NBCS 有限国家区块链 OS 内核

Author :陈书增 walksing@qq.com 20190710

目录

有限去中心化区块链

1，我们的社会中，几乎所有的机制，都是中心化的。

2，绝对的去中心化并不优于绝对的中心化，这点类似民主和集权的关系，中心化拥有集权带来的好处，而民主带来的坏处，去中心化也一个没落下。基本上，中心和去中心的概念推广到社会体制，就是集权和民主。

3 ,区块链并不直接带来绝对的去中心化 ,它只是一个可以用来去中心化的工具。就如同议会制 ,选举 ,投票 ,三权分立可以作为民主的工具一样 ,不同的区块链，根据采取的共识机制的不同 ,几乎就像是绝对民主 ,代议制民主这些不同的民主制度一样，提供了不同程度的去中心化。

综上，区块链是一种工具，但是，它和很多人描述的不同，它并不是一个创造无政府主义或者绝对自由和平等的工具，它只是一种能够去中心化的工具。并不是使用了区块链就会带来绝对的去中心化，而是，在目前这种几乎任何服务或者应用都必须通过中心化的方式提供的社会中，提供一种中心化的方式之外的，能够提供某种程度上去中心化的服务的选择。

去中性化区块的缺陷

区块链的去中心化，天然是以牺牲性能为代价的。同时，在成本上，区块链系统并不比中心化系统有天然的优势。此外，在匿名性，隐私性上，以目前的区块链技术，所能提供的优势很有限。所以说，现存的区块链系统和现存的中心化系统竞争的话，优势基本只有一个，就是去中心化，而劣势则非常多。

而相反，大量的区块链项目，尤其是采用 ICO 的公有链，为了吸引投资者，总是把目标市场定在某个大家最耳熟能详的领域，把自己描写成某个著名公司或者应用的替代者，例如，我们要取代银行（支付宝），我们要取代腾讯（百度），我们要取代滴滴等等，而这些领域，恰恰是中心化竞争对手最强大的领域，因为很显然，如果对手本身实力不强，那么它凭什么这么出名？而以目前的区块链技术，无论是功能，输出，还是隐私性，区块链和这些成熟的中心化应用，几乎都没有一战之力。

于是，区块链在这个领域和中心化系统竞争，只有两种可能——

a，对匿名性和隐私性远超其他性能的应用：例如黑市交易，洗钱。这里明确一点，区块链并不天然提供隐私和匿名性，但是，由于任何中心化系统都不可能提供绝对的隐私和匿名，所以区块链技术是唯一**有可能**实现隐私或匿名的技术。然而，目前在隐私和匿名方面，区块链技术仍旧很局限，基本上，除了账本，也就是数值交换系统之外，其他的应用都无法实现。

b，中心化系统实在是做得太烂的情况：例如，津巴布韦币这种。但是实际上，但凡是中心化系统做得不太烂，易用性和性能都还是强于去中心化系统。所以，目前的区块链技术性能和中心化系统还是差距很大，所以，除了某些性能不重要

的应用，例如之前说的洗钱这种，否则，基本上一般大众还是会选择中心化系统，毕竟中心化的概念更深入人心。

2，这里，是很多人忽略的，但却是区块链最有希望落地的领域。

首先，这个领域的公有领域很少，因为基本上，在公众的范畴内，能够产生中介的领域，经过了这么久的互联网热潮，基本上都已经被第三方占据了。所以能够使用区块链而且还没有中心化竞争对手的场景，几乎不存在。

但是，在具体的，非公众领域，这种场景有很多。

我们可以分为三类：

a）因为各种原因天然没法找到中介的。

b）利益太小没有中介生存空间的。

c）新出现还没有衍生出中介的场景。

a 类——只要考虑一个多方场景，如果多方有利益冲突，有信任问题，但是没有中介的，大抵都是此类。从这种角度讲，朝核问题也算，而且是个很好的例子，在国际性事务上，如果涉及到五常，而且其中几方有分歧，基本都谈不拢，因为没有哪个机构有资格当五常的中介。

这个并不是特例，而是一个很直观的例子——通常情况，能够作为第三方的，主要是政府和金融机构，还有一些互联网巨头。然而，它们之间想要找第三方的话，就会出现找不到第三方的尴尬情况。同理，如果涉及到跨国的一些大企业之间的合作，那么找不到可以信任的第三方的情况就很多了。

而区块链在这个领域就有大展拳脚的空间了，例如最早的联盟链之一 ripple，以及目前最大面向金融领域的 r3，都是这类公司。ripple 主要面向的就是银行跨国交易的结算问题，这东西就是一个困扰了金融界很久的问题，传统方式效率非常低下，而又没有这些跨国银行中介都能够信得过的结构当中介。区块链就是这种问题的解决方案。

b 类有很多，基本上，在产业链上横向或者纵向产生关联几个公司之间，经常会希望进行某种程度的合作但是又有信任问题，这个时候就需要中介。如果这几个公司是金融机构，那么刚才已经说了找不到中介的问题。如果这里面其中有个企业占主导地位，那么它可以充当中心或者第三方的角色。然而，如果没有，这些企业也不是政府，金融或者互联网巨头，那么他们通常就会找政府，金融机构或者互联网巨头当第三方。

但是，有的时候你想找第三方，第三方却未必看得上你，或者，第三方开的价钱太高。

于是，通常情况下，这种合作就只能作罢。

然而区块链就提供了这种可能性，目前这个方向，例如物流，供应链这种涉及多方的场景，都是区块链应用的热点。

c 类可以说是区块链应用的甜区，但是这方面的场景可遇不可求。目前我所知的一个很热门的领域是能源——去中心化的能源市场就是一个新兴场景，供给来自家用的太阳能板，需求来自电动车，而基础设施的数字化又刚刚由智能电网完

成。这个领域有中介的需求，但是暂时还没有中介进入，而这个时候区块链出现了，于是目前有不少在这方面应用的项目。

3，其实，这是才是区块链的潜力所在。

以上，2 是区块链能够迅速落地的领域，1 是我们看得到的区块链能够逐渐取代的目标，而这里，才是区块链技术令人兴奋的部分——我们目前大部分的应用和服务，都是中心化的，而现在，没人能够想象，去中心化的社会会是什么样的。

