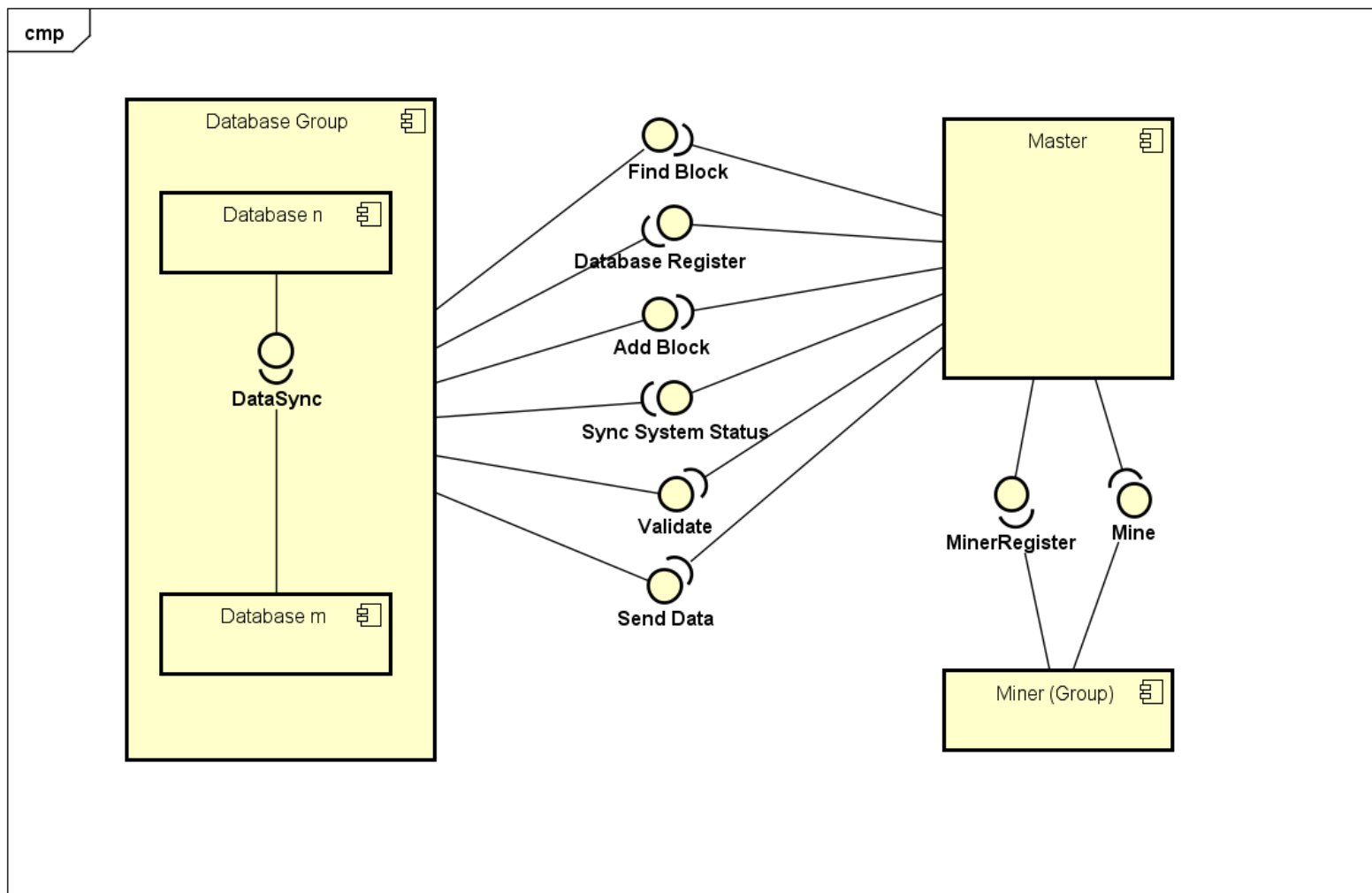


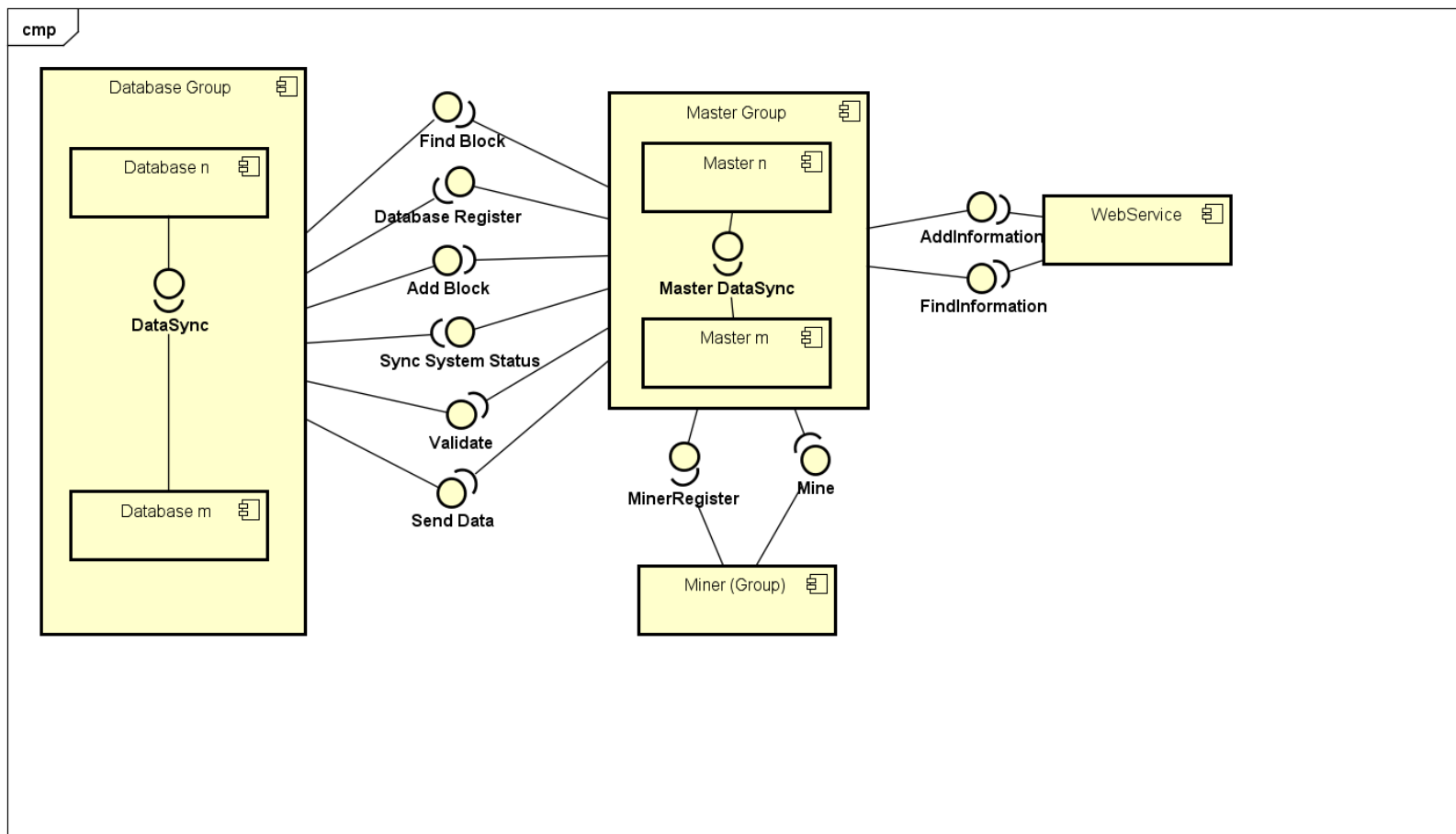
ChainStore: 基于区块链的分布式存储系统

技术细节和技术发展展望



