BCAC: 新零售生态区块链技术

技术黄皮书（初稿）

BCAC技术团队

摘要：本文介绍了BCAC新零售生态的初步设计和技术细节。包括用户和记账节点的认证机制，改进的DPOS机制来进行记账节点的选举，RAFT+共识算法，以及侧链技术。

1. 背景

区块链技术的出现，为各个行业提供了极大的驱动力来解决交易和共识的问题。但随着区块链应用的深入发展，区块链存在已久的问题，限制了区块链实际应用的落地。比如bitcoin、ethereum的性能，eos等性能公链的伪去中心化，等等。从设计角度，公链做为交易结算链，不适合也不应该承担应用数据上链的需求。

但是在短期内，不会有取代bitcoin、ethereum做为数字货币基础的新一代数字货币出现。而作为一个生态，区块链和数字资产也不应该是互相竞争和取代的关系。在BCAC的设计中，整个区块链技术会作为一个生态，通过侧链技术，从基础公链中剥离出应用数据。降低对基层公链数据/结算压力的同时，通过高性能的区块链技术，为区块链应用，尤其是新零售区块链应用落地提供支持。

1. 认证
   1. KYC认证

对于BCAC新零售生态用户，必须要通过KYC认证。

Know Your Customer（KYC）是识别和验证其客户身份的业务流程。在区块链应用落地过程中，Know Your Customer（KYC）的重要性正变得越来越重要。KYC是指金融机构（或企业）采取的步骤：

建立客户的身份

了解客户活动的性质（主要目标是验证客户资金来源是否合法）

评估与该客户相关的洗钱风险，以监控客户的活动

* 1. BCA认证

Business Credit Authentication（BCA）是为区块链侧链技术服务商提供的认证方案，用于识别区块链服务提供者，共识节点参与者的商业资质和信誉保证。BCA采取的步骤：

建立客户的身份

了解客户活动的性质（主要目标是验证客户资金来源是否合法）

评估与该客户相关的洗钱风险，以监控客户的活动

评估客户的商业资质和信誉

1. DPOS

委托权益证明（DPOS）是最快，最有效，最分散，最灵活的共识模型。 DPOS利用利益相关方批准投票的权力，以公平和民主的方式解决共识问题。所有网络参数，从费用表到阻止间隔和交易规模，都可以通过当选代表进行调整。

根据DPOS，利益相关者可以选出任意数量的见证人来作为记账节点。块是一组更新数据库状态的事务。每个帐户允许每个见证人每人一票，这个过程称为批准投票。选择完全批准的前N名见证人。确定见证人的数量（N），使至少50％的投票利益相关者认为有足够的权力下放。当利益相关者表达他们想要的见证人数量时，他们也必须至少投票给那么多见证人。利益相关者不能投票支持更多的权力下放，而不是他们实际投票的见证人。

每次见证人生产一个块时，他们都会获得奖励。他们的奖励由利益相关者通过他们选出的代表设定（稍后讨论）。如果证人未能产生块，则他们不会获得报酬，并且可能在将来被投出见证人列表。每个维持间隔（7天）更新一次活跃见证人名单。

当计票结束后，通过RAFT+共识算法以每2秒一个块的固定时间来产生区块。任何人都可以通过观察见证人参与率来监控网络健康状况。

选举代表的参数更改

代表的选举方式与证人相似。委托人成为特殊帐户的共同签名者，该帐户有权提议更改网络参数。此帐户称为创世帐户。这些参数包括从交易费用到块大小，见证工资和块间隔的所有内容。在大多数代表批准了拟议的变更之后，利益相关者将获得2周的审核期，在此期间他们可以投票给代表并使提议的变更无效。

选择此设计是为了确保代表在技术上没有直接的权力，并且所有对网络参数的更改最终都得到利益相关方的批准。这样做是为了保护代表免受可能适用于加密货币管理者或管理员的规定。根据DPOS，我们可以真实地说，行政权力掌握在用户手中，而不是代表或证人。与证人不同，代表不是有偿职位。但是，预计这些参数不会经常变化。

1. RAFT共识算法
   1. 一致性问题

在分布式系统中,一致性问题(consensus problem)是指对于一组服务器，给定一组操作，我们需要一个协议使得最后它们的结果达成一致。

由于CAP理论告诉我们对于分布式系统，如果不想牺牲一致性，我们就只能放弃可用性，所以，数据一致性模型主要有以下几种：强一致性、弱一致性和最终一致性等，在本节中，我们主要讨论的算法Raft，是一种分布式系统中的强一致性的实现算法。

强一致性的一般实现的原理：当其中某个服务器收到客户端的一组指令时,它必须与其它服务器交流以保证所有的服务器都是以同样的顺序收到同样的指令,这样的话所有的服务器会产生一致的结果,看起来就像是一台机器一样.

