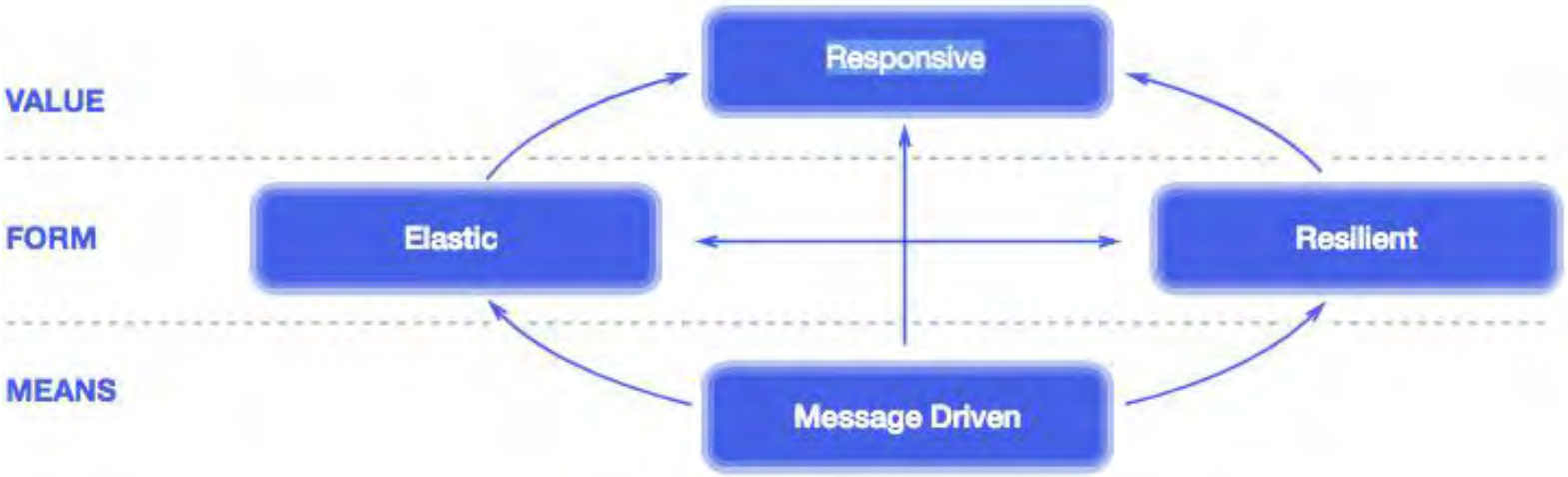
BDTC 2017 中国大数据技术大会
Big Data Technology Conference 2017

RepChain
轻量许可链的实现和应用实践

RepChain是什么

- Re 即Reactive，采用Actor模型实现的响应式编程
- p 即Permission，采用身份许可的准入机制，节点之间使用TLS安全通信
- Chain 即区块链
- RepChain是第一个采用**响应式编程**实现的**许可链**基础组件



