基于以太坊的私有区块链 Hydrachain 的介绍

蔡维德[1]郁莲[2]姚亚飞、胡成建、李冠男[3]

私有区块链（private blockchain）是区块链技术讨论中的热门话题。北航数字社会与区块链实验室研究了开源的私有区块链项目——Hydrachain，基于以太坊（Ethereum）[1]开发而成。实验室总结了 Hydrachain 的技术实现，给感兴趣的学者做参考。

本文所述是基于 Hydrachainv. 0.1.7 版本[2]，由于 Hydrachain 还不成熟，代码版本也一直在变更中，本文所述内容不保证正确性。

1. Hydrachain 与以太坊

Hydrachain 是一种私有区块链，在以太坊的基础上修改了建块方式，将之前的挖矿建块的方式改为通过一致性算法投票建块，是以太坊的一种扩展。本文介绍了 Hydrachain 作为私有区块链的实现方式，并着重介绍了其一致性算法及其实现。

不论 Hydrachain 亦或以太坊，官方并未给出自己的技术架构图。我们实验室根据自己的理解，试着画出了 Hydrachain 的架构图，如图-1 所示，供大家参考。

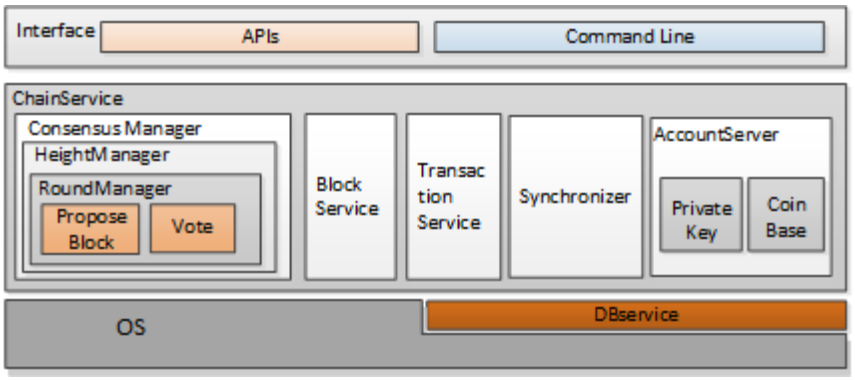

图-1

Hydrachain 架构图中主要组件介绍：

- Consensus Manager 主要用于区块一致性算法的实现；
- BlockService 主要用于区块的管理和发送；
- Transaction Service 主要用于交易收发及其处理；
- Synchronizer 主要用于和其他节点同步区块信息；
- AccountServer 主要用于 Hydrachain 中的账户的管理；

Hydrachain 大量的调用了以太坊的功能接口，包括 DBService，AccountsService，NodeDiscovery，PeerManager，JSONRPCServer，Console 等。这就意味着在安装 Hydrachain 之前必须要安装以太坊的 pythapp，如果仅仅是要建立私有区块链代码上还略有冗余。Hydrachain 重新定义的 ChainService，也是在继承了以太坊的 chainservice 及基础上实现的。

---

[1]北京航空航天大学千人计划教授；北京航空航天大学工信部工业和信息化法治战略与管理重点实验室高级研究员；计算法律学专家；亚利桑那州立大学名誉教授；前清华大学长江讲座教授；前明尼苏达大学教授；麻省理工学院学士，加州大学伯克利分校博士，OW2（中国-欧盟开源软件联盟）副理事长。

[2] 北京大学软件与微电子学院教授；1999 年 4 月博士毕业于日本横滨国立大学计算机工程与电子系。2000 年至 2005 年美国亚利桑那州立大学做博士后研究工作。2005 年 9 月加入北京大学软件与微电子学院。近年主要从事高可靠软件开发、情境感知服务、等方面的理论与方法研究，发表论文 50 余篇。

[3]北京大学 13 级在读硕士，专业方向为软件工程。

通过重写原公有区块链的 check_pow()方法，将其改为“return true”，Hydrachain 的 chainservice 放弃了挖矿建块。

实现私有区块链的方式改为了传统的一致性算法。利用这样的一致性算法，可以保证在忠诚的节点数大于 2/3 时，私有区块链是安全的。每次的投票要求 2/3 以上节点同意。

Hydrachain 的安全性依赖一些注册节点，且这些节点都是可信任的。这是私有区块链的存在的重要前提。

2. 一致性算法

Hydrachain 的一致性算法是一种类似于 PBFT（Practical Byzantine Fault Tolerance 拜占庭将军问题解）[3]的传统一致性算法，保证了建块过程中的一致性，每次只会有一个块被投票通过。

不同于公有区块链，私有区块链的一致性算法要求每个节点知道所有参与建块和投票的节点。其中一个原因为只有知道所有参与投票的节点数量，才能在统计最后的通过节点数量的时候确认同意节点的数量是否达到了 2/3，这是一致性算法的必然需求。

（1）节点确认

为此，一致性算法首先要执行 ready 信息的发送和接受，每个节点会在进行投票和建块之前根据自己收到的 ready 信息决定将哪些节点作为参与者。这也是检测节点能否正进行正常收发投票和块的验证。

Hydrachain 引入了 height 和 round 的概念，每一个块都有唯一的一个高度，为了建一个快，会有一轮到多轮的建块投票。这样的做法使得所有节点步调更加一致。

（2）Round Robin

在一轮投票的开始阶段，会选出一个节点提交一个块，Hydrachian 利用 round robin 算法来选择这个提交者。

在选择提交者时，每个节点对当前高度（height）和轮数（round）进行哈希，每个节点使用相同的哈希算法，因此在同一高度同一轮下，哈希结果是一致的，利用这个哈希结果映射到参与者列表中的一个参与者，可以得到唯一提交者。因此每个节点得到的提交者是一样的。

