基于区块链的日志式数据库——ChainSQL

区块链是分布式的、去中心化存储的一种链式数据结构。它是一个分布式的帐本，所有的记录由多个节点共同完成，每个节点都有完整的帐本。区块链本身具有的最显著的特征是：分布式、去中心化、信息不可篡改[1]。

数据库是按照一定的数据结构来组织、存储和管理数据的建立在计算机存储设备上的仓库。数据库的特性有：减少数据的冗余度、数据的独立性、数据实现集中控制[2]。

区块链从本质上来讲也是一个数据库，是一个去中心化的数据库。但是对数据的查找速度、数据格式化处理方面有天生的不足。

本文将结合区块链与传统数据库，设计一种全新的基于区块链技术的数据库，这样的数据库不仅具有区块链的分布式、去中心化、可审计的特性，同时兼备传统数据库的快速查询、数据结构优美的特性。两者的结合使得数据库的恢复变得快速、数据可靠性得到质的飞跃。

一、 设计原理

区块链上所存储的数据，我们统一称为交易。

在本设计中，把对数据库操作的每一条指令都记录到一条交易中，即一个交易对应一个数据库操作，区块链网络会以交易的形式记录下所有对数据库的操作。

对于配置了数据库的区块链节点，在区块链网络记录交易的同时会完成对数据库的操作。对于未配置数据库的网络结点，交易只会记录到本节点的区块中。

已经配置数据库的节点，可以通过配置从区块链网络上的第一个区块开始搜索，去获取数据库表对应的交易，根据这些交易去再次执行数据库操作，从而生成对应的表，获得与其它区块链网络节点一致的数据库表内容。

二、 设计方案

1. 区块链网络的选择：

最常见的区块链网络就是 BitCoin 网络，但是 BitCoin 网络在实际应用中有两个缺点[3]：

1) 速度慢：一笔交易被全网验证通过需要大约 10 分钟的时间，真正得到安全地确认需要大约一个小时。
2) 区块的生成需要矿工来完成，这个过程要经过大量的计算，对资源浪费比较严重

作为改进，Ripple 的出现解决了 BitCoin 网络存在的不足，Ripple 网络通过自己独有的 UNL 方案的引入，使得 Ripple 网络的节点能有效地验证自己收到消息的真伪，不需要经过大量的计算即可生成区块，其每一条交易从发出去验证只需要 3-8 秒[4]。

基于 Ripple 与 BitCoin 的对比，我们选择 Ripple 作为本系统的区块链网络。

2. 整体结构及流程

chainSQL 的实现主要分成三个部分：

1) 区块链网络：各个节点 N 构成 Ripple 网络，完成区块链网络的架设。
2) 普通数据库：在需要生成数据库表的节点对数据库进行配置。
3) 客户端：可选择自己创建一个区块链节点接入网络，然后向这个节点发送数据，如图 1 中 C2。也可以直接向网络发送交易，如图 1 中 C1。

我们先架设区块链网络，这时已经可以向网络发送数据库操作的交易了，不需要配置任何的数据库，如图 1 中 C1。

客户需要查看网络上的数据库表或者想真实看到传统意义上的数据库表时，需要在本地创建一个区块链节点 NC2，连入网络，同时在 NC2 配置数据库 DB，这时发往区块链上的数据库操作就会实时地在 DB 中反应出来，如图 1 中 C2。

客户不想对表进行操作，仅想查看其它客户创建的表时，需要在本地创建一个区块链节点 NC1，同时在 NC1 配置数据库，在配置文件中设置需要同步的数据库表名与所属用户，即可得到对应的数据库表。

