基于区块链的扶贫资金管理平台关键技术的研究与设计

导师： 马小峰　　答辩人： 李一鸣

论文背景

Contents

选题来源：

本文选题来源于2017年贵州省大扶贫工程项目，参与方有贵州省政府、同济大学、工商银行。该项目是央行法定数字货币应用探索项目。

项目痛点：

痛点1：业务层级过多，信用可达性和管理有效性逐级衰减，监管难度增加。

痛点2：无法实时、全面的了解扶贫资金的使用情况。

解决方案：

区块链简介

What is Blcokchain

一句话区块链是什么

区块链是一个分布式的数据库。

1

2

数据以区块的形式存储，每个区块之间有相互耦合，牵一发而动全身，因此有了不可篡改的特性。

在这个分布式的数据库中，每个节点存储的信息是一样的，因此具有透明性和去中心化的特点。

3

4

为了保障每个节点的信息是一致的，在一个去中心化的体系下，就有了共识机制，挖矿就是其中的一种。

PRESENT

目录

Contents

数字汇票体系

——保障扶贫资金的权威性和信用可达性

实时对账系统

——实时流水对账，及时发现对账差异.

共识机制

——基于信用评分的主节点切换协议的CBFT共识算法

多链架构

——多链架构，提高区块链的系统吞吐量

典型共识算法分析

Algorithm for Distributed Consensus

PoW、PoS、DpoS...

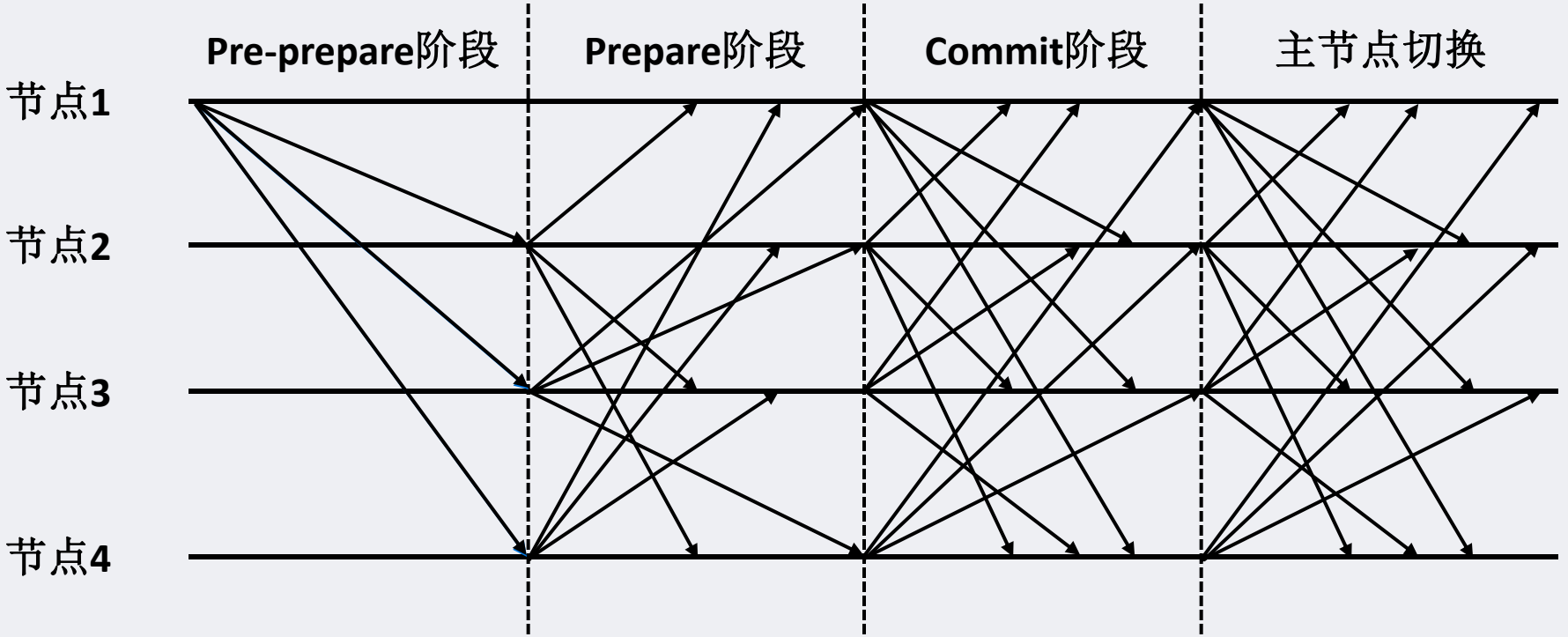
Raft、Paxos、Zab、Pbft...