架构图

第一版，初赛作品



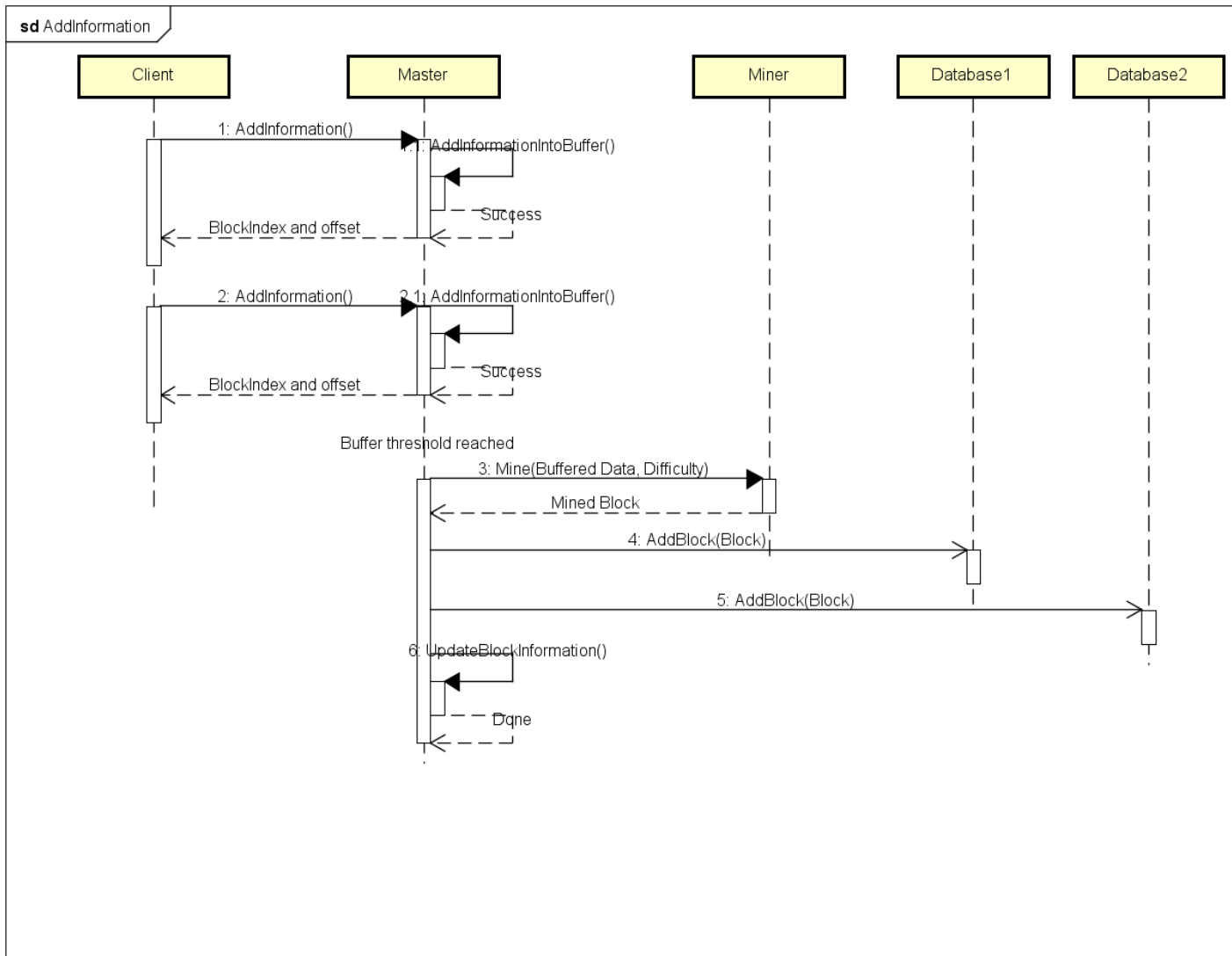
架构图

系统组件

- 存储（Database），存储群（Database Group）
 - 数据真正存储的地方。每个存储都有整个系统的所有信息
- 矿机（Miner），矿机群（Miner Group）
 - 计算中心，计算区块hash
- 主机（Master），主机群（Master Group）
 - 维护系统状态，管理系统运行
- WebService
 - 对系统外提供增加和查询的服务