在生活中，其实类似于 2 里面所举的因为缺少信任或者第三方的情况比比皆是，而如果某个，或者某几个去中心化区块链达到了如同微信或者银行或者手机这种普及程度的话，人人都可以基于它架构一个去中心化的服务来解决信任问题，大到借贷，交易，财产转让，小到打赌，游戏，都不需要通过第三方进行。

这个，是区块链技术之所以被人看好的原因，就在于它拥有非常广阔的前景。

综上所述，我们需要去中心化吗？

答案是需要，可能不是你想的那些，但是，可能比你想得还更需要。

最后回应一下你问题里面的部分。

1，可信度。首先，区块链不仅仅是可信的储存，可信的储存只是输出，区块链是一个能够保证输出可信的系统。

其次，其实，源头造假是个问题，但绝对不是唯一的问题，造假账的可不一定是刚记上的时候就造假。诚然，区块链领域目前的一个难点就是如何保障数据来源的可信，因为区块链本身并不能保证这个。然而，区块链能够做到如果有人造假，他的记录可以被溯源，可以被检测，可以被追责，这个人可以被黑名单，很多情况下，这已经是最好的结果了。而在很多中心化系统中，你做不到这一点。

再次，你所说的例子，恰恰是中心化的问题。刷信用或者水军这种东西，技术上想要防止太简单了。之所以这种情况存在，恰恰是因为完全防止刷信用这种东西，对于中心是不利的。例如某宝，你难道觉得它是个中立的平台？是商家在养着它啊！它自然会站在商家一边，刷单这种事只要不过分，它没有任何理由去制止。

2，安全性，区块链并不保证安全性。它不比传统系统更安全，也不比传统系统更不安全。如果说你觉得公私钥加密系统安全的话，你可以自己把你存在云盘里的东西加密一遍。如果你觉得记私钥太麻烦的话，你也可以把它存在你云盘里。

3，稀缺性，稀缺性和区块链以及去中心化没有一毛钱的关系。

4，容量。容量是大问题，去中心化系统容量天生不如中心化系统，所以，需要高容量的应用，可以根据需求选取中心化程度较高去中心化程度较低的区块链系统，基本上，所有的所谓大容量高并行低延迟的区块链系统，其实都有某种程度上的中心化，中心化程度越高越快。

之前已经说了，区块链提供的不是完全的去中心化，而是，你可以用它在任何层面，进行任何程度的去中心化。所以，你对容量需求高，就少去中心化一点好了，至少在可靠性上，它可能会比完全中心化的系统强。

但以上两点已经说明 ,去中心化本身 ,其实并没有天然的优势 ,和中心化系统比，最终还是看哪个更好用。

现有区块链背景缺陷

挖矿和共识协议的弱点

1、中本聪一失之虑

比特币的设计者中本聪毕竟不是神，他在设计比特币时，以去中心化为根本前提，原本希望利用分散的计算资源，通过每个人的计算机解决算力问题，以完成区块链共识和交易上所必需的复杂计算，所以设计了 PoW，以奖励参与计算的节点。在这份协议的基础上，全球每个比特币的参与者都可以开动自己的电脑进行挖矿，公平参与来获取比特币。

但后来的发展应该是设计者不想看到的：由于 CPU 挖矿效率极低，人们发现 GPU 效率相对高点，发展出 GPU 挖矿，再后来有 FPGA，最后发展到 AISC（专用集成电路）挖矿，如果说 GPU 挖矿还和“人人为我我为人人”沾点边的话，那么 AISC 专业矿机的诞生就彻底背离了当初中本聪“一机一票”的设计初衷。

从此 PoW 机制仿佛进入了军备竞赛，最后矿机的集中分布形成了矿场，算力的中心化让后来者无法公平参与。同时算力的过于集中不利于整个比特币网络的安全性，毕竟还有著名的“51%攻击”的潜在威胁。

所谓“矿池”,就是大家整合算力,一起解决同一道题。这种方式需要统一管理，一般做法是矿池开出任务，并准备适合的奖励措施，无论算力高低，把一种类似赌运气的挖矿赌博变成一种统计学的回报，以降低回报的波动性。这种工业式的挖矿革命将随着 PoW 共识机制的推广而逐渐完善

2、挖矿和算力集中困境

矿池算力集中化带来的相关安全话题是一个热门话题。曾经有一段时间，比特币是一个大众参与的游戏，人们使用自家的家用电脑可以碰运气挖比特币。然而，随着挖矿难度的增加，专业的计算机芯片和专业的比特币采矿集团出现了，并形成了一些大规模的矿池。它们主要分布在中国，以及一些电力便宜的国家和地区。

比起区块链技术应用落地的困境，比特币“挖矿”的生意风景这边独好。这里展开的，是一场“算力”的军备竞赛。由于比特币的机制，矿圈的这场“权力游戏”，胜者甚至可以决定比特币的命运和走向。

因为大多数区块链共识算法的“51%攻击”问题,以及日益集中的矿池算力，导致我们的争议焦点集中在去中心化系统以及实际上日益集中的算力导致的中心化争论上。目前实际上并未出现 51%攻击的问题，但不可否认，算力的集中至少违背了比特币去中心化的初衷，成为其继续发展的一大隐患。

3、其他共识算法及其问题

区块链的自信任主要体现在分布于区块链中的用户无须信任交易的另一方，也无须信任一个中心化的机构，只需要信任区块链协议下的软件系统即可实现交易。

这种自信任的前提是区块链的共识机制，即在一个互不信任的市场中，要想使各节点达成一致的充分必要条件是每个节点出于对自身利益最大化的考虑，都会自发、诚实地遵守协议中预先设定的规则，判断每一笔记录的真实性，最终将判断为真的记录记入区块链中。换句话说，如果各节点具有各自独立的利益并互相竞争，则这些节点几乎不可能合谋欺骗用户。而当节点们在网络中拥有公共信誉时，这一点体现得尤为明显。