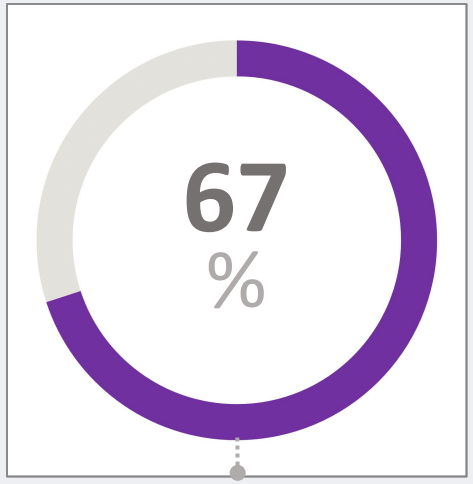
资源浪费、效率较低！

存在安全隐患！

共识算法

Algorithm for Distributed Consensus





容错率

在保证系统活性和安全性的前提下，可以容忍系统中有33%的节点是拜占庭节点。

01

3f+1容错机制

符号说明：

N ：分布式的系统中节点的个数。

f ：分布式的系统中拜占庭节点的个数。

约束条件：

活性：一定能在有限的时间内做出判断

安全性：做出的判断一定要保证其正确性

关系证明：

极端情况1：f 个拜占庭节点收到消息后不回复；为了保证系统的安全性，系统必须在收到 $N-f$ 个回复后作出判断。

由此推导出=》系统判断阈值：$\varphi = N-f$

极端情况2：在收到的前 $N-f$ 个回复中有 f 个回复来自拜占庭节点，为了保证系统的安全性，好节点的回复个数要大于拜占庭节点回复的个数，即：$\varphi - f > f$，由此推导出：$N > 3f$ 。又因为：$\lim_{n\to+\infty} \frac{2f+1}{3f+1} \approx 0.67$，所以算法的容错率为67%。