确定了提交者之后，提交者会提交一个块，以广播的方式发给所有参与节点，这个块是自己建立的或者之前一轮的块。

（3）块提交

提交的块可以是自己建的，也可能是上一个轮还没有被 2/3 以上节点通过但是已经被 1/3 以上节点通过的块。这也就意味着每次的建块者都是唯一的，且不需要挖矿来实现，相比于公有区块链减小了建块的 CPU 成本。

Hydrachain 假设系统内的不忠诚节点个数少于 1/3，因此当有 1/3 以上节点通过某一个块的时候，就意味着至少有一个忠诚的节点投票通过，Hydrachain 认为这样的块“可能”会被所有节点通过，因此在接下来的一轮的投票还会继续使用这个块。

（4）投票过程：

接下来每个节点都会为对这个新的块进行投票，如果投票者收到的块合法，会把对块哈希的数字签名广播出去。每个节点接受投票，如果对于某一个块的投票达到了 2/3，则将其存入链中，否则进入下一轮。

每一轮投票都有截止，截止时间到了以后，一个节点如果还没有投票，则默认没有投反对票。为了保证不会由于网络原因导致投票频繁不能达成一致。每一轮的截止时间是不同的，后一轮的投票总是比前一轮的截止时间长，这样的做法可以在网络情况较好时在较短的迅速达成一致，网络较差时也不会由于传输速度过慢导致无法达成一致。

Hydrachain 的一致性算法每一轮投票的流程图如图 2 所示：

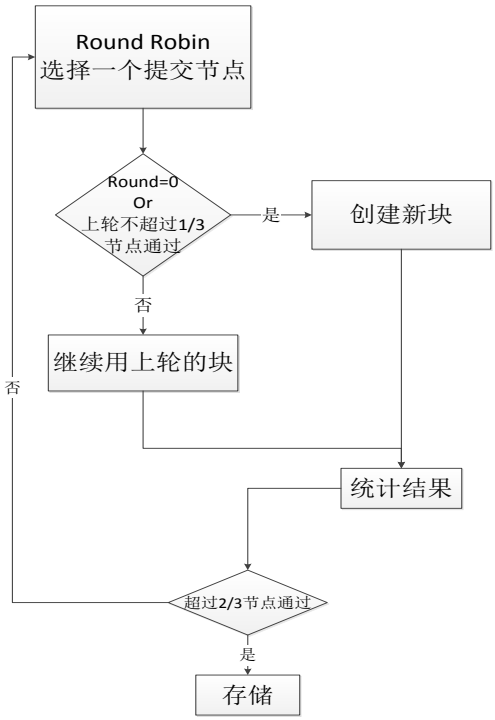

图 2

3. 一致性分析

在一致性方面，算法本身保证每个高度上只会有一个块被通过投票。每个节点只有在收到了 2/3 以上的投票之后才会进行到下一轮。只有在收到了 2/3 以上的肯定投票之后再会进入下一个高度。这保证了在所有节点在行动上的一致性。

除此之外，系统有自己的同步机制。每个节点在进行投票建块之前会检测自己是否有块的缺失，例如系统收到的块和本身的高度最大的块大小大于 1，则该节点至少少了一个块，该节点从其他节点处请求缺失块，保证链长度与其余节点一致。

考虑到 Hydrachian 的一致性算法保证了每一次都只有一个节点提交建块，且对于每个高度，只会有一个块被通过，系统在任意时刻区块链都是唯一的，区块链不会分叉。

为了实现一致性算法，Hydrachain 引入了 consensusManager，对每个高度创建 HeightManager，并在每一轮创建 RoundManager，将其作为在执行一致性算法时的处理模块。同时定义了一些新的数据结构，包括 Vote 和 Lock、LockSet。LockSet 是被存储在区块链中的一个数据结构，一个合法的 LockSet 是包含 2/3 以上节点投票的集合。

4.安全性分析

每个被通过的块都会有 2/3 以上节点的投票，也就会得到 2/3 以上节点对于块 hash 的

数字签名，这样的一个数字签名列表会被存到块中，这也是 Hydrachian 在继承以太坊的 chainservice 的基础上对块增加存储的一个重要字段。每个块存储了这样的一个数字签名列表之后，安全性由于数字签名的存在有了保证。

Hydrachian 的数字签名的加密技术采用的是椭圆曲线加密。每个节点保存自己的私钥，对其发出的信息进行加密形成数字签名。保证了数据的安全和实现了发送者的识别，是区块链安全的一个重要原因。

5. 结束语

北航数字社会与区块链实验室也和北京大学合作，于 2015 年中着手开发了自己的私有区块链，早于 Hydrachain 的开发。其中，去除挖矿机制而采用拜占庭将军问题解决区块一致性的问题，也是实验室最早的决定，这和 Hydrachain 的想法是不谋而合的。

相较于共有区块链的公开性，私有区块链有更严格的访问权限，使得金融机构和一些政府组织更倾向于采用私有区块链技术。所以，实验室的私有区块链将速度、安全作为首要目标。而且较之于 Hydrachain，我们还引入了一些新的技术，使得私有区块链的性能和功能更加的完善和安全。

6. 参考文献及引用

[1] 以太坊官网——https://www.ethereum.org

[2] Hydrachain github 代码仓——https://github.com/HydraChain/hydrachain

[3]Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. Appears in the Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999

[4] 蔡维德 & 罗佳.区块链所带来的公信力革命——以区块链对保险行业的影响为例.http://www.civillaw.com.cn/zt/t/?29937, 2015/12/15