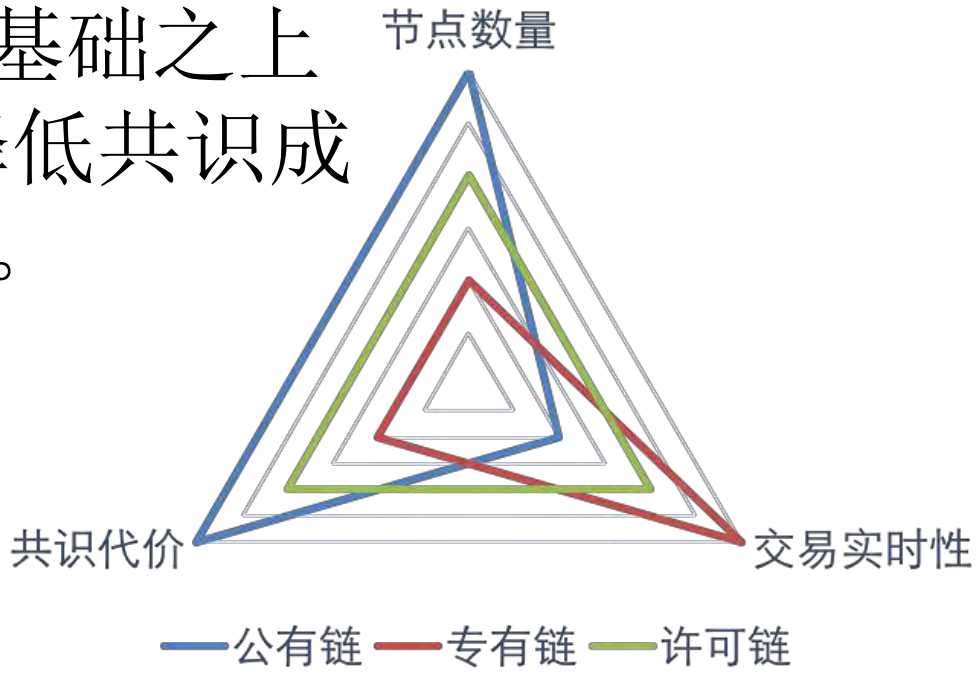
（引自《The Reactive Manifesto》）

内容一览

- 为什么采用许可链
- 场景对话RepChain
- 系统组成和特点
- 演示
  - 平台演示：4节点组网的资产管理
  - 应用演示：跨终端的图片存证应用

为什么采用**身份准入**的许可链？

许可链在身份准入的基础之上建立TLS安全信道，降低共识成本，提高交易实时性。



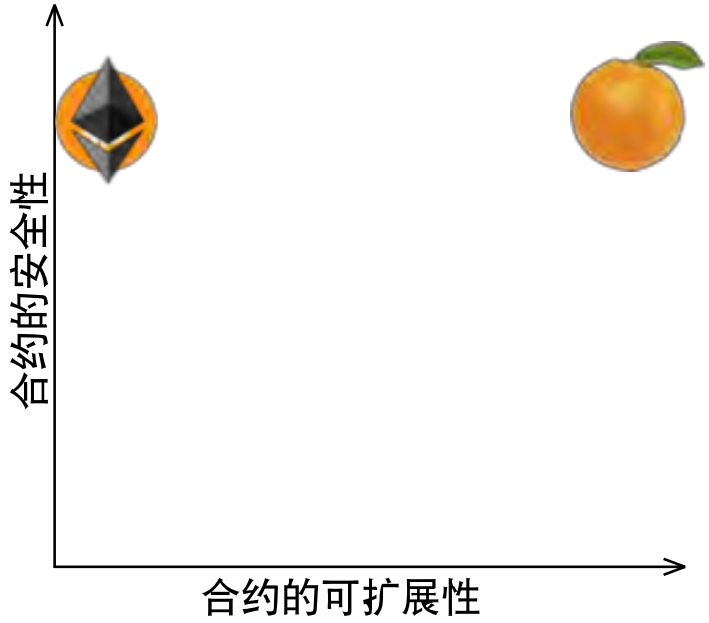
区块链分类——系统组成

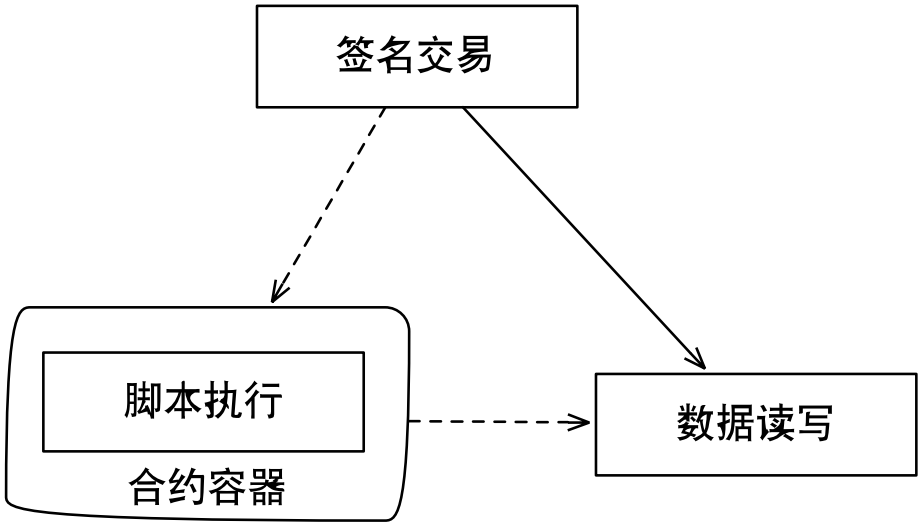
	公有链	联盟链	专有链
智能合约层	✓	?	
激励层	✓		
共识层	✓	✓	
网络层	✓	✓	
数据层	✓	✓	✓