02

主节点切换协议

该协议针对主节点在打包交易时故意不将特定交易打包进来的作恶方式提出的对抗方案。

1.信用评价机制：

指标1：共识是否成功。成功：S_s分，失败：S_f分。

指标2：下一论共识时，打包区块中是否包含交易时间小于打包时间的交易。无：S_s分，有：S_f分。

由此定义节点评价函数：$S_i = \dfrac{S_i \times (c-1) + S_i'}{c}$

2.主节点选择策略：

主节点按概率产生，每个节点被选中为主节点的概率与其评价函数大小成正比。具体操作如下：

（1）计算每个节点被选中的概率：$P_i = \dfrac{S_i}{\sum_{j=1}^{N} S_j}$

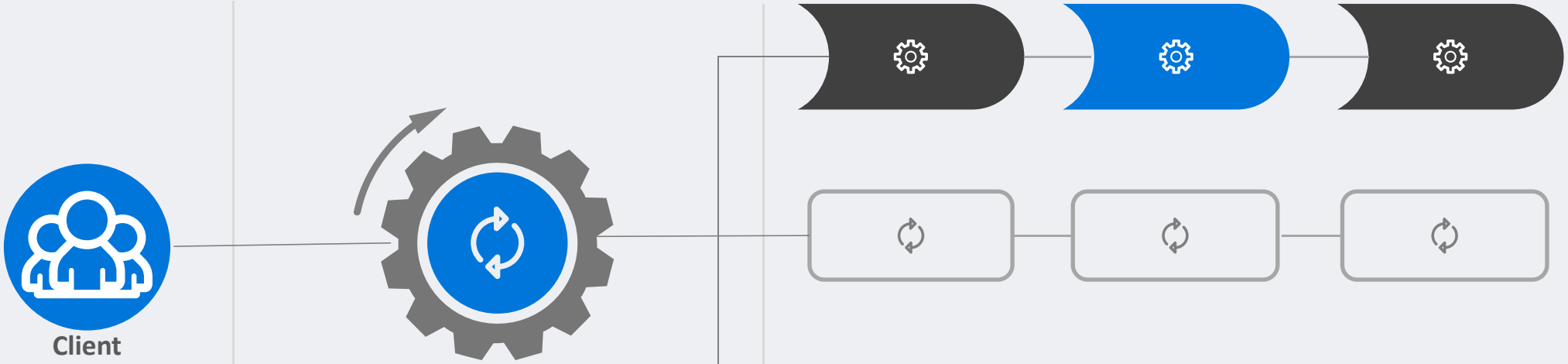
（2）计算出每个节点的累积概率：$q_i = \sum_{j=1}^{i} P_j$

（3）在区间内产生一个均匀分布的随机数 $random$，若 $random < q_1$，则选择节点1为下一阶段共识的主节点，否则，选择节点k，使得 $q_{k-1} < random \le q_k$ 成立。

通过调节 S_s 和 S_f 的参数，可以控制主节点的作恶概率为：$\dfrac{S_f}{S_s}$ 。

多链架构

Multi-chain Construction



获取路由策略

客户端向中继层发送请求，路由模块调用主链的路由管理合约，获取路由分配策略。

子链转发

根据获取的路由策略，将请求转发至指定子链，子链会立刻返回请求的摘要，中继层缓存该摘要，用以异步回调。

子链执行

子链执行请求，执行完成后，将请求摘要和执行结果返回到中基层。

主链确认

路由模块收到回复后，根据请求摘要，寻找对应对调，并将结果确认在主链上。

测试环境

Testing Environment

硬件环境

本文实验硬件采用4核8线程，Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz处理器，8G内存的服务器。

软件环境

- Docker - v18.02.0
- Docker Compose - v1.16.1
- Node.js - v6.9.5
- Linux - v3.10.0-514.6.1.el7.x86_64

区块链配置

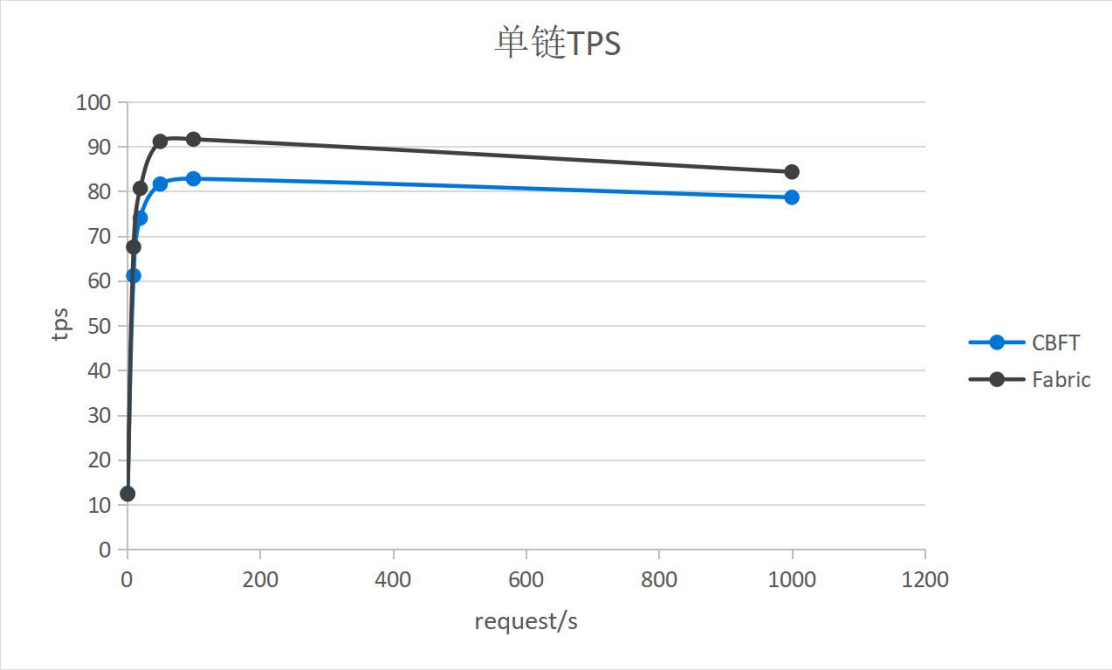
- BatchTimeout: 2s
- MaxMessageCount: 10
- AbsoluteMaxBytes: 98 MB
- PreferredMaxBytes: 512 KB