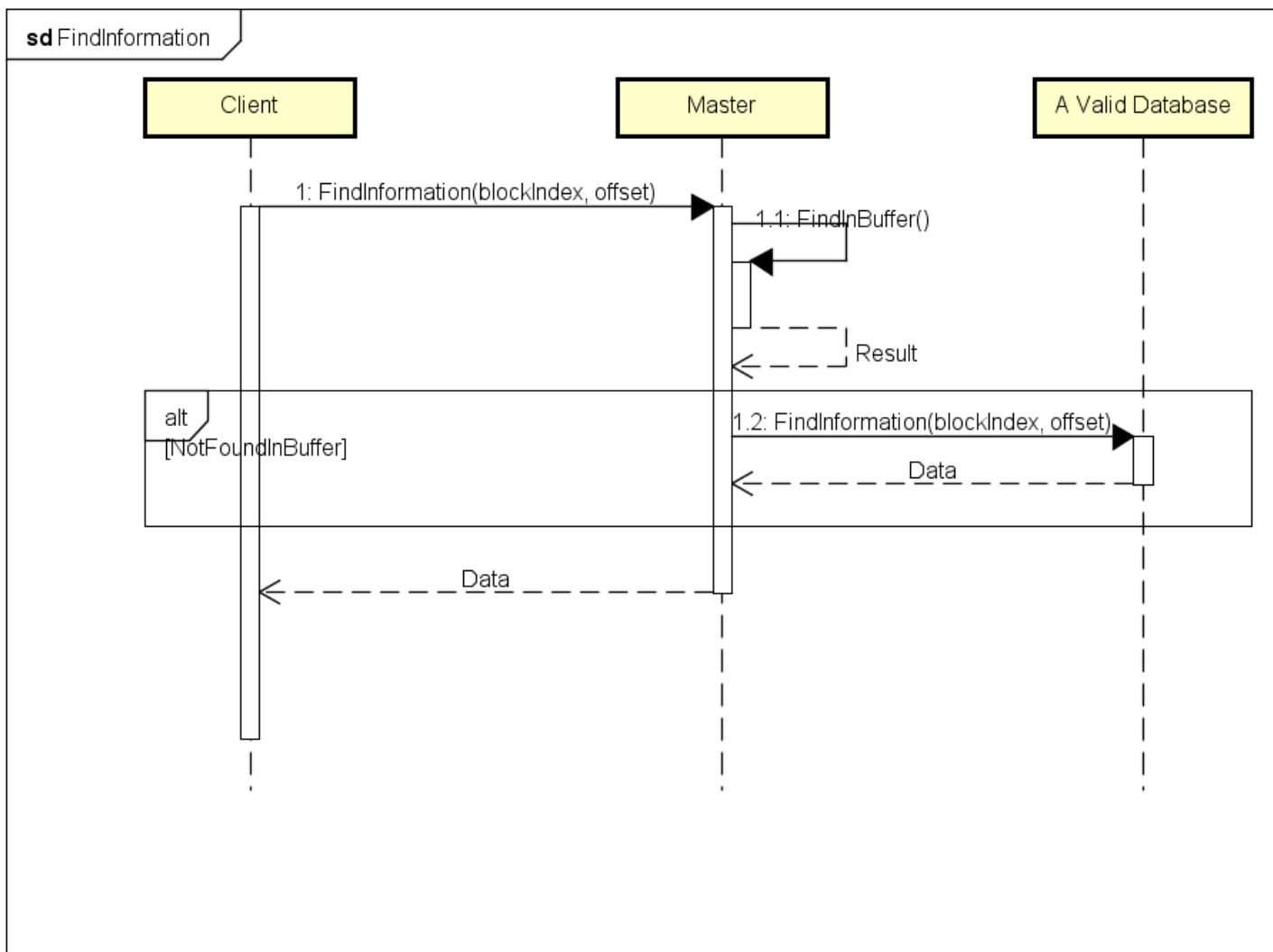
系统关键流程

1. 增加信息
2. 查询信息
3. 系统初始化
4. 定时检查存储数据完整性
5. 存储不可用，通过其他存储恢复信息（存储数据同步）
6. 主机控制信息同步



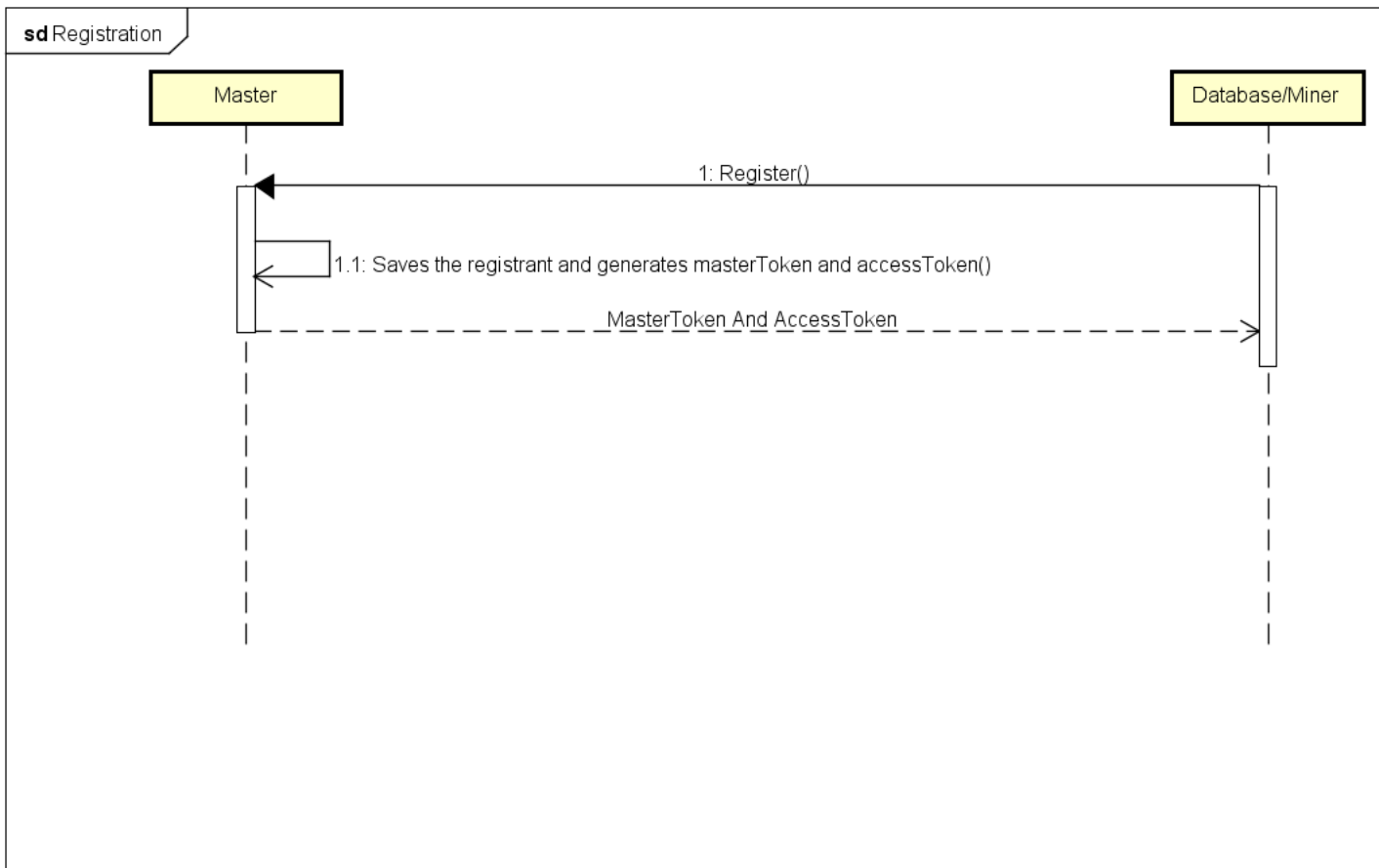
增加信息

1. 主机收到信息，加入缓冲区
2. 缓冲区满，矿机通过这些信息计算一个新区块
3. 主机将区块发往所有存储机
4. 存储机接受到新区块后，
 1. 处于有效状态的存储将会在收到新区块的时候立刻将数据存储存储系统；
 2. 处于其他状态(收、无效、验证、发)的机器将会将新区块存入自己的缓冲区，待自己转换有有效状态的时候再将缓冲区的数据存入存储系统。