共识机制	代表	优点	缺点
PoW	比特币，莱特币	实现简单 安全可靠 网络资源消耗小	计算资源消耗大 易分叉 速度慢
PoS	Peercoin，NXT 和 Qtum	资源消耗少	实现复杂 安全漏洞 网络资源消耗大
DPoS	Bitshares，EOS，LISK	资源及网络资源消耗小 吞吐量高 共识时间短	实现复杂 安全漏洞
PBFT	Fabric0.6	共识效率高，可实现高频交易	当系统只剩下 33% 的节点运行时，系统会停止运行
DAG	IOTA，Byteball，Nerthus	高吞吐量，高并发 异步通信	实现复杂 同步难 网络资源消耗大

区块链各种共识机制的比较

共识机制最好的设计是提供可插拔模块化共识。共识算法的选择与应用场景高度相关，不同的应用应该有不同的共识算法的选择。

交易效率问题

1、比特币和以太坊的交易效率困境

谈到交易效率，首先我们需要一个衡量指标，在区块链系统中用 TPS 指标来衡量一个系统的交易效率。

TPS 可基于测试周期内完成的事务数量计算得出。例如，用户每分钟执行 6 个事务，TPS 为 0.10 TPS。同时我们会知道事务的响应时间（或节拍），如此例中，60 秒完成 6 个事务也同时代表每个事务的响应时间或节拍为 10 秒。

一个系统吞吐量通常由 TPS、并发数 2 个因素决定。每套系统的这两个值都有一个相对极限值。在应用场景访问压力下，只要某一项达到系统最高值，系统的吞吐量就上不去了，如果压力继续增大，系统的吞吐量反而会下降，原因是系统超负荷工作，上下文切换、内存等等其他消耗导致系统性能下降。

根据这个指标，以比特币为例，其 TPS 约为 7，以太坊大概为 20，换算到一天 24 小时的概念，大概相当于比特币 30 万笔/天，以太坊 45 万笔/天。

根据 Blockchain 的数据，投资者大概需要平均 78 分钟来确认一次比特币交易。个别时段，这一平均时长一度高达 1188 分钟，也就是将近 20 小时。这将大大降低用户使用比特币的兴趣。

2、比特币扩容

一种货币不是天生就有价值，而是很多人相信它有价值的时候才会有价值。这也可以说在一定群体里形成的“共识机制”。由于前面提到的比特币交易速度慢的问题，比特币扩容一直是社区里被广泛重视的一个重要问题。

首先要澄清的一点是，比特币扩容不是增发比特币，而是针对比特币交易量不足增加比特币的交易量上限。而为什么要增加交易量上限呢？

比特币最初的设计是规定每 10 分钟(左右)挖出一个大小为 1MB 的区块，每笔交易平均下来是 250 字节，于是，每块可以放进 4000 笔交易，换算成每秒则近似等于每秒 7 笔交易。这个数字太小了，比如 Paypal 是每秒 100 笔量级的，而像支付宝这种集中式交易系统，在“双十一”的时候可是每秒 100 000 笔量级的。和它们一比，比特币根本就不能称之为交易系统。

在比特币的扩容问题上有两个技术难题。一是技术上如何实现，即扩容多少合适。第二个问题是如何实施。考虑到比特币系统是一个分布式系统，它面临的实施层面的问题会更大，因为涉及在实施层面上的新旧节点如何协调，新旧账本如何共存和互认的问题。

分布式系统的升级必须让每个节点都升级才行。如果有人不升级，将会产生分叉。

3、比特币的隔离验证、闪电网络与侧链

区块链的可扩展性问题，至今仍旧是一个学术难题。例如交易量问题一直是比特币的最大问题，那么如何实现比特币交易量扩容？简单说应该有以下 4 种方式。

- 改变比特币采用的 **PoW**（工作量证明）共识机制

  这相当于改变了比特币的安全机制，或者说采用其他共识机制来进行比特币的升级很难得到原有比特币相关人员的认同。因为比特币已经承载了太多的用户和价值，甚至还承担了整个数字货币和区块链旗帜的重任。想要完全更改共识算法，冒着不可预测的风险去扩容，无论是投资者、矿工、开发者，都不会轻易答应的。

- 可以**改变区块大小**，但是不能增得太大，因为数据存储和传输工作量会大大增加。
- **改变区块生成间隔。**这个间隔可以缩小，但是会使得比特币的网络出现大量的孤块和分叉，造成大量的算力浪费和安全隐患。
- **修改数据存储规则**，相同大小的区块能承载更多交易。

隔离验证就是一种能够在不增加区块大小的前提下增加交易容量的方法。

前文介绍过，比特币的一笔交易大概 250 字节，主要数据包括以下 2 个部分：

- **转账记录**，也就是交易方和交易额；
- **用户有权利做这笔交易的证明**，这个证明是一组数字签名。

实际上，比特币的签名数据很大。粗略估计，签名大概占了交易大小的 2/3。

这样，我们就可以把交易里所有的签名单拉出来，然后把所有的签名打包放在数据块的后面，可以节省大约 2/3 的空间。也就是说，每笔交易都被分成了 2 部分：交易和见证（签名）。交易部分只有 100 字节左右，于是一个 1MB 的区块里面能放 10 000 笔交易（原来是 4000 笔），然后，所有的见证部分，大约 1.5MB～2MB，都被放到了后面。

采用了隔离验证技术的新节点当然可以接受这种数据格式，而旧节点虽然不能识别数据块后面的见证部分，但它们仍旧会认为前面的部分是合法的区块。这样通过软分叉就可实现隔离见证的升级。采用这种隔离验证的方法，大约可以让比特币提高 2～3 倍的交易量。

除此之外，隔离验证还修复了比特币一个被称为“可变性”（Malleability）的缺陷。比特币的签名方式比较复杂，其签名只针对 UTXO，并不包含交易里的所有信息。这样的话，攻击者可以改变交易里的信息，也可以改变交易 ID，但签名信息仍然有效。隔离见证将签名信息从交易中提出来，可以针对整个交易签名，使得比特币的交易不能改变，交易 ID 可以固定。更重要的是，可以更容易地实现一个叫作“闪电网络”的技术。