联盟链需要“智能”合约吗？

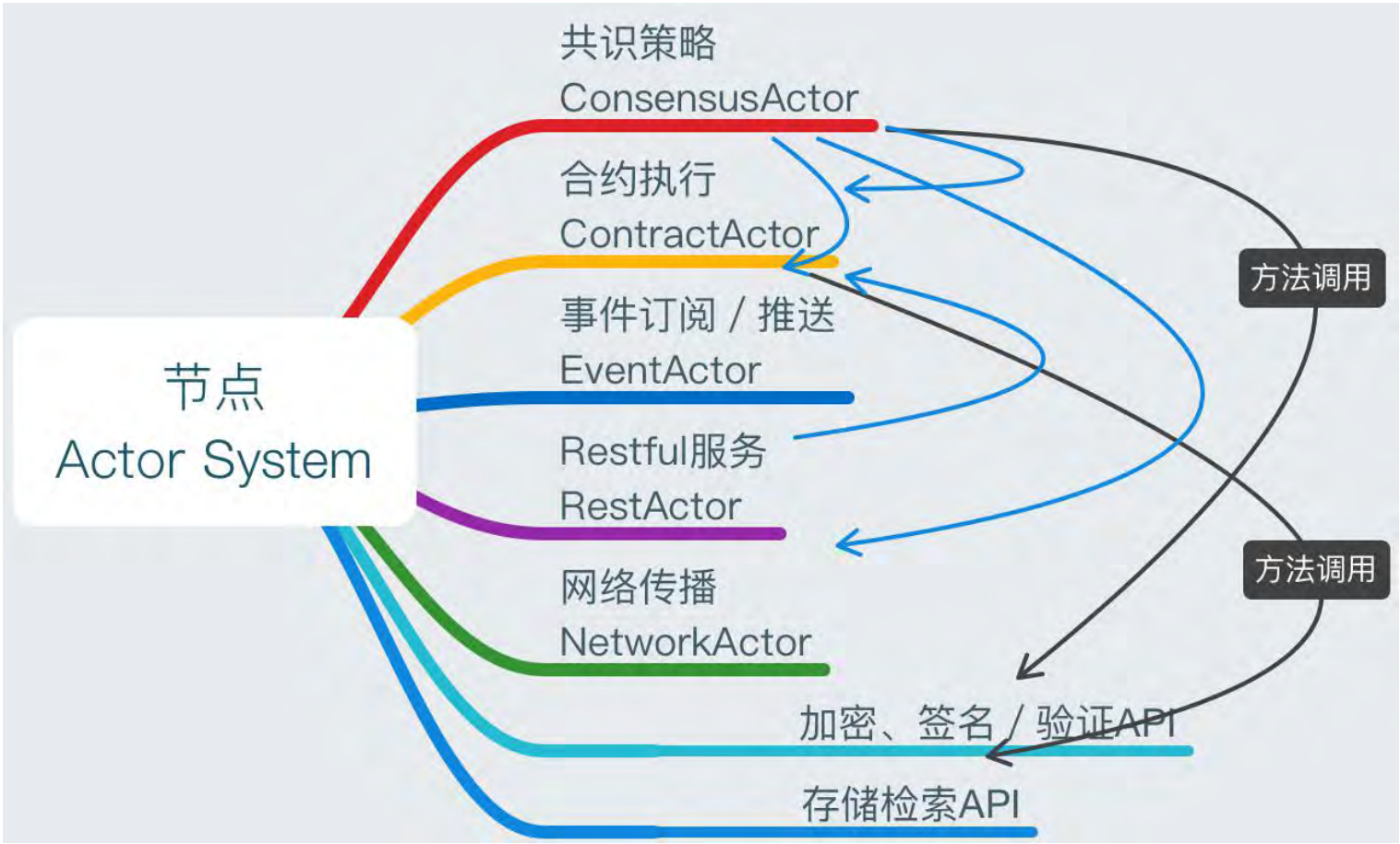
- 以太坊必须“智能”，否则就是又一个山寨币

- 一链多用的联盟链，保留智能合约机制
- 专链专用的联盟链，不妨“非智能”或去合约化



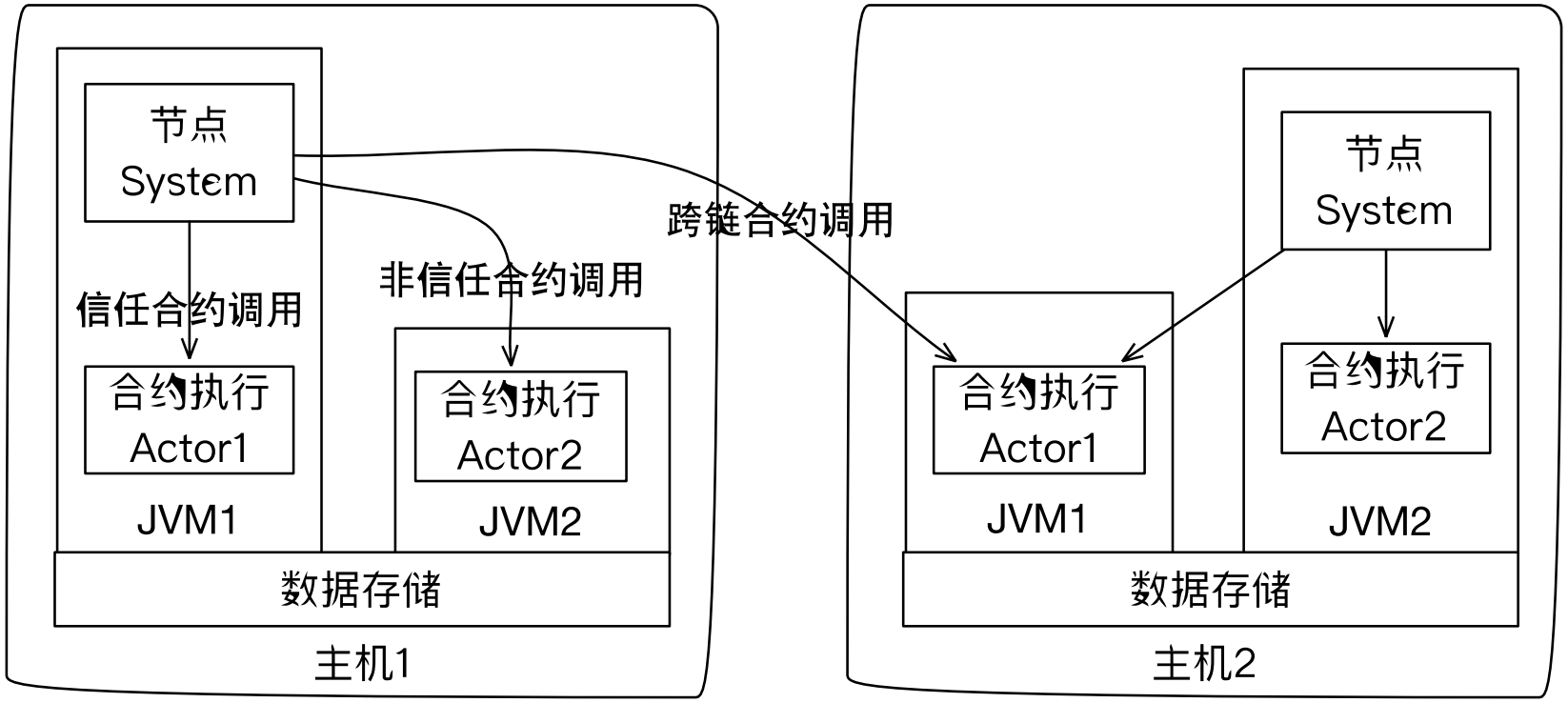


机构用户：我希望区块链基础组件模块化，允许根据场景替换甚至去掉某些模块。



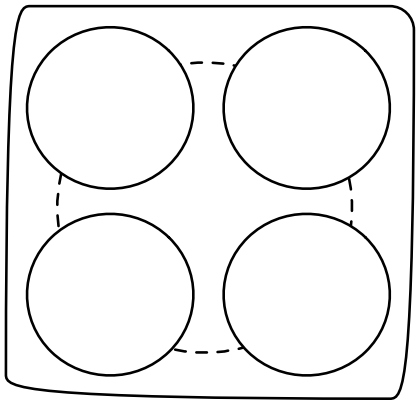
RepChain：消息驱动，最适合松耦合的模块化封装

架构师：我要针对不同的合约类型，采用不同的执行策略，还要支持跨链合约调用

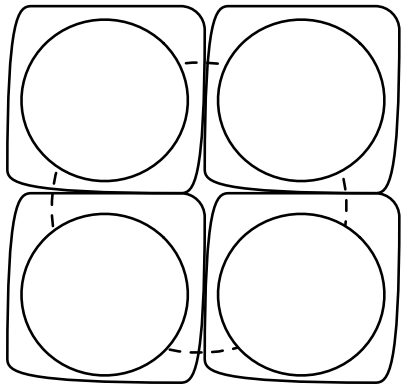


RepChain：利用Actor位置透明性，合约调用代码不用关心合约部署的位置。

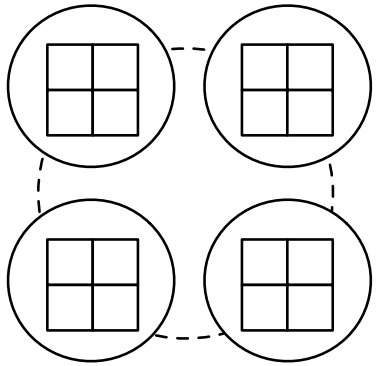
开发人员：能否支持单机开发调试，分布式部署运行？



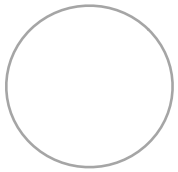
开发调试模式
单主机运行多个组网节点



低频交易的部署模式