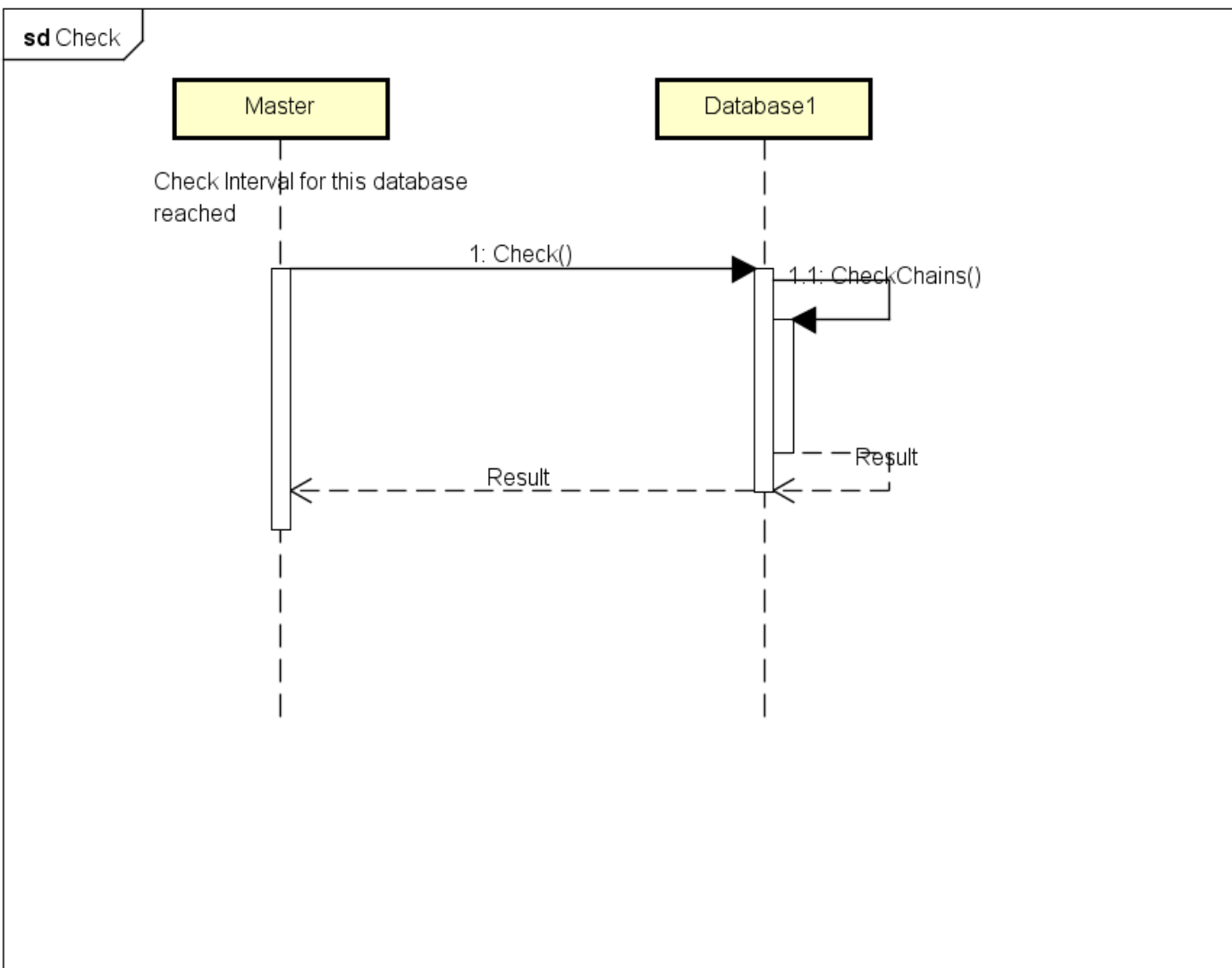
查询信息

1. 外界给出区块号和块内偏移
2. 主机首先检查区块号是否即为缓冲区（即数据仍然在缓冲区中），
 1. 若是，则直接根据偏移返回数据；
 2. 否则，任意找一个处于有效状态的存储，要求其找到对应位置的数据。存储查找到数据后，返回给外界。