闪电网络是比特币的一个不改变主链结构的扩容机制，简单说就是一个在链上提供担保的链下交易机制。实际上就是在比特币上签署一个协议，在比特币主链以外再架设一个通道，用户的币存在这个通道上可以进行快速支付。闪电网络是一个去中心化架构的网络，和传统的交易所有本质区别。

例如你经常给某个人转钱，你不用每次都把交易上传到比特币的链上。你们双方可以先在比特币上签署一个协议，交一笔保证金，然后只要你们之间转账的总额不超过保证金，转账就可以私下进行，而这个协议保证如果对方耍赖了，你可以凭着转账记录上传到区块链上把属于你的钱拿走，不用再次通过对方授权。这种方式其实和主链交易没有可比性，它完全是另一种交易形式，提供了另外一种支付手段。闪电网络可以将一部分交易挪到链下进行，减轻了主链的负担。

在交易过程中，闪电网络允许创建“微支付渠道”，类似交易双方建立一个交易链，多笔比特币交易在无须与主链进行互动的情况下，仍能安全地进行。这些在通道中的支付交易速度极快，与当前的比特币支付需要冗长的交易验证时间不同，交易链中的交易只有最后一笔需要真实地进入比特币区块链。如果任何一方终止合作，或者说在约定的时间内没有响应，该通道可以被关闭。重要的是，这种支付是可路由的，它是跨越多跳路径建立的专门通信管道。

相较于为每一个新的合约方创建一个渠道，你可以维持一些渠道，连接少数良好的安全中介机构，并通过他们来完成交易。这就是简单的支付通道背后的思路。目前已经存在这种支付通道。你可以一直向某人发送可替换的交易，每次额度比上一次大一点点，一旦达到某种条件，通道被终结，只有最后一笔支付向全网广播。

事实证明，只需要少量几乎没有争议的比特币升级，人们就可以生成更加通用的支付通道，它允许双向支付，也允许“条件支付”。条件支付允许用户构建一个支付网络。实际上，用户可以通过安全和非信任依赖的方式设定一些条件，

例如“如果张三支付了李四，我就支付给张三”。一些事情发生之后，用户的钱包就会自动向比特币网络广播这个条件支付交易，然后等待。

从理论上来讲，这种分布式小额支付网络（闪电网络）可以将比特币的日交易量扩充到数十亿笔，并且极少地使用到区块链，以及仅需少量的交易费。

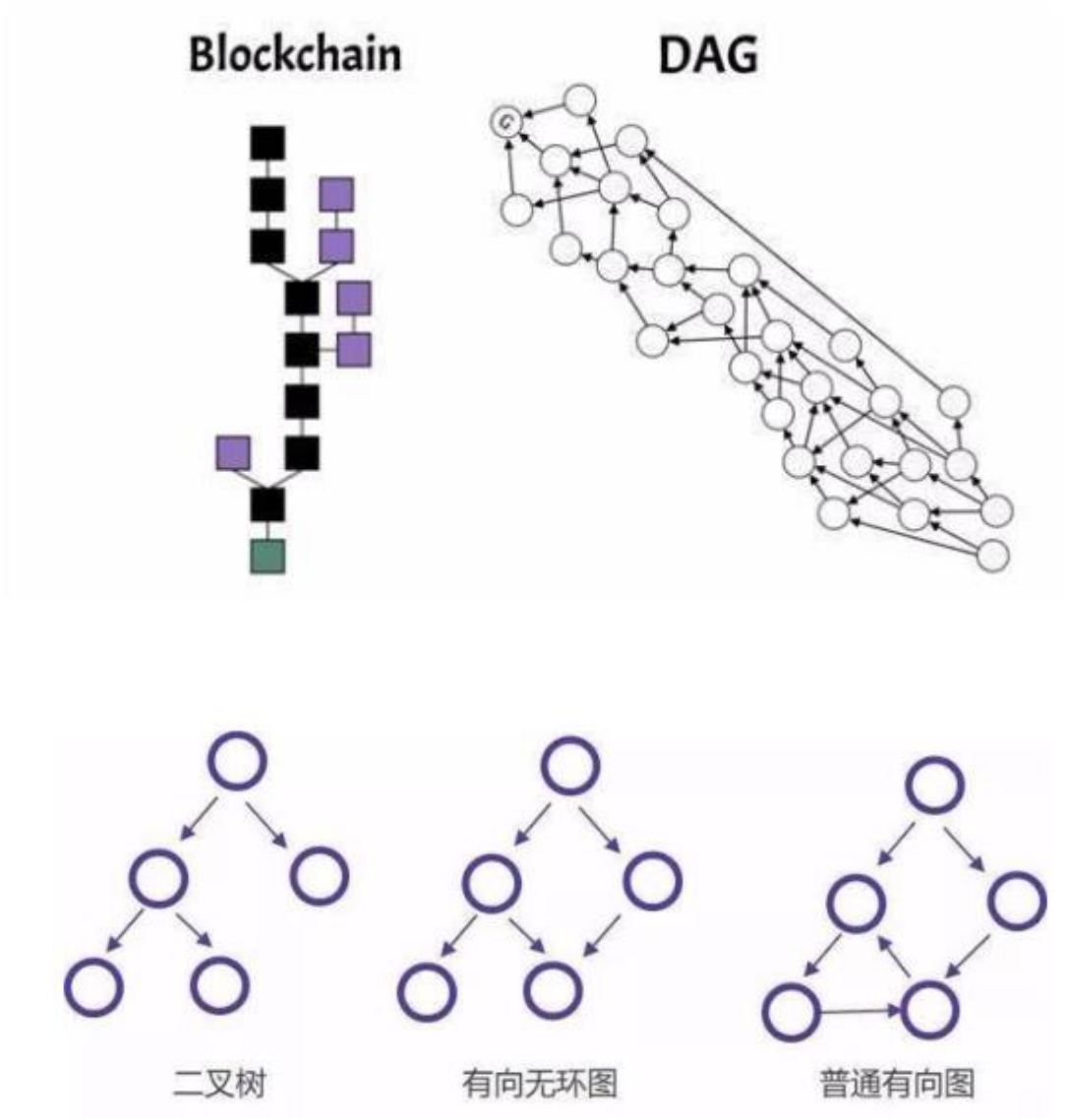
当然这种闪电网络的机制也存在安全漏洞，如果在这个通道里的交易在未得到主链的确认之前出现安全问题，将会导致一些交易无法确认，造成财产损失。