Raft 有几个特性：

强领导者（Strong Leader）：Raft 使用一种比其他算法更强的领导形式。例如，记账事件只从领导者发送向其他服务器。这样就简化了对记账事件的管理，使得 Raft 更易于理解。

领导选取（Leader Selection）：Raft 使用随机定时器来选取领导者。这种方式仅仅是在所有算法都需要实现的心跳机制上增加了一点变化，它使得在解决冲突时更简单和快速。

成员变化（Membership Change）：Raft 为了调整集群中成员关系使用了新的联合一致性（joint consensus）的方法，这种方法中大多数不同配置的机器在转换关系的时候会交迭（overlap）。这使得在配置改变的时候，集群能够继续操作。

* 1. 复制状态机（Replicated State Machine）

一致性算法是在复制状态机的背景下提出来的。在这个方法中，在一组服务器的状态机产生同样的状态的副本因此即使有一些服务器崩溃了这组服务器也还能继续执行。复制状态机在分布式系统中被用于解决许多有关容错的问题。

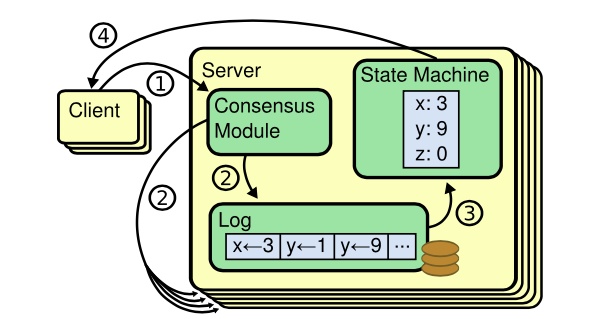


图-1：复制状态机的架构。一致性算法管理来自客户端状态命令的复制日志。状态机处理的日志中的命令的顺序都是一致的，因此会得到相同的执行结果。

如图-1所示，复制状态机是通过复制日志来实现的。每一台服务器保存着一份日志，日志中包含一系列的命令，状态机会按顺序执行这些命令。因为每一台计算机的状态机都是确定的，所以每个状态机的状态都是相同的，执行的命令是相同的，最后的执行结果也就是一样的了。

如何保证复制日志一致就是一致性算法的工作了。在一台服务器上，一致性模块接受客户端的命令并且把命令加入到它的日志中。它和其他服务器上的一致性模块进行通信来确保每一个日志最终包含相同序列的请求，即使有一些服务器宕机了。一旦这些命令被正确的复制了，每一个服务器的状态机都会按同样的顺序去执行它们，然后将结果返回给客户端。最终，这些服务器看起来就像一台可靠的状态机。

应用于实际系统的一致性算法一般有以下特性：

确保安全性（从来不会返回一个错误的结果），即使在所有的非拜占庭（Non-Byzantine）情况下，包括网络延迟、分区、丢包、冗余和乱序的情况下。

高可用性，只要集群中的大部分机器都能运行，可以互相通信并且可以和客户端通信，这个集群就可用。因此，一般来说，一个拥有 5 台机器的集群可以容忍其中的 2 台的失败（fail）。服务器停止工作了我们就认为它失败（fail）了，没准一会当它们拥有稳定的存储时就能从中恢复过来，重新加入到集群中。

不依赖时序保证一致性，时钟错误和极端情况下的消息延迟在最坏的情况下才会引起可用性问题。

通常情况下，一条命令能够尽可能快的在大多数节点对一轮远程调用作出相应时完成，一少部分慢的机器不会影响系统的整体性能。

1. 未来方向

BCAC共识算法的研究还在进行中，在下一版本的黄皮书中。我们会着重探讨以下问题：

• RAFT+共识算法。

• DPOS见证节点的奖励机制。

• 侧链技术和BCAC的大侧链概念。

• 数字资产在不同链之间的转移。

• BCAC的智能合约体系。

1. 结论

BCAC致力于通过侧链技术和共识算法，来解决区块链应用在落地时，现有公链无法满足其对于性能、架构、价格等的需求的问题。

参考文献

1. In Search of an Understandable Consensus Algorithm <https://raft.github.io/raft.pdf>
2. Delegated Proof-of-Stake Consensus <https://bitshares.org/technology/delegated-proof-of-stake-consensus/>
3. Know your customer <https://en.wikipedia.org/wiki/Know_your_customer>