**井大在多伦多群关于分片的解读**

日期:Feb.17,2018

【王云海】:我现在感兴趣的一个是分片，一个是DPoS的实验，还有一个是statechannel。因为看起来性能是必须解决的问题，不然杀手级的应用不可能落地。

【rubyrubyru】:分片我有点怀疑

 【王云海】:愿闻其详，分片的技术材料我没有太仔细的读懂,接下来我会花点时间去仔细读懂他，你有什么心得可以和我分享一下吗。

【rubyrubyru】:我也不清楚，不过我比较怀疑分片以后如何达成共识，是不是需要无条件信任其他分片的执行结果。

【井大】:分片我可以说说

 【王云海】:太好了！期待，我已经拉过小板凳。

【井大】:先说一下比特币和以太坊，简单可以这样说，比特币是交易 transaction，以太坊是交易+智能合约。

【王云海】:对，比特币没有账户概念，我不打断你，你继续说。

【井大】:我在做墨客的时候，有这么一个假定，是我认为未来的主要堵塞的流量来自于智能合约。因此我首先是做一个分层，把交易和智能合约分到不同层次。那么在底层我维持用目前已经实践证明有效的pow处理交易，系统合约执行。那么在上层，我用分片按照智能合约来分到不同片。而我认为各种共识有其pro和con，那么让用户自己去选用符合自己需求的共识。所以在智能合约片里面，你可以选用bft，pos，tendermint，和你自己定义模块，保证可插拔。

那么说一下大家知道有一家叫做zilliqa的，也在做分片。他们当然没有分层，因为他们不支持完备图灵机。所以大家可以忽略这一部分，他们就是按照固定600个节点分一个片，里面跑交易，用了中心化改变的bft。

【王云海】:明白

【井大】:基本上就是要保证同一个发起交易的地址，必须放到一个片里面去，不然肯定会出现双花。我觉得他们有好几个点，都是蛮大风险的，这个可以具体聊。

最后就是以太坊，也是没有分层。那么必须同时解决交易分片，以及智能合约的状态分片。状态分片就是state channel，或者state sharding，难度不是一般的高，大概就是这样情况。目前可以说成功分片的，墨客是一家。其他的等产品出来再看吧，说完了。

【张十一】:墨客最新测试情况怎么样？大概啥时候上线呢

【井大】:三月底，现在排队排了20多个了，希望今年上来100个子链。

【王云海】:statechannel难度高在哪里。你们也遇到了这样的问题，并且解决了吗。是不是因为你们有分层。所以这个问题就好办的多

 【井大】:墨客暂时绕过了这个难点，我们采取智能合约分片，这样一个完整的合约，在一个自己的片里面跑，而不是把一个合约按照先后持续，分到不同的片。

【阿川 】:小蚁系的Trinity也是说成功用了state channel

【井大】: trinity是类似闪电的侧链吧，和分片没啥关系

【王云海】:有几个statechannel是不一样的。有一个项目叫做AE，他的合约是不保存状态到主链的，除非出现了争议才放到主链上进行公决。你们的合约保存状态到主链上吗，还是状态只在自己的分片上保存。如果状态只在自己的分片上保存，那我就可以大致理解了。

【井大】: 定期要flush下去，形成全网共识的。你可以类比一个vmware，下面一个物理机，上面跑很多不同虚拟机这种。我们类似于上面逻辑分片。

【王云海】:大致理解了，有意思。我去找你们的技术资料看看，谢谢。非常精彩的解释。

【井大】: 我们是子链subchain，他们是侧链 sidechain，我的想法就是子链可以作为公共服务提供者，比如我们可以部署IPFS子链，时间戳子链，真随机数子链，Schnorr签名子链，零知识证明子链。其他人的子链可以免费或者付费获得服务，也可以自己免费或者付费提供服务。另外就是合约采取异步调用，可以跨区块，用来做原子跨链。

【严挺@众享比特】: 什么叫真随机数？

【井大】: random number generator

【严挺@众享比特】: 现在大家都是伪随机数？

【井大】:有的是吧

【严挺@众享比特】:区块链里面哪些真哪些伪？谁研究过？

【井大】:很多pos都是。

【王云海】:定期flush下去。形成全网共识。如果有概率形成全网共识失败，怎么处理？这个定期flush共识是多长时间呢。是几秒级别的还是几小时级别的。如果是几秒级别的会不会严重的影响，整体性能呢。如果是几小时级别的。会不会缺少实际意义呢。因为很难推翻之前的分片共识？推翻之前共识的代价会不会太大？