闪电网络论文提出了生成通道和支付网络的机制。它也是如今比特币创新的一个热点。

侧链是以锚定比特币为基础的新型区块链，就像美金锚定到金条一样。比特币在区块链里相当于是货币体系的黄金地位，具有最去中心化、最多分布节点、最公平区块链。侧链是以融合的方式实现加密货币金融生态的目标，而不是像其他加密货币一样排斥现有的系统。利用侧链，我们可以轻松地建立各种智能化的金融合约，如股票、期货、衍生品等。用户可以有成千上万个锚定到比特币上的侧链，特性和目的各不相同，所有这些侧链依赖于比特币主区块链保障的弹性和稀缺性。比较著名的比特币侧链是 Rootstock 和 BlockStream 推出的元素链。

4、基于 DAG 的提速技术

DAG（Directed acyclic graph），有向无环图，是计算机领域一个常用的数据结构。因为独特的拓扑结构所带来的一些特性，它经常被用到处理动态规划、导航中寻求最短路径、数据压缩等场景中。



第一次提出 DAG 跟区块链结合是在 Nxt 社区，可以发现 DAG 最初出现就是为了解决区块链的效率问题。比特币的效率一直比较低，基于 PoW 共识下的出块机制是一个原因，由于链式的存储结构，整个网络中同时只能有一条链，导致出块无法并发执行。社区有人提出用 DAG 的拓扑结构来存储区块，这个时候更多还是类似侧链的解决思路，不同的链条存储不同类型的交易，降低出现“双花”的可能，在之后某个节点需要合并的时候，几个分支再归并到一个区块。

通过以上设想我们可以改变区块的链式存储结构，变成区块 DAG。在区块打包时间不变的情况下，网络中可以并行地打包 n 个区块，网络中的交易就可以容纳 n 倍。

这时候 DAG 跟区块链的结合还是停留在侧链的思路，不同类型的交易可以并行在不同的链条进行，达到提升性能的目的。这时候的 DAG 还是有区块的概念。

但是区块的概念其实也是妨碍我们提升效率的关键因素。那么，可不可以没有区块的概念呢？为什么一定需要区块呢？能否让每一笔交易直接参与维护全网的交易顺序？这样交易被发起后直接跳过打包区块的阶段，直接融入全网，如此达到所谓的“无区块”（blockless）效果。这样确实连打包交易出块的时间都省去了，DAG 最初跟区块链的结合就是为了解决效率问题，现在不用打包确认，交易发起后直接进入确认网络，理论上效率自然提高很多。

自此，以 blockless 独树一帜的 DAG 区块链雏形基本形成。其中 IOTA 和 Byteball 在市场上的表现最为耀眼。DAG 系的区块链有些概念很有趣，了解这些概念更容易理解 DAG 技术。

DAG 与链式结构的本质区别在于异步与同步通信。DAG 通过将事务操作进行异步处理来增加网络吞吐量，采用某种传播算法在节点间发送操作日志，并通过某种机制（IOTA 每次验证前 2 条交易，并计算一个 PoW 代表权重）将一个权重赋给该操作。相比起同步操作的链式结构，DAG 结构与任何异步机制一样，

能够带来的提升在于吞吐量,但是产生的问题则在于无法有效预测交易被确认的时间与周期。

DAG 网络一个重要的问题就是解决网络宽度。DAG 网络中,每笔交易被确认,都需要链接到已经在网络中存在的并且比较新的交易;如果都选择网络中比较早的交易,会导致网络宽度过宽,新的交易难以得到确认。理想的状态是,新的交易发起时,选择网络中已经存在并且比较新的交易做链接确认,这样网络的宽度保持在一定范围,能让新的交易有足够快的确认时间。DAG 的主要特点如下:

- **交易速度快**:DAG 摒弃了区块概念,交易直接进入全网中,所以交易速度预期比基于 PoW 和 PoS 的需要出块的区块链会快很多;
- **无须挖矿**:DAG 把交易确认的环境直接下放给交易本身,无须由矿工打包成区块后同意交易顺序。所以 DAG 网络中没有矿工的角色;
- **无手续费**:交易发起只需要做简单的 PoW 工作量证明,整个网络中的 PoW 都是发起交易者自己做的,而不是交给矿工,所以发起交易无须手续费;
- **需要见证节点**:DAG 需要见证人机制的存在,这一部分不管是 DPoS、PoS、PBFT,大家最终都会在效率、安全性上寻求一种平衡。

5、其他提速思路

目前区块链效率问题比较突出,但是笔者相信随着时间的推移会有更多的新技术产生,提速可以从以下几个方面来考虑。

网络带宽:网络带宽的发展会进一步允许更好更先进的分布式共识机制的产生;

硬件速度：包括各种 CPU、GPU 等硬件速度的不断提高会大大提高区块链的效率；

共识算法：目前的算法都有缺陷和不足，将逐步发展，协议也将不断完善；

并发执行：链状结构理论上缺乏并发机制，类似 DAG 之类的异步并发技术也将不断完善；

数据格式：区块链里存储的数据格式可通过压缩技术存储，提高区块链的运行效率。

系统升级维护问题

1、硬分叉史记

以太坊：2017 年成功实施的“拜占庭”硬分叉，通过对底层协议的升级创建新的规则，来完成对整个系统的性能提升和功能增设。2017 年 10 月 16 日，以太坊官方宣布，“拜占庭”在以太坊第 437 万个区块高度成功实施硬分叉，将协议升级后调整了区块奖励，减小区块大小，并为平台上包括区块链隐私性等问题引入了零知识证明等解决方案，完成了开发人员打造更为适合去中心化应用生态环境的技术目标。

a）以太坊（ETH）和以太经典（ETC）

The DAO 计划基于以太坊智能合约建立一个众筹平台，于 2016 年 5 月正式发布，截至当年 6 月，募集资金超过 1.6 亿美元。之后，The DAO 被黑客利用智能合约的漏洞，转移了市值五千万美元的以太币。为了挽回投资者资产，以太坊社区投票表决决定将更改以太坊代码，希望索回资金。为此，以太坊在第 1,920,000 区块进行硬分叉，回滚所有以太币（包括被黑客占有的）。