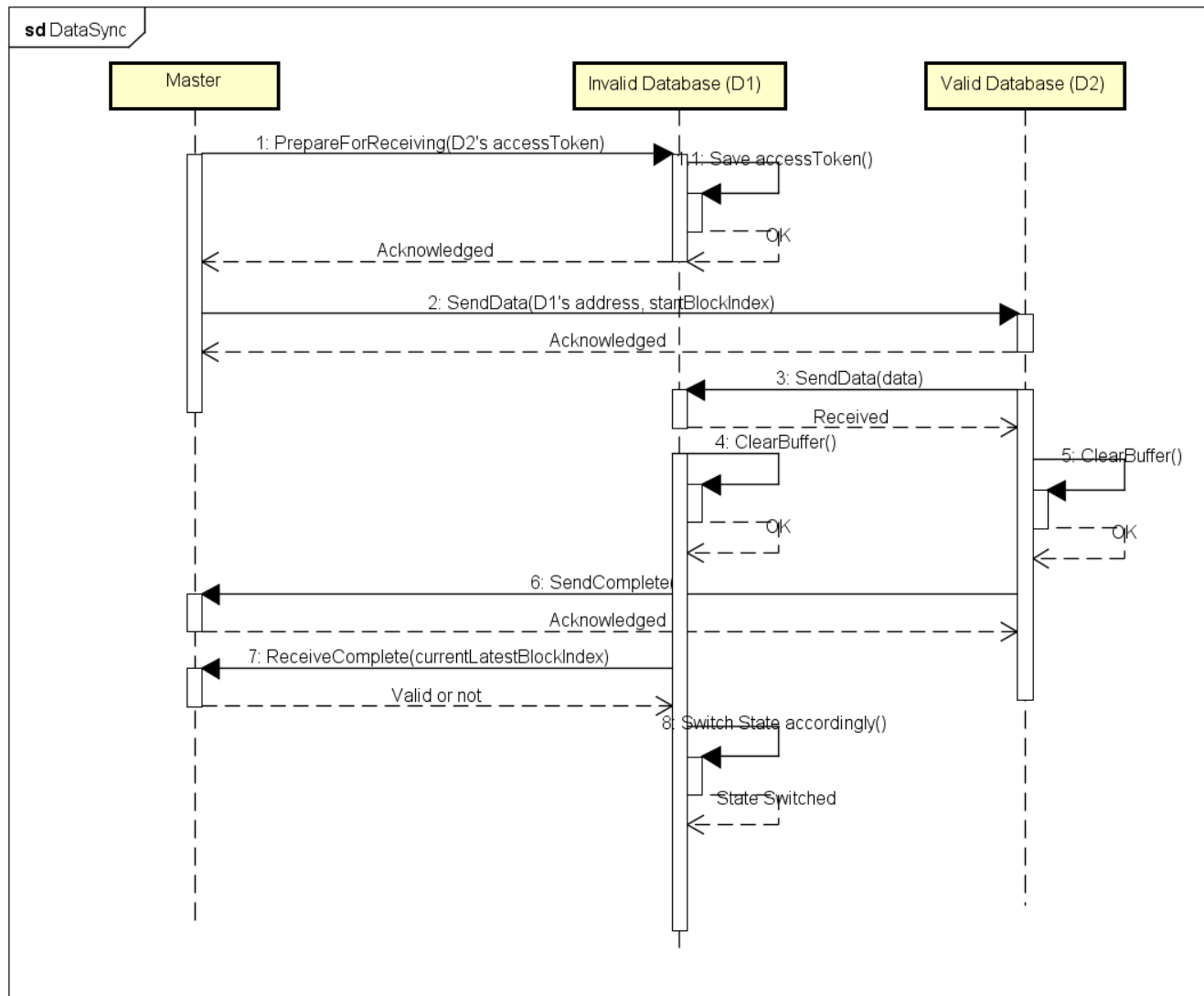
系统初始化

1. 启动任意一台主机
2. 存储和矿机启动后，向任意一台主机注册，主机将会记录下注册者的地址，并发放token进行鉴权
3. 主机将会同步所有控制信息



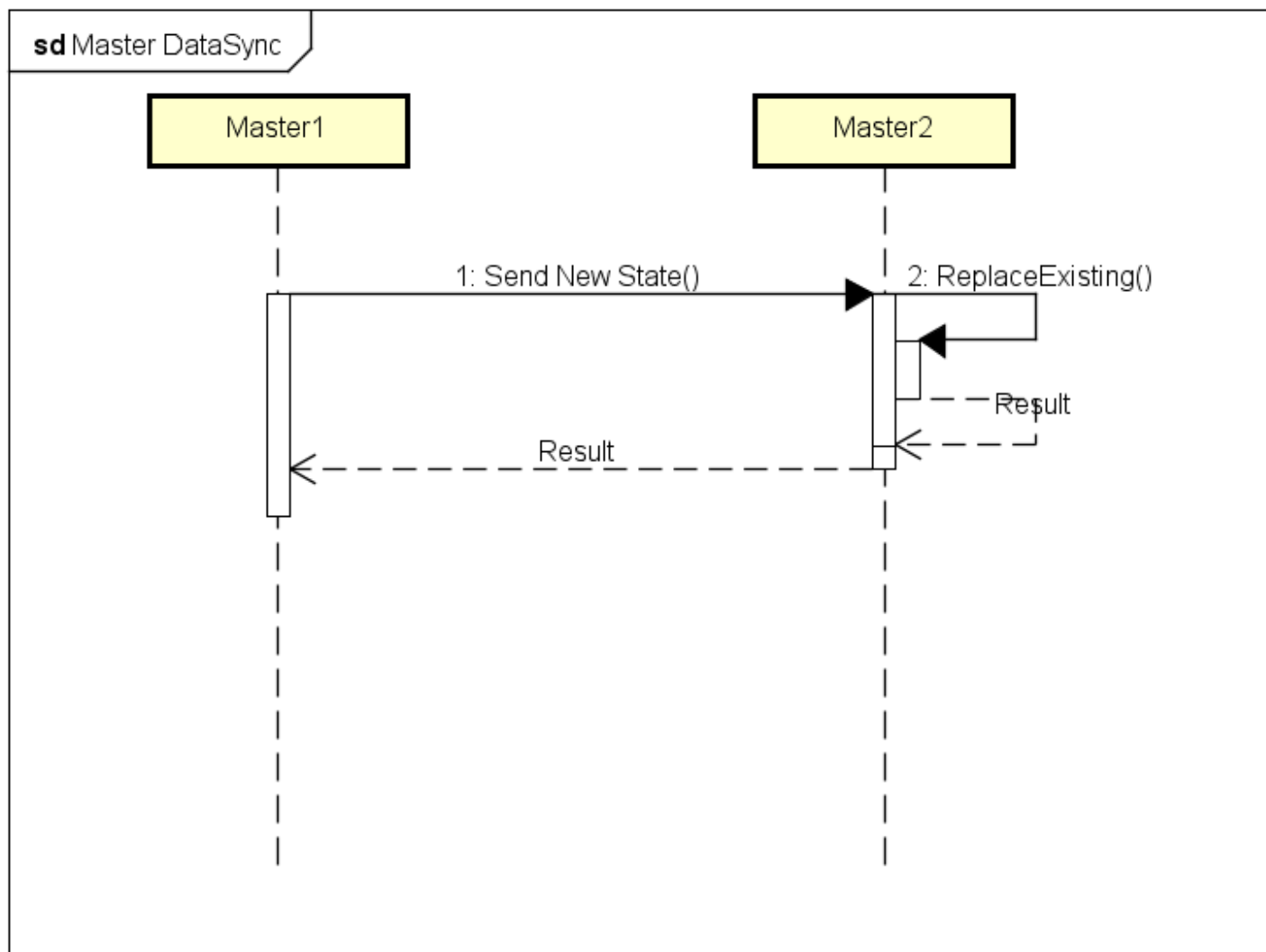
定时检查存储数据完整性

1. 主机将会发给存储目前最新的区块号。存储将会转换为验证状态，并开始从第一个区块开始检查自己保存的链的可用性。当出现以下两种情况之一时，进入无效状态，并将第一个无效区块的编号给主机：
 1. 链从一个区块开始，hash不匹配，报告hash不匹配的的第一个的区块编号
 2. 全链hash匹配，但是最新的区块号不匹配（意味着丢失了信息），将会报告第一个缺失的区块编号
2. 当以上条件均不满足时，存储通知主机检查完毕无异常，重新进入有效状态。
3. 检查结束后，主机将会记录下存储的目标状态，并进行进一步的处理。



存储不可用，通过其他存储恢复信息（存储数据同步）

1. 当存储（D1）数据检查完毕而且检查结果为无效时，主机选择一台处于有效状态的存储机（以下称为D2），并让D2从D1检查出的无效区块的编号开始的所有数据发送给D1。
2. 在此期间，D1应检验发送者是否为D2。
3. 发送结束之后，D2通知主机发送完毕，清空缓冲区。
4. 向主机发送目前最新区号，若不匹配，则重新进入无效状态，重新进行数据同步；若匹配，则进入有效状态。



主机数据同步

1. 当主机的状态表发生改动时，应立刻发送新状态表到其他主机；
2. 其他主机使用新状态表覆盖自己的状态表

其他设计选择

- 运行于JVM，兼容几乎所有平台
- 基于Spring Boot，RESTful接口进行系统内和对系统外交互（可更改为RPC等以提高效率）
- masterToken和accessToken鉴权，过滤伪造请求：
 - 在注册时生成，主机和注册者均保存一份