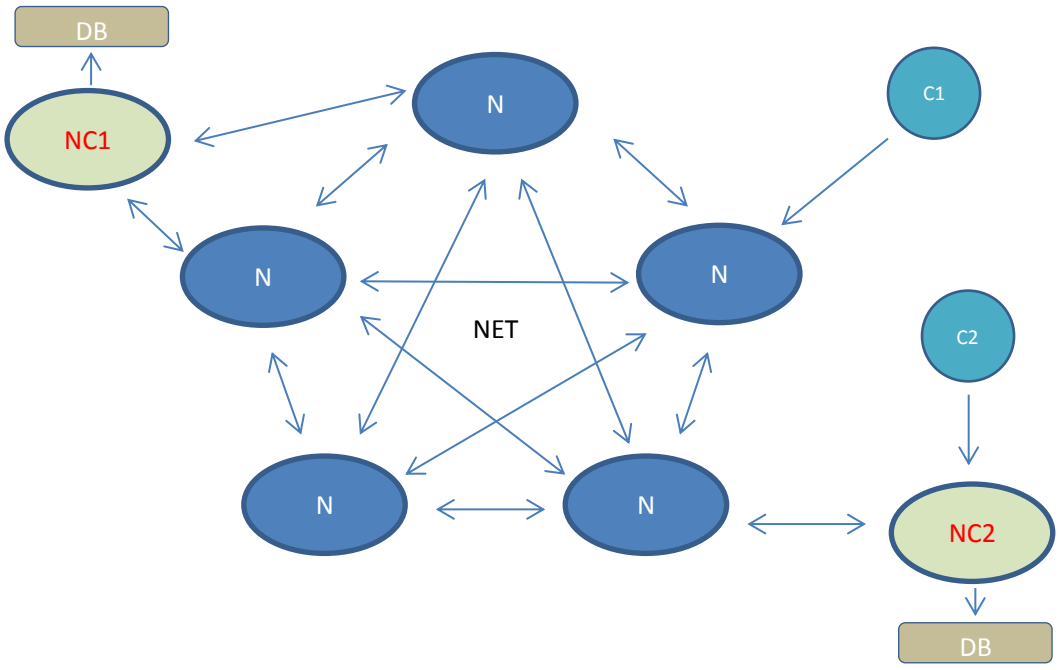

图 1

3. 具体设计：

1) API 接口的提供:

在区块链的应用层提供 API 接口供用户调用，用户向区块链发出交易命令就像操作

数据库一样。

2) 先入库再共识：

基于区块链的应用有个基本的做法就是交易要先经过区块链网络进行共识[5]，然后交易才能知道是否有效。我们在处理时：在一定条件下，先由本地节点验证交易，然后写入数据库，数据库写入成功后，再发到区块链网络上进行共识。如果共识不能过，则回滚数据库操作。这样的设计以便于用户快速地得知自己 SQL 语句执行的结果[6]。

如果节点已经配置了数据库及对应的表。区块链网络在接收到数据库操作交易的数据时，会直接传导到对应的数据库进行数据库操作，这样就实时反应用户对数据库的操作。

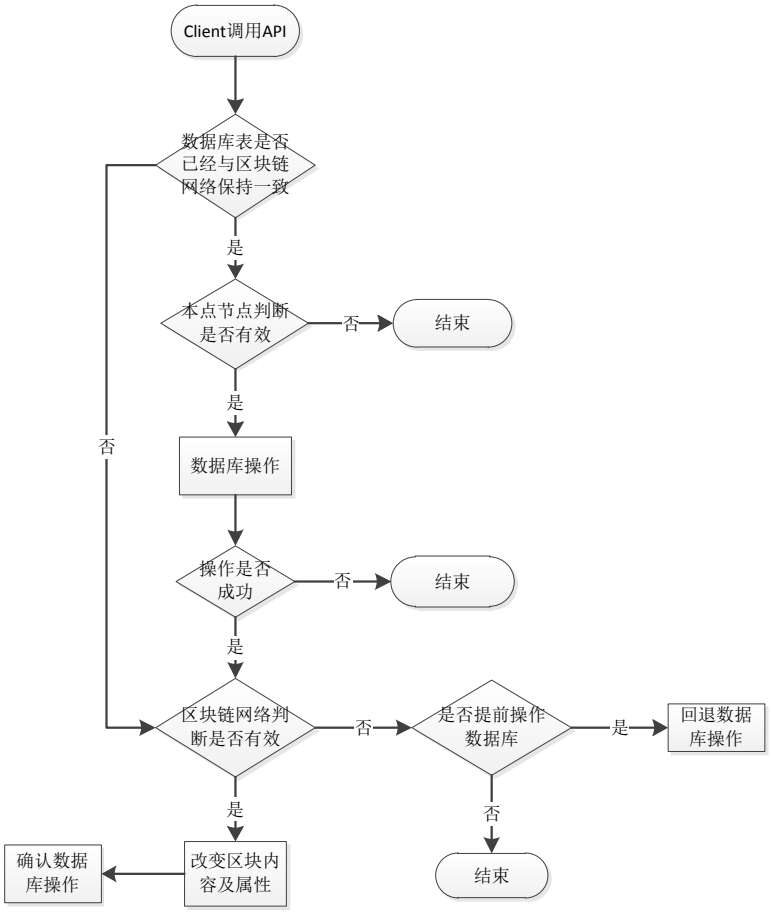

图 2

3) 根据配置进行数据库表的恢复

在某一区块链节点配置数据库，把存放在区块链网络中的数据库交易取出，按这些操作去执行数据库，达到重建一张表的目的。

区块链网络上的某一个节点，可以是全记录节点（拥有区块链网络中的所有交易数据），也可以是部分记录节点。

本地节点获取数据的时候，如果有对应表的数据库，则直接从本地获取数据库操作交易数据；如果本地是部分记录节点时，本地缺少某个区间的区块，这时只要从其它节点去获取对应范围内的数据库操作交易数据即可。