单主机运行单个组网节点



高频交易的BAAS模式
节点使用跨主机的Actor集群



节点

主机

组网

RepChain：Actor具有位置透明的特性；而且内存占用小，您甚至可以在单机仿真大规模组网或集群的分布式协同

运维人员：我希望节点算力能够根据负载自动伸缩，
让我每天都能睡个好觉

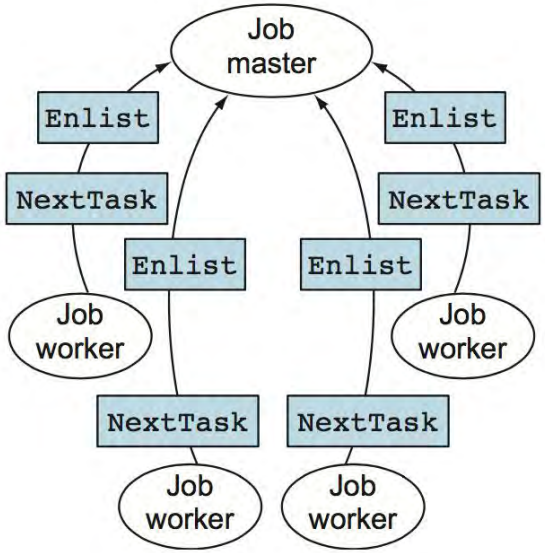


Figure 14.14 JobWorker enlists itself and requests NextTask

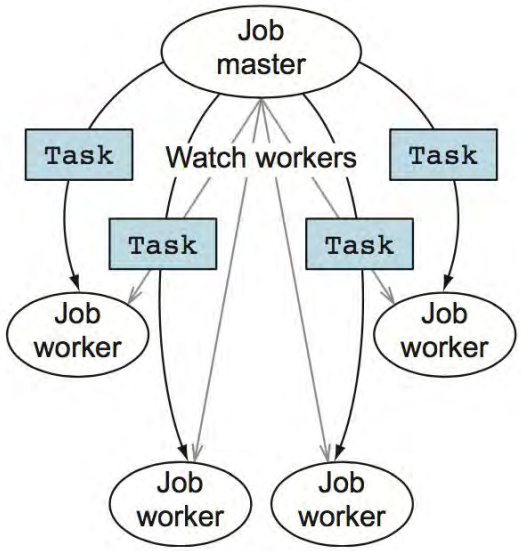


Figure 14.15 JobMaster sends Tasks to JobWorkers and watches them

（引自《Manning.Akka.in.Action》）

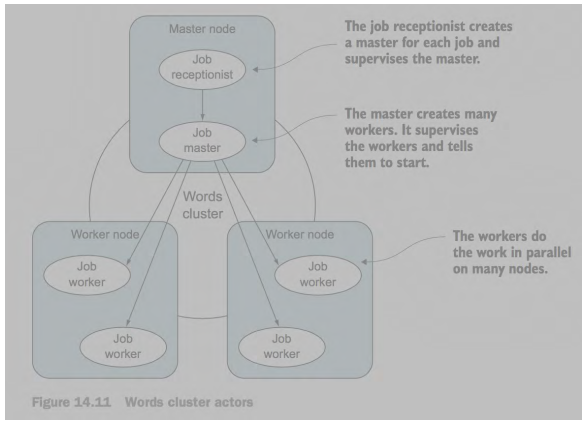


Figure 14.11 Words cluster actors

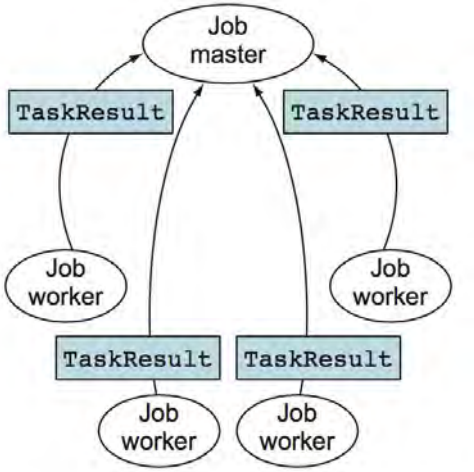
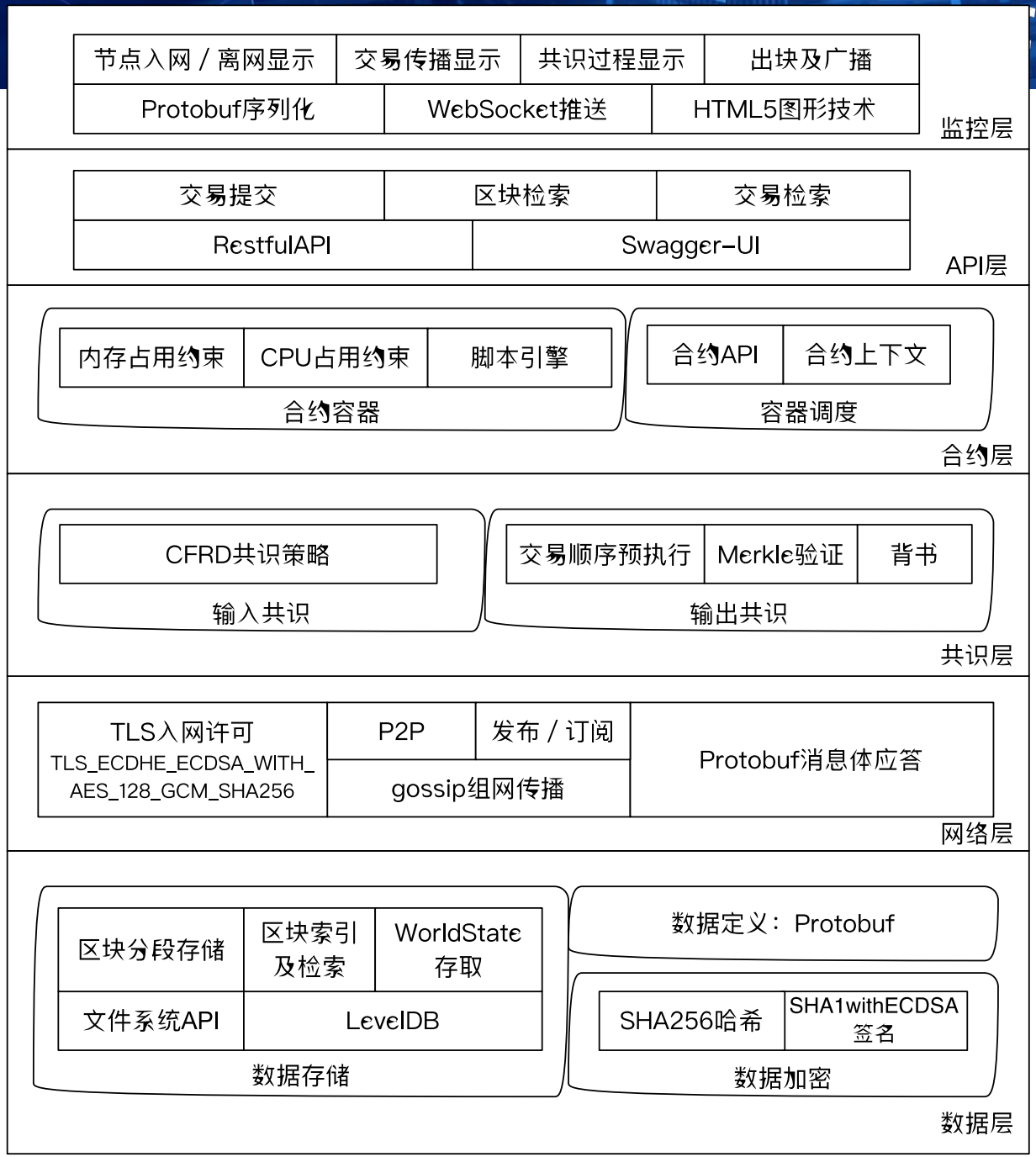