但是，有一部分人认为以太坊这种做法违背了区块链的去中心化和不可篡改精神，坚持在原链上挖矿，从而形成两条链：一条为不承认回滚交易的链—以太经典（ETC），一条为承认回滚交易的链—以太坊（ETH），各自代表不同的社区共识以及价值观。分叉时持有以太币的人在分叉后会同时持有 ETH 和 ETC。

以太雾（ETF）是以太坊在 2017 年 12 月 14 日分出的公有链，主打雾计算的创新技术，增加了分布式储存和分布式计算的能力，拥有缩短网络延迟、节省计算资源、减小核心网络压力的优势，同时带来更高的可靠性。

b）比特币黄金

比特币黄金（Bitcoin Gold，BTG）是在 2017 年 10 月 25 日左右的又一次比特币硬分叉产物。比特币黄金是对大矿工们集中算力的一种对抗，比特币矿工越来越多地使用定制的 ASIC 来挖矿，但 ASIC 价格昂贵，只有大量买进时才会降低价格，所以大矿工们可以通过较低价大量买进 ASIC 来获得巨大的算力，导致比特币网络的算力被集中。比特币黄金将使用一种新算法来避免情况恶化。

2、系统升级维护难题和分叉

区块链系统的升级维护包括硬件和软件两个方面

硬件方面将随着技术的发展而逐渐完善，随着区块链的发展，将有更多的区块链硬件设备涌现，包括矿机、芯片、区块链硬件节点，以及各种应用相关类硬件出现。比如基于区块链系统设计的各种物联网设备、智能电表、水表、气表、手机以及各种穿戴设备等。

软件方面的升级主要包括以下几个方面。

- **数据结构**：例如比特币现金（BCH）从 1MB 区块改为 8MB 区块就是一种数据结构的升级；
- **共识算法**：随着系统的运行，最初设计的共识算法满足不了系统日益发展的需求时可以修改共识算法，带来的将是系统的升级；
- **加密算法**：算法问题是区块链安全的核心，再安全的算法也是百密一疏，因此随着黑客技术的进步将不断催生加密算法的改进和升级；
- **应用升级**：系统的应用发生改变时也面临升级问题；
- **漏洞修补**：任何软件系统将不断完善，寻找自身漏洞并不断完善。

以上任何一种类型的修改都将可能导致分叉的出现。当然分叉也包括人为因素，因为毕竟区块链网络是由人来控制的。分叉后不可避免地会出现新、旧链之间的数据协调以及用户的分流问题。以上内容，就是区块链行业的常见问题分析。

NBCS 国家区块链内核架构

我们建立了一种基于量子并行计算模式的分布式存储引擎系统改造的 NBCS 国家区块链系统，建立一种真正可落地的应用场景内核架构。

QOS 具有以下特点：

1） 高效率的数据存储处理能力，秒存，秒取

2） 交易量 理论 TPS 1000000+

3） 安全性高所有节点扩展以 2 的 n 次方几何级路由扩展。扩展后节点数据自动重新均衡转移。不会影响老用户数据使用

4） 数据节点加密授权基于集中式委托中央政府背后可信赖的企业。以国家信誉为担保。

5） 数据难以修改，可追溯 用户与用户之间通过父子 usrid 进行级联，智能分润

6） 自实现编译器动态解析，安装，卸载 智能化合约 ACS，ACS 存于用户大数据中心 AFS，编译解析指令过程 ACS 合约代码不出底层 AFS

7） AFS 可支持大用户数据中心全民共享，账单大用户中心，区块部落节点

8） AFS 具有异步非阻塞通讯存储秒存秒读数据能力.

9） AFS 根节点是集群规避单点故障，当一个节点不可用自动尾盘给顺序的后续节点。具有智能感知状态，不需要进行议会选举。采用中国共产党军衔制度，上级领导挂了自动由次级领导跟上。军长挂了依次，师长，旅长，团长…

10） 所有数据分布式存储在云中心，用户无底层访问权限。所有数据存取是通过 QOS-VME 接口代理执行。保障底层系统安全性。

11） 扩展性强，可轻易扩展为其它系统。

12） VME 自带 job 执行器，支持秒调度执行；一个 job 执行失败不会影响到整层 VME 其它 job.