合约设置

每个节点部署相同的pressureMeasureCC.go智能合约。该合约初始化一个账户A，账户初始金额为100，设置有add接口，每次调用智能合约的add接口，账户A资金加1。

测试结果

Testing Result



数据

Fabric

90笔/s

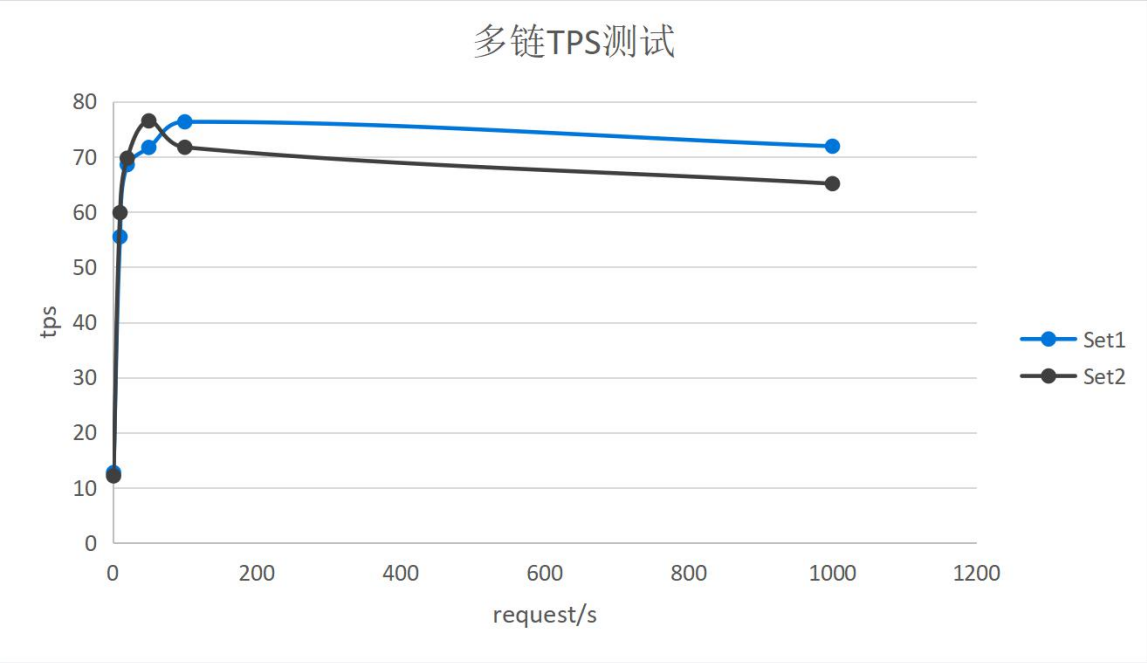
CBFT

80笔/s

经过改进的CBFT算法相较于同样是“联盟链”定位的Fabric，拥有相对差不多的TPS，但是安全性有了提高。

测试结果

Testing Result



数据

Set2

65笔/s

Set1

75笔/s

Total

140笔/s

多链测试，两条子链TPS峰值差不多有70左右，那么可以认定整个系统同一时间最高可以承受140笔/s的交易。

数字汇票体系

The Digital Draft System