Figure 14.16 JobWorker processes Task and sends back TaskResult

RepChain：对可能的瓶颈环节使用Actor集群

小结

- RepChain采用响应式编程，能有效解决区块链实施中的常见问题


节点入网 / 离网显示
交易传播显示
共识过程显示
出块及广播
Protobuf序列化
WebSocket推送
HTML5图形技术
监控层
交易提交
区块检索
交易检索
RestfulAPI
Swagger-UI
API层
内存占用约束
CPU占用约束
脚本引擎
合约容器
合约API
合约上下文
容器调度
合约层
CFRD共识策略
输入共识
交易顺序预执行
Merkle验证
背书
输出共识
共识层
TLS入网许可
TLS_ECDHE_ECDSA_WITH_
AES_128_GCM_SHA256
P2P
发布 / 订阅
gossip组网传播
Protobuf消息体应答
网络层
区块分段存储
区块索引
及检索
WorldState
存取
文件系统API
LevelDB
数据存储
数据定义：Protobuf
SHA256哈希
SHA1withECDSA
签名
数据加密
数据层

RepChain的特点

- 轻巧（场景交集做加法）
  - 源代码体量小
  - 资源占用小，单机可仿真100节点组网
  - 出块迅速：CFRD共识算法，提高了交易的实时性
  - 合约容器轻：用Actor封装，可使用独立的JVM隔离
  - 跨平台、部署方便
- 稳定
  - java生态圈成熟
  - 加密／验证采用JDK工具库，可替换为国密算法
  - 去中心化组网采用经过工程实践检验的组件
- 可信
  - 身份准入与TLS安全通信
  - 图形化的实时状态显示及日志回放（眼见为实）

平台演示—资产管理

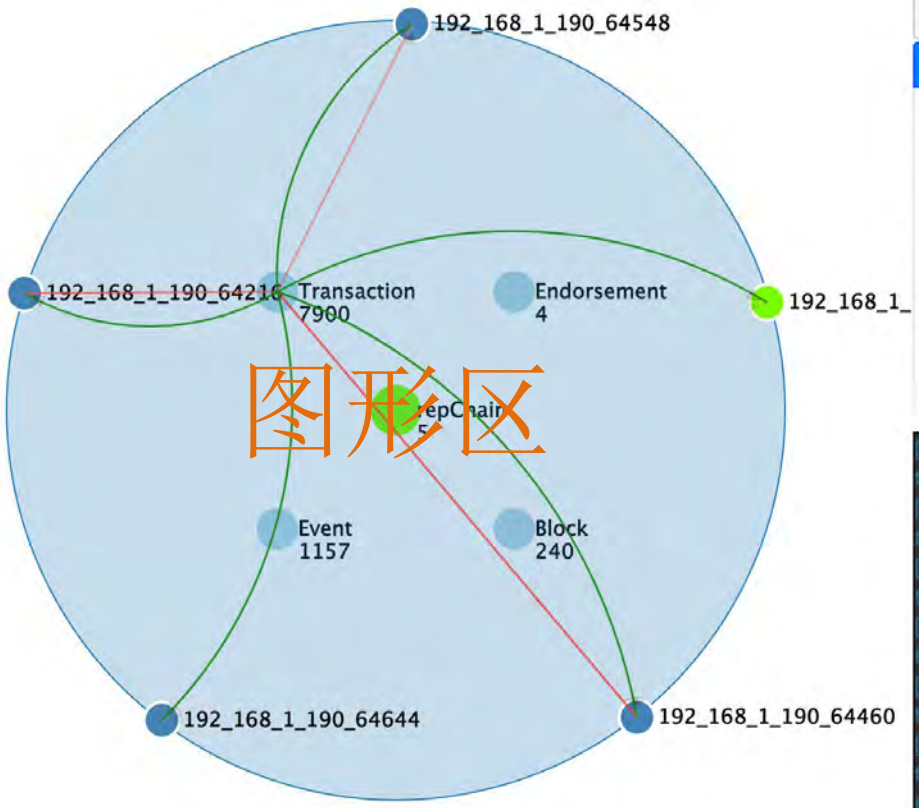
① 4个节点配置各自密钥对、信任证书列表、seed-nodes

② 初始节点加载定义JSON文件，生成创世块
- 创世块中部署资产初始化和资产转移合约
- 创世块中为账户分配初始资产

③ 节点入网根据区块高度同步数据
- 区块同步
- WorldState同步

④ 节点定时发起资产转移交易

平台—实时状态显示


192_168_1_190_64548
192_168_1_190_64216
Transaction
7900
Endorsement
4
192_168_1_
Event
1157
Block
240
192_168_1_190_64644
192_168_1_190_64460
图形区


Block240 2017/7/21 下午1:58:19
Block239 2017/7/21 下午1:57:29
Block238 2017/7/21 下午1:56:39
Block237 2017/7/21 下午1:55:49
前块哈希值:
本块交易数: 33
d91ef260-6dbd-11e7-8d72-5d14a4895cf4
d9bd5540-6dbd-11e7-8d72-5d14a4895cf4
da792b30-6dbd-11e7-8d72-5d14a4895cf4
daf31620-6dbd-11e7-8d72-5d14a4895cf4
db904080-6dbd-11e7-8d72-5d14a4895cf4
dcb586a0-6dbd-11e7-8d72-5d14a4895cf4
dd541090-6dbd-11e7-8d72-5d14a4895cf4
de0f9860-6dbd-11e7-8d72-5d14a4895cf4
块堆栈区