【井大】:按照目前以太坊的节点数目，我们分片之后，tps估计可以到每秒5000，当然需要实际跑起来，但是2000tps应该无疑问。

【严挺@众享比特】: 一开始能有几个节点？

 【井大】:看矿机部署吧，可以到10000个。

【严挺@众享比特】:矿机是什么？还自己做矿机？

【井大】:pow和以太坊一样，智能合约这里可以流量盒子或者手机

【阿川 】:底层用pow的好处是啥？

【井大】:唯一实践证明可以在超大规模网络达成共识。

【阿川 】:完全pos不行？

【井大】:pos在超大网络没有验证过，小规模没问题。

【rubyrubyru】:分片以后怎么相信其他分片的结果？有没有简单的办法验证？如果需要全网验证，那就没有所谓分片了

【井大】:类似于撸猫的在一个片，撸狗的在另一个片。撸狗的只要知道撸猫的已经达成了共识，而其本身并不关心撸猫。

【rubyrubyru】:但是要消费元币，元币需要共识，元币需要在所有分片共享，如果没有distribution lock，分片之间可以双花。

【井大】: 我们不做交易分片，所以没有双花问题

【文延】: 刚和家人喝个早茶就错过这么精彩的技术讨论，我想补充的是早期分片技术可以一个数量级的解决网络拥堵的问题。分片也会遇到自己的性能问题，就是那个统一做同步调度的进程或工具就成为瓶颈，在数据库集群技术里我们叫catalog service，catalog service 会成为瓶颈，解决这个问题还是需要全网同步数据。

【井大】: 我这里用系统合约控制

【庞小鱼】: 可以请教一下分片逻辑么？

【井大】:  用智能合约分

【文延】:我发明一个技术叫动态账本技术，分hot ledger and cold ledger

Cold ledger vs hot ledger 将可以极大限度的提高区块链交易性能，成就可以跟传统关系型数据库才能达到的TPS。

【井大】:   嗯，这个方向有意思

【文延】:大数据的Eventually consistency 因为不是强数据一致性所以都不靠谱，这个是传统关系型数据库技术走到极致的结果，必须用到区块链来。sharding还是mySQL的master/slave模式只是读写分离部分解决问题而已，最终完全分布式必须走share everything 的构架，但是方向上对数据本身进行hot/warm/cold分离。In memory databases technology will be the killer feature to improve share ledger performance。

【rubyrubyru】:所以所谓的区块链又回到了简单的分布式问题了。

【井大】:   本来就一直是分布式计算问题

【文延】:杭州的趣链成功的利用了浙大院士在分布式计算上的优势在概念和构架上强先同行半个身位，但是在我看来还不够。区块链技术本质就是分布式共享账本技术，性能瓶颈自然是在全网做共识。今天我们讨论的区块链底层技术问题事实上价值远超百万，也是未来区块链技术的淝水之战。

【井大】:呵呵，完全明白你说啥

【文延】:所以你在做mother of all chain的时候你应该知道这个mother其实不单单要每一个儿子都要完全独立share nothing也可以看作所有的儿子们都是一体，只是大脑分离而已。你团队的部署也需要重新调整，sharding 可以解决问题，但是做RDBMS领域已经证明还不是最好的技术。In memory hot data technologies 才是你最终想要的，儿子们共享衣服工具手套什么的，有必要甚至可以共享部分不影响全网做共识的外围生态系统，自己根据行业应用场景去定义hot/warm/cold。

【严挺@众享比特】:  真正的业务复杂多了

【文延】: 你说的那个业务在business logic layer不属于数据同步和共识层

【严挺@众享比特】:   会有影响的，不同系统的TPS和数据库QPS之间本来就没有唯一对应关系，业务复杂度更加提升的时候不是简单分布就能解决问题的，否则全世界玩分布式数据库的大神早就牛逼大了。

【文延】:底层根据上面business logic层做一个workload 调优就可以了

【严挺@众享比特】:  真没那么简单，兄弟，我们现在和分布式数据库做接口的时候遇到了各种各样稀奇古怪的问题，不说了，都是工程实现的。