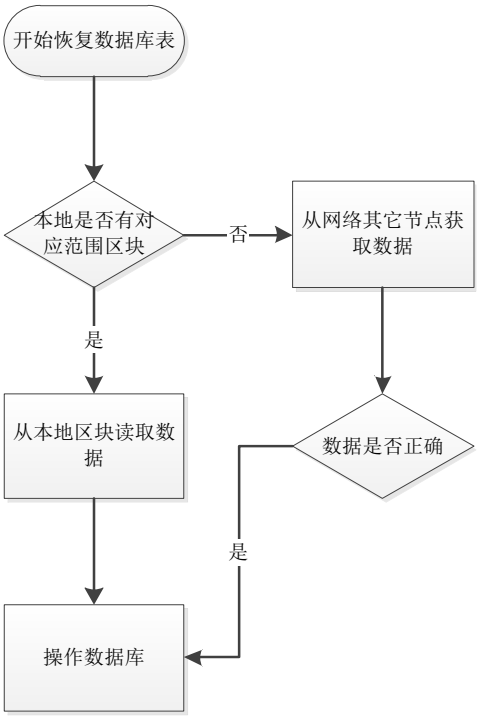

图 3

4. 设计要点

1) 安全性设计：以用户为管理单元，即一张表默认只隶属于一个用户（表的创建者），其它用户想对本张表进行操作，得让表的所有者对其授权。

2) 数据库的操作与数据库表的分离：操作以交易的形式记录在区块链网络中，而真实数据在数据库中查看。

三、 特性与应用场景。

1. 历史记录不可更改性：对于传统的数据库，对于记录的更改及删除可由管理员或者黑客随意操作。对于 ChainSQL，由于在区块链网络上记录了对数据库某张表的所有操作记录，则单独对数据库进行更改不会改变区块链网络上的记录。区块链网络交易的不可更改性决定了 ChainSQL 数据的不可篡改性。
2. 满足审计要求：对数据库表的操作记录全部记录在了区块链网络中，区块链对交易存储的特性使得我们可以知道交易发生的时间、具体内容。审计人员只需要从可靠的区块链网络节点中去恢复一张数据库表即可完成对数据的审计。
3. 数据可在任意时间恢复到任意地点：只要启动一个区块链网络节点，与区块链网络连接，配置好对应的数据库，即可恢复区块链网络中存在的任意一张表。
4. 数据的插件式管理：本地可以配置任意常用的数据库，包括：mysql，sqlite，oracle 等。
5. 简单编程模式：通过简单的 API 或者 JSON，可以在网页或者 APP 上对数据库进行写入及读取。

6. 快速区块链应用的开发：任何想用真实数据库来存储数据的应用，同时想兼顾区块链特性的应用，都可以应用本系统，通过调用本设计提供的接口来快速完成。

四、 结束语

本设计将区块链与传统数据库相结合，构建了一种基于区块链网络的日志式数据库。该数据库系统兼备了两种系统的优点，能随时随地恢复数据库表。该设计不仅将传统数据库的特性进行了增加，同时使得基于区块链的应用开发变得简易。

本设计中采用了先入库再共识的做法大大增加了数据入库的速度，增强了用户体验。可以随时随地对数据库表的恢复功能使得审计变得更加的方便。是进行基于数据库进行安全开发的良好平台。

参考文献

[1] 谭磊，陈刚 区块链 2.0. 电子工业出版社，2016

[2] Abraham Silberschatz , Henry F.Korth, S.Sudarshan. Database System Concepts. 机械工业出版社, 2012.3.1

[3] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system”. Consulted 1.2012(2008): 28

[4] Ripple Labs Inc. “Ripple developer center”. https://ripple.com/build/

[5] David Schwartz, Noah Youngs, Arthur Britto. The Ripple Protocol Consensus Algorithm. 2014

[6] 陈志泊. 数据库原理及应用教程. 人民邮电出版社, 2014.2