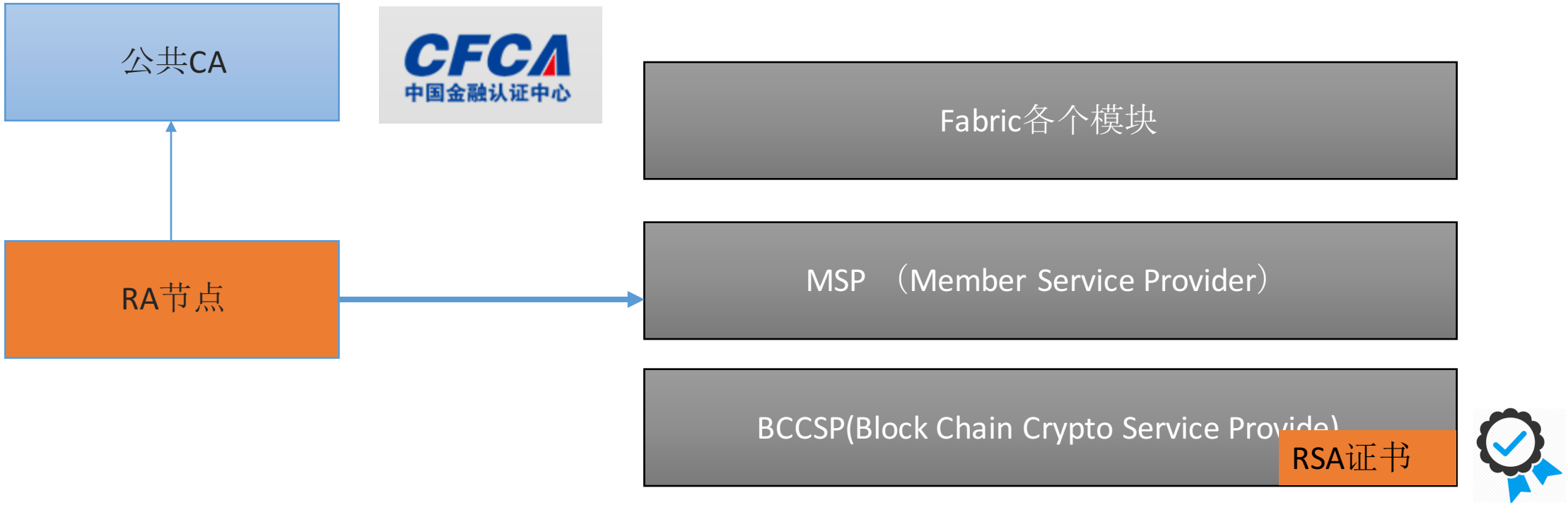


上面那张图的架构中CA只是拿来写论文的

# 自签名CA没有法律支持

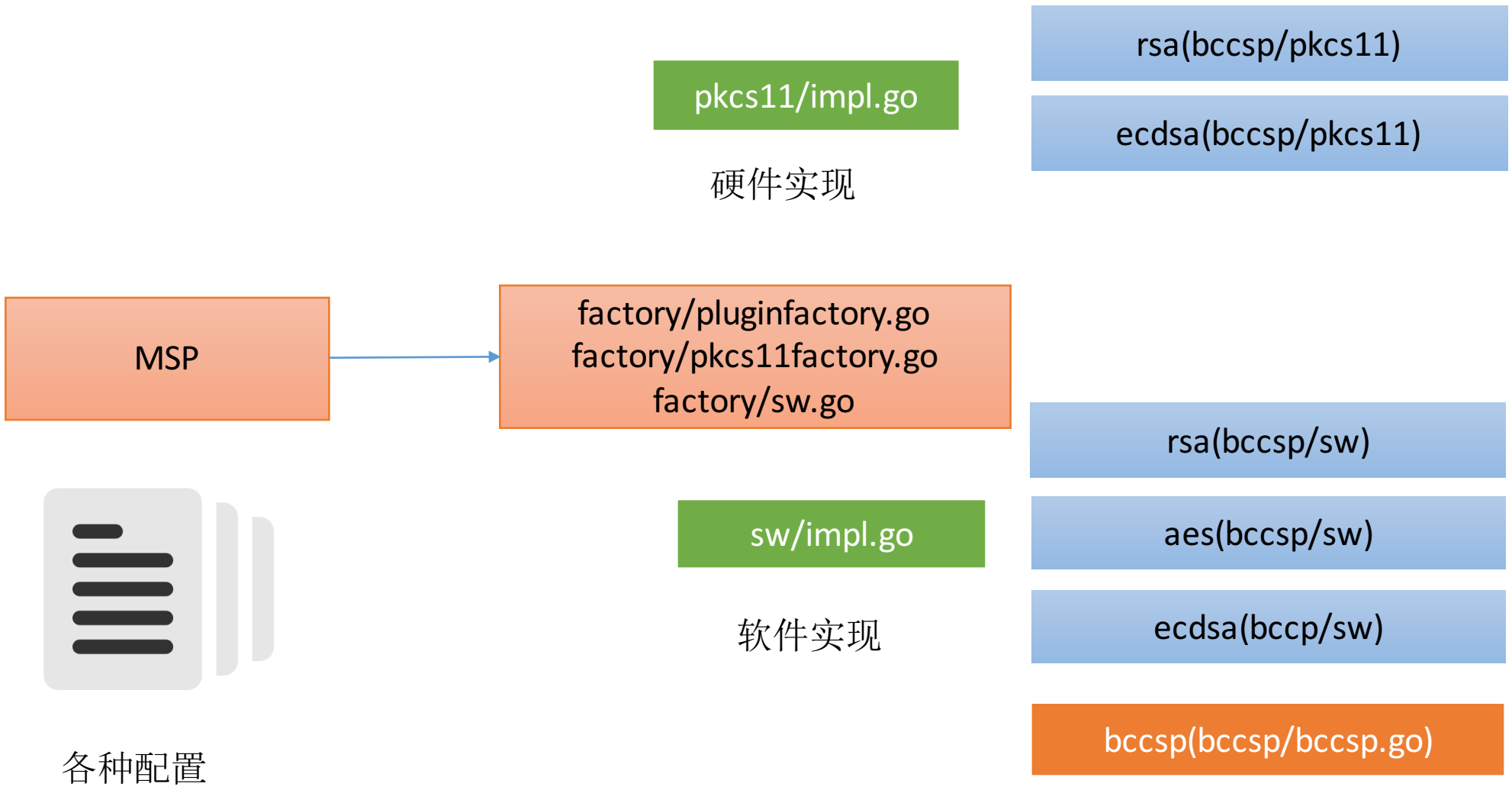
国内没有提供ECDSA证书的机构

# Fabric 最可能的落地方案




橙色部分得自己来

# Fabric 插件结构


rsa(bccsp/pkcs11)
pkcs11/impl.go
ecdsa(bccsp/pkcs11)
硬件实现
MSP
factory/pluginfactory.go
factory/pkcs11factory.go
factory/sw.go
rsa(bccsp/sw)
sw/impl.go
aes(bccsp/sw)
ecdsa(bccp/sw)
软件实现
bccsp(bccsp/bccsp.go)
各种配置

# Fabric BCCSP插件工厂

HiBlock 区块链社区

https://github.com/hyperledger/fabric/blob/master/bccsp/factory/pluginfactory.go

```
55          // attempt to load the library as a plugin
56          plug, err := plugin.Open(config.PluginOpts.Library)
57          if err != nil {
58                  return nil, fmt.Errorf("Failed to load plugin
59          }
60
61          // lookup the required symbol 'New'
62          sym, err := plug.Lookup("New")
63          if err != nil {
64                  return nil, fmt.Errorf("Could not find require
65          }
```

# Fabric 插件实现

参考：Fabric/examples/plugins/bccsp/plugin.go

```
15  type impl struct{}
16
17  // New returns a new instance of the BCCSP implementation
18  func New(config map[string]interface{}) (bccsp.BCCSP, error) {
19          return &impl{}, nil
20  }
21
```

然后实现BCCSP定义的方法

KeyGen
KeyDeriv
KeyImporter
GetKey
Hash
GetHash
Sign
Verify
Decrypt

# Fabric特征

上面的内容只是覆盖了Fabric的一小部分

HiBlock
区块链社区

扫码关注HiBlock公众号
一起研究区块链技术

# 谢谢！