 - masterToken用于存储和矿机检验请求是否为主机发出
 - accessToken用于主机检验请求对象
- 使用文件系统保存数据：通用

视频演示

运行于单台机器，运行3台存储机、3台主机、1台矿机（跑在不同端口）

ChainStore系统特点

1. 强调区块链本质和最大的特点：已上链数据不可修改
2. 架构简单，专注存储和管理数据，可支持各种各样的上层应用
3. 安全性：
 - 想要修改数据必须：
 1. 修改算出一整条完整分支；
 2. 修改主机的状态表（长度和上一个hash）；
 3. 攻破所有存储机并修改数据；
4. 易部署
 1. 使用Spring Boot构建，使用HTTP协议进行系统内部和外部的传输，便于组网
 2. 可在任意规模的设备上部署（支持HTTP即可，可以使用RPC等更高效率的通信方式）
 3. 可进行中心化部署和去中心化部署
5. RESTful对外接口，方便应用
6. 开源开放，促进社区：<https://github.com/NJUChainStore/ChainStore>

WebService

- 自主运营的基于ChainStore的对外区块链数据存储服务
- 核心：自主运营的ChainStore系统
- 服务：
 - 对非盈利项目：在项目公开或者数据公开的前提下，免费使用区块链服务进行数据存储
 - 对普通企业：私有项目/数据，收费使用区块链服务
 - 针对注重私密性但是技术实力不够强的大客户：官方外包队伍为企业量身定制
 - 针对技术实力比较强的客户：自己使用ChainStore定制属于自己的区块链服务
- GitHub/GitLab

技术前景总结

- 核心服务开源：
 - 取得用户信任
 - 通过Origins这一强有力的应用推广，促进社区的形成
 - 强技术实力的公司可以在此基础上搭建自己的架构
- 针对各类型项目和客户（非盈利项目/普通企业客户/注重私密性的客户）有独特的完整解决方案
- 针对特性需求的官方外包服务