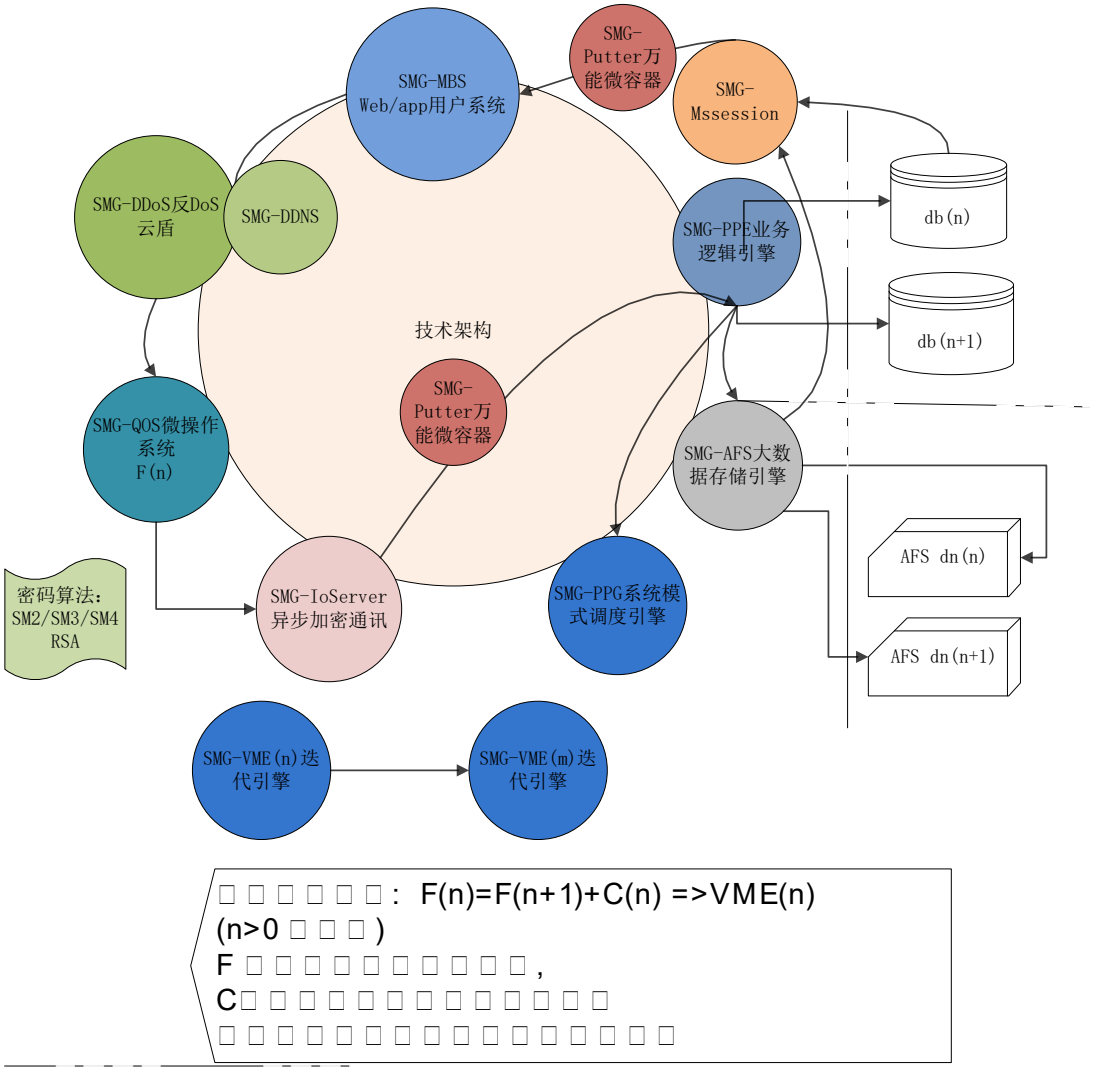
13） 不需要进行 PoW,PoS 工作量证明，不需要挖矿。需要可信集团提供高可靠存储刀片服务器。

14） 跨节点 ZKP(零知识证明) QOS-VME 容器版本安全性。

1 QOS-VME 技术架构图

NBCS Kenerl OS
（国家区块链内核系统）

Runus 20190629



说明:

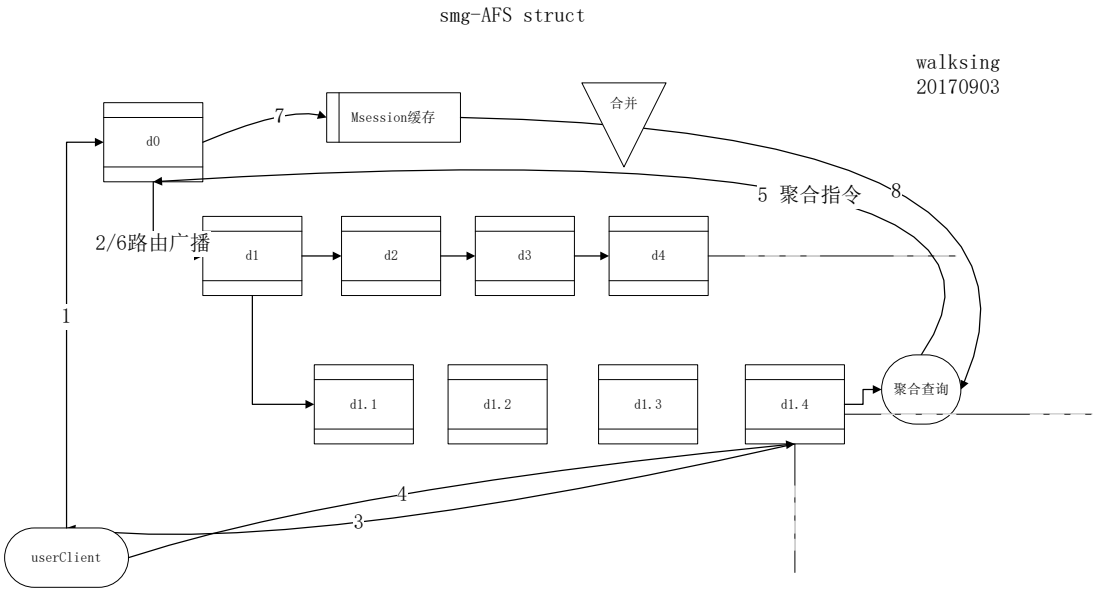
1) 用户界面系统 SMG-MBS 完成大用户的注册,登录,各个运营商的运营.数据统计.有 web 版,webapp 版.可实现注册登录,数据查询,交易,视频连接,服务调度等.有 Msession 缓存.Putter 微信息数据交换.
2) 系统安全由 SMG-DDoS 反 dos 云盾.进行 DDNS 流量清洗.以及动态 IP 前端无痕代码验证机制进行数据前端加密解密.
3) 底层消息由操作系统进入 SMG-QOS 量子操作系统经过 IoServer 异步通讯加密传输.传输给 SMG-PPE 业务逻辑引擎.
4) PPE 分发数据给 db 数据节点进行业务数据处理,部分数据以 SMG-AFS 大数据存储引擎,存储在 AFS. AFS 支持任意节点自动扩展.支持海量数据迁移..

5) SMG-PPG 系统模式引擎进行消息调度,并执行 job(作业).并实现数据定时采集,数据分发,流程处理.
6) 支持国密植入算法加密核心数据

2 AFS 异步非阻塞分布式存储

重新设计分布式存储系统 AFS 采用几何级路由树扩展 2 的 n 次方扩展

2.1 AFS 结构算法图



1)d0 ->dn vme路由节点支持迭代

2)所有的路由操作需要根节点d0完成

3)vme 引擎支持forward/backward 指令 .如聚合算法forward 遍历所有子节点.