[下午1:58:48] Received: 1 from:Transaction
to:akka.ssl.tcp://repChain_@192.168.1.190:64339/user/pm_2/trans#1609610165
[下午1:58:48] Received: 1 from:Transaction
to:akka.ssl.tcp://repChain_@192.168.1.190:64216/user/pm_1/trans#-32634835
[下午1:58:48] Received: 1 from:Transaction
to:akka.ssl.tcp://repChain_@192.168.1.190:64548/user/pm_4/trans#-1281444764
[下午1:58:48] Received: 1 from:Transaction
[下午1:58:48] Received: 1 from:Transaction
[下午1:58:48] Received: 1
from:akka.ssl.tcp://repChain_@192.168.1.190:64644/user/pm_5/trans#1260246525
to:Transaction
[下午1:58:48] Received: 1 from:Transaction
to:akka.ssl.tcp://repChain_@192.168.1.190:64644/user/pm_5/trans#1260246525
[下午1:58:48] Received: 1 from:Transaction
日志区

平台—Swagger-UI API

block

chaininfo

GET /chaininfo 返回块链信息

system

GET /system/start/{startCount} 启动System

GET /system/stop/{stopFrom}/{stopTo} 停止System

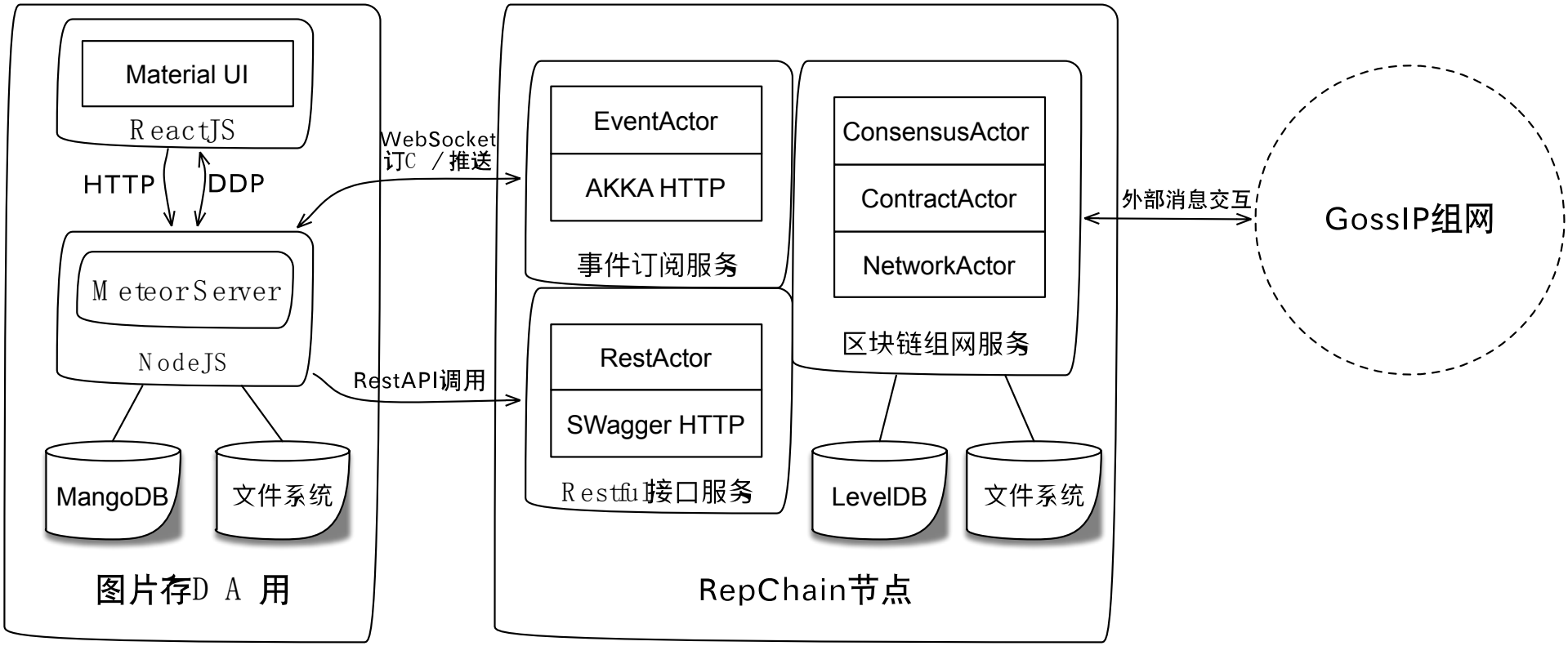
transaction

GET /transaction/{transactionId} 返回指定id的交易

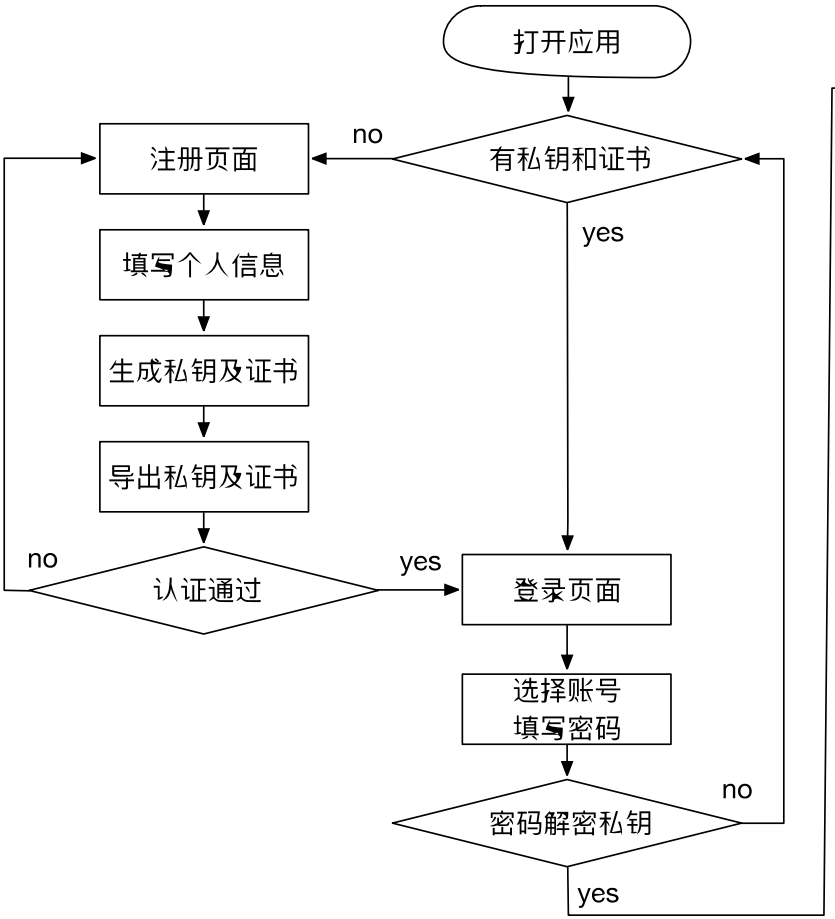
POST /transaction 提交交易

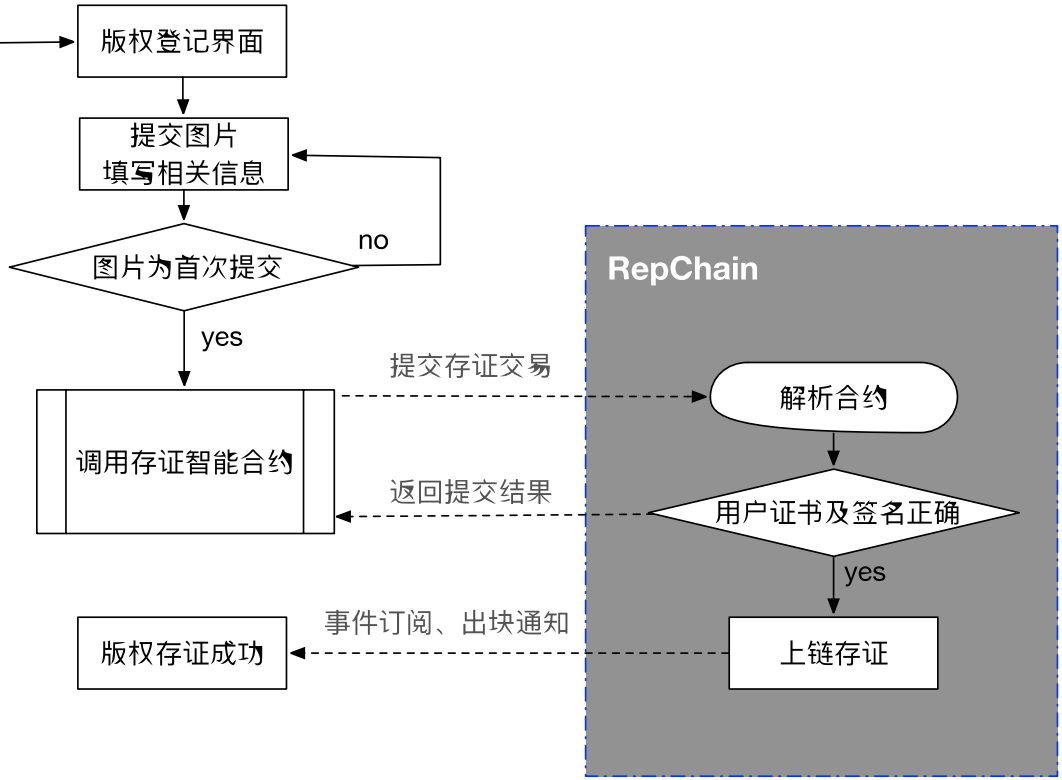

localhost:8081/web/g1.html
Animation
Transaction
2
Endorsement
repChain
Event
Block
1

应用演示—图片版权存证技术架构



应用演示—图片版权存证流程



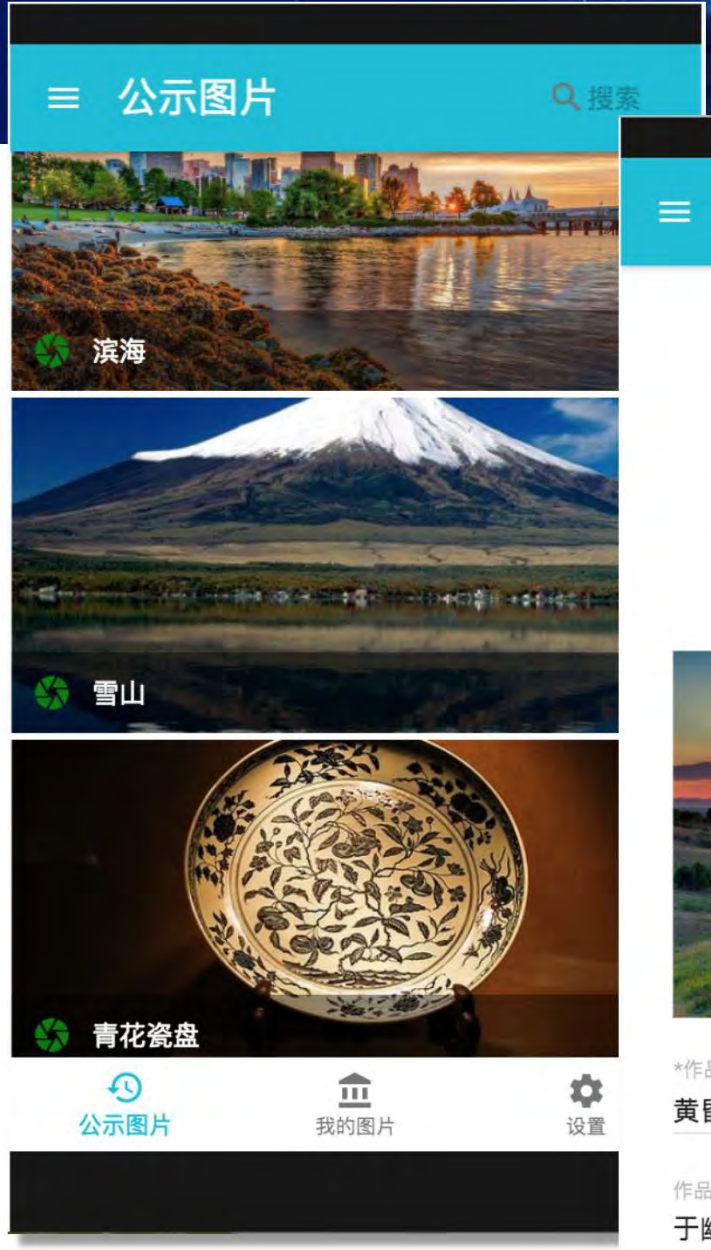


账户管理

图片存证


返回登录
注册
1 注册方式
选择注册方式
1. 您可以生成新的私钥文件及对应的证书文件
2. 您也可以导入已有的私钥文件及其对应的证书文件
新建
导入
下一步
2 新建
3 账户生成
新建信息
xyz@x.com
输入通讯住址
北京市海淀区中关村南四街四号
输入工作单位名称
中国科学院软件研究所软件发展研究部
输入密码以保护用户私钥
输入密码
再次输入密码
确认
取消
设置
侯 子默
TEL: 39138472619
账户地址
1TUT4AMTFHQB9EJLBP8TQOST3YSHQ
认证日期
2017/11/29 下午5:56:22
查看证书
导出证书
更改证书
公示图片
我的图片
设置