链上流转

“数字汇票”是运行在区块链上的智能合约。一旦上链，不可篡改。

信用背书

“数字汇票”由省领导小组办公室发行，信用背书保障了信息的高度可信。

责任证明

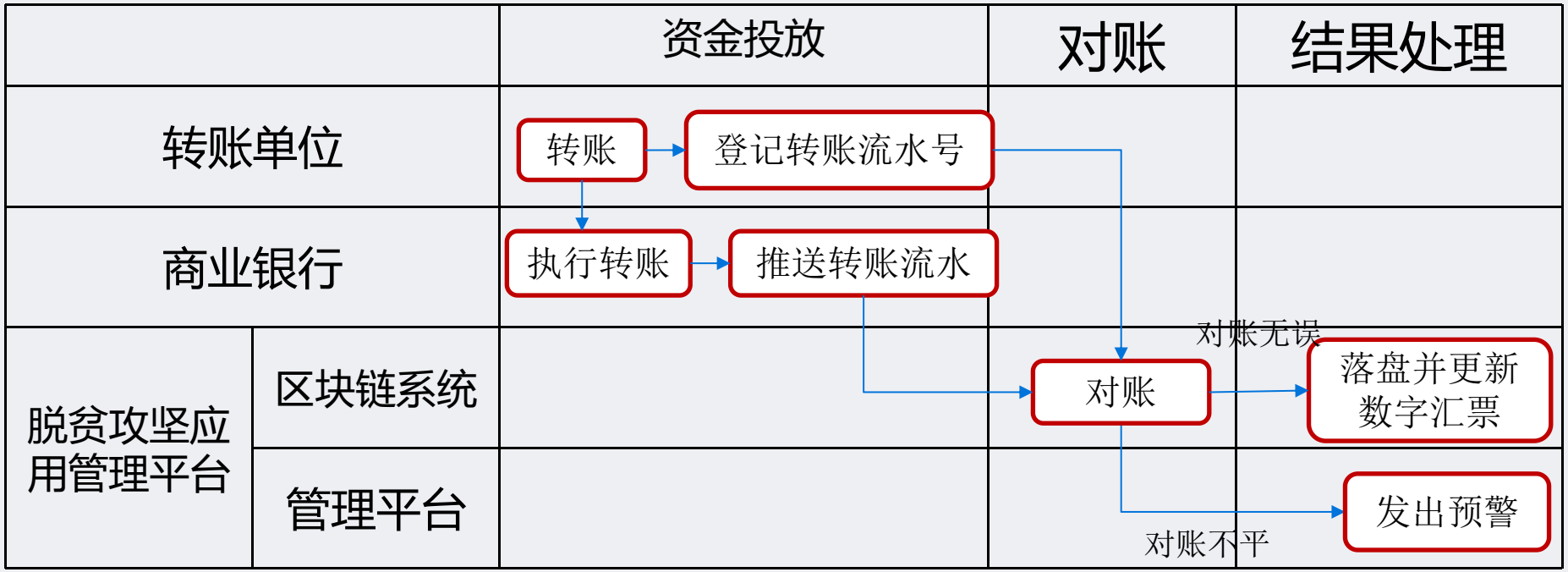
“数字汇票”是资金在数字世界的代表，代表了资金的实时动向。

信息透明

“数字汇票”流经谁，现在在谁手上，在区块链上一目了然。

实时对账系统

Real-time Reconciliation System



上链信息真实

银行，作为一类做信用吃饭的公司，其信息的真实性得以保障

提供数据放心

数据如何分发，如何处理都写在智能合约里，好比法律合同，清楚透明，消除银行的顾虑

协同作业高效

合作方无需开发新系统

系统展示

The Pain Points

系统展示

System Show

Thanks