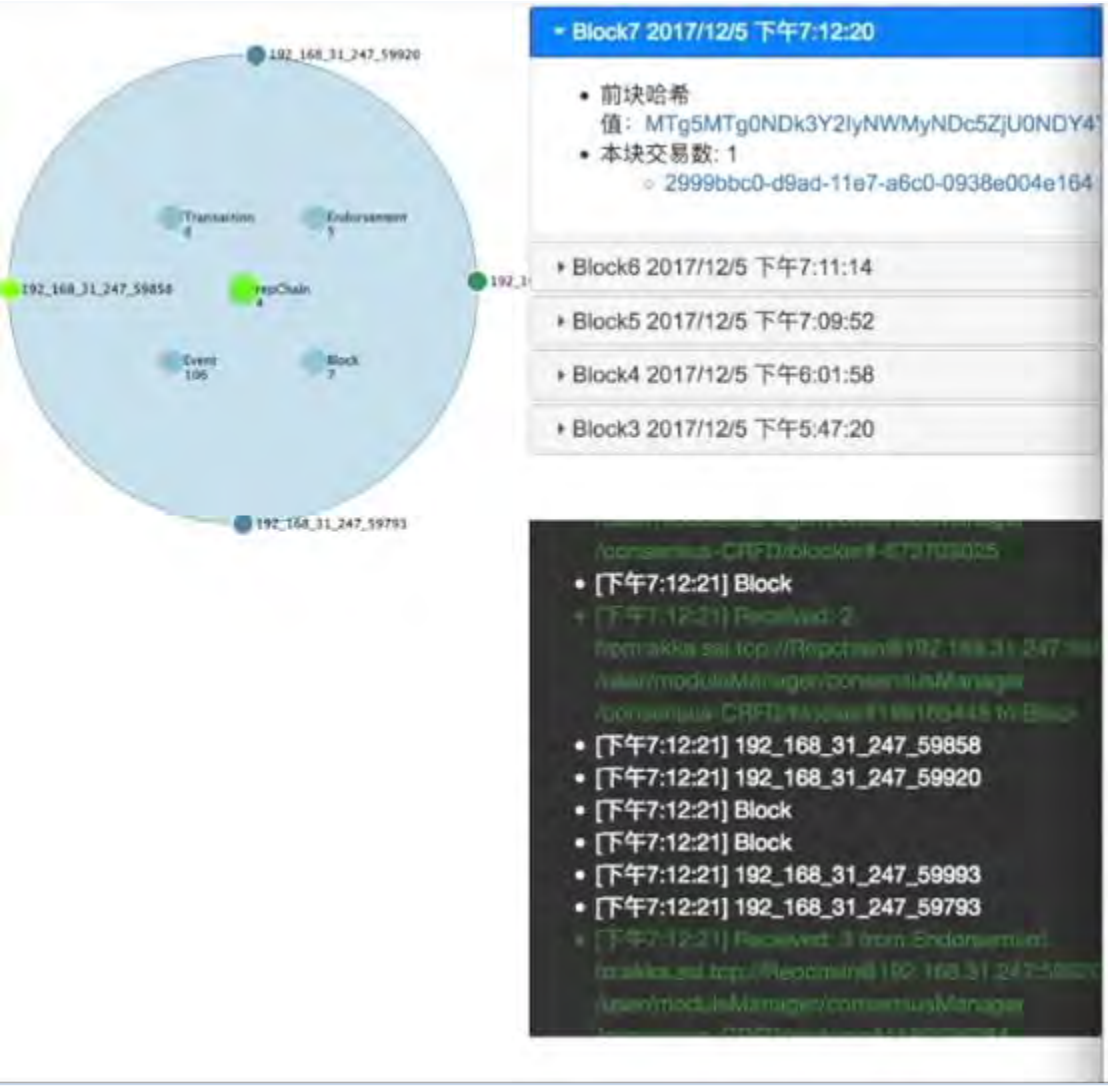
账户管理


公示图片
搜索
滨海
雪山
青花瓷盘
公示图片
我的图片
设置


登记作品
+将上传图片拽到此处,
或点击此处选择图片
上传了1张图
*作品名称
黄昏夕阳
作品描述
于幽静山丘观落日所摄


版权信息
版权登记证书
登记编号:
fd922b20-d57e-11e7-ac18-8d48e5d0bbc9
图片标识:
4ab31f7d0f13a5032482cc097020f3f41c55892ab0ded2f
bf0ba350740ba26fa
作品名称: 黄昏夕阳
作者: 候子默
著作权人: 侯 子默
著作权人编号:
1TUT4AMTFHQB9EJLBP8TQOST3YSHQ
证书状态: 已上链确认
登记时间: 2017-11-30T19:31:46+08:00

图片存证


192_168_31_247_59920
192_168_31_247_59858
192_168_31_247_59793
Block7 2017/12/5 下午7:12:20
前块哈希
值：MTg5MTg0NDk3Y2IyNWMyNDc5ZjU0NDY4
本块交易数: 1
2999bbc0-d9ad-11e7-a6c0-0938e004e164
Block6 2017/12/5 下午7:11:14
Block5 2017/12/5 下午7:09:52
Block4 2017/12/5 下午6:01:58
Block3 2017/12/5 下午5:47:20
[下午7:12:21] Block
[下午7:12:21] 192_168_31_247_59858
[下午7:12:21] 192_168_31_247_59920
[下午7:12:21] Block
[下午7:12:21] Block
[下午7:12:21] 192_168_31_247_59993
[下午7:12:21] 192_168_31_247_59793
登录

RepChain面向工程实践，
是轻量化、模块化、可视化，
并易于集成的区块链基础组件。
欢迎大家共同探讨！

BDTC 2017 中国大数据技术大会
Big Data Technology Conference 2017

实践中遇到的一些问题及心得

- JDK内置脚本引擎性能拖累了TPS
- 序列化的性能问题✓
- 消息耦合要适度✓
- 证书体积大✓
- NodeJS的加密／验证与JDK对接顺利✓