4)每个节点有自己独立的Msession缓存.

5)所有VME 系统模式相同，业务逻辑系统相同，可处理不同业务系统。

6)当需要增加子节点时.原有的根节点数据自动分发到子节点.原有节点升级为根节点.根节点不存储数据.只负责调度转发数据与指令.

7)实例中用户通过d0根节点计算返回子节点给客户端,客户端后续通信可跟子节点d1.4建立通信.如果发送聚合指令,该节点再向跟节点d0派发路由请求.聚合结果后发给d1.4. 由d1.4返回给客户端.

8）普通数据的读取，写入指令由代理客户端之间输入pk按主键id进行动态映射算出地址，直接向数据 d(n)节点建立连接发送通信指令。

9）集群节点的扩充，以2的n次方+1几何级幂函数进行扩展。其中1 为父节点。

10）所有节点共享一组lib库

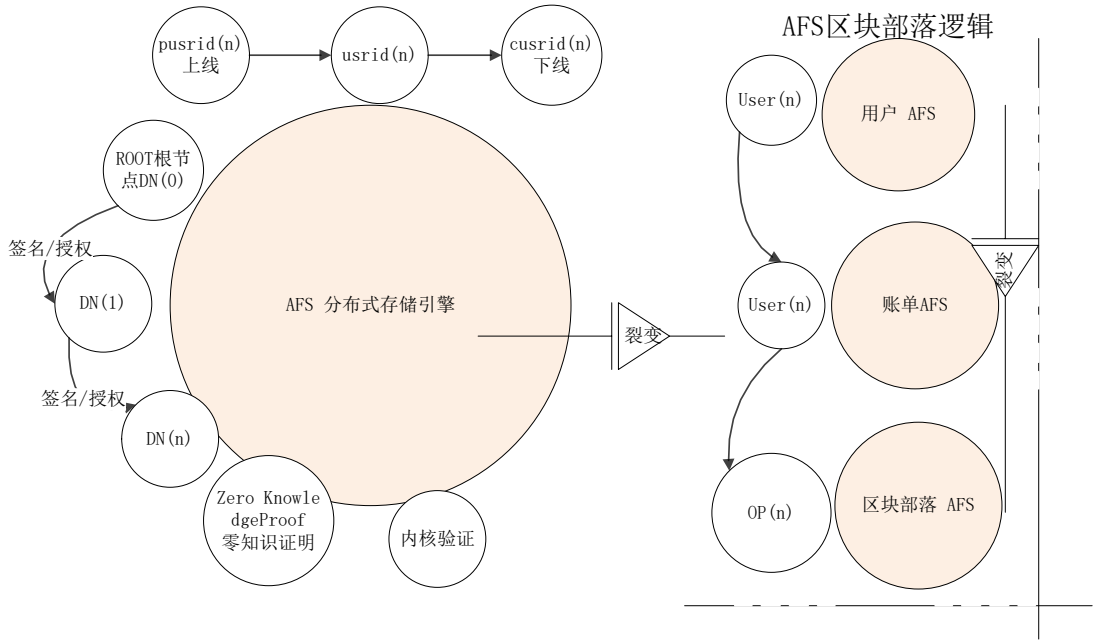
11)节点存数据以Queue 队列进行块写数据.

12)节点在存储数据时，支持指令触发智能合约，先解析结果更新写容器Putter.再flush写回AFS永久保存。

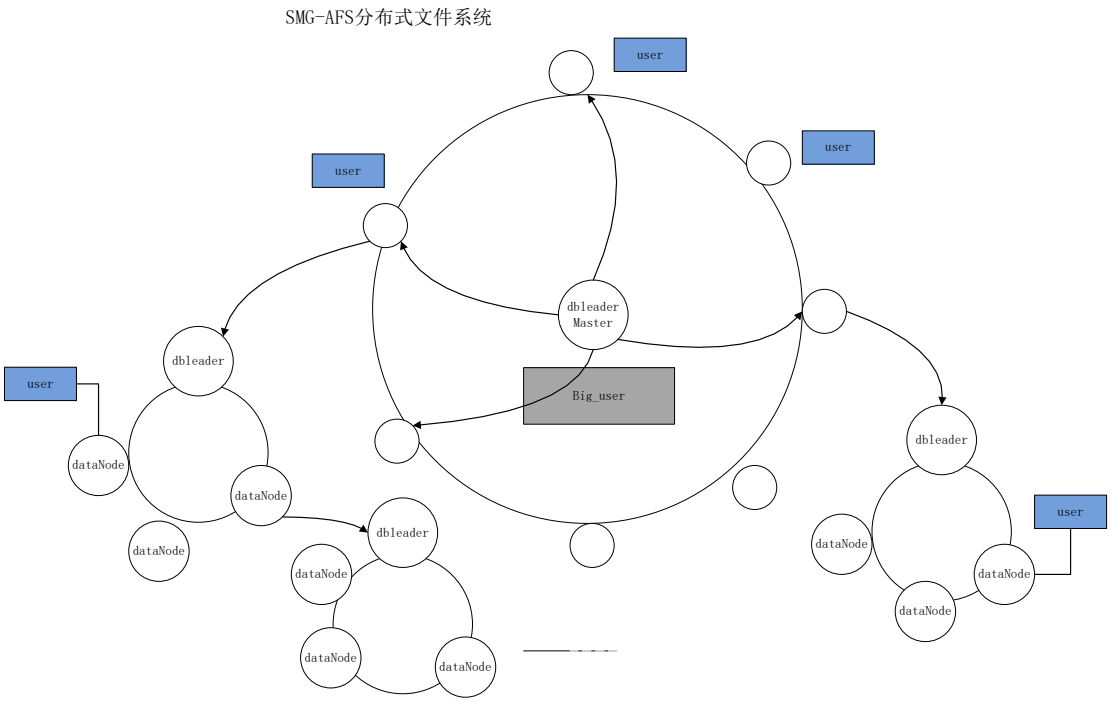
13)智能合约存在用户AFS的特点标识的key内，通过指令特殊标记被编译器动态解析触发执行，存储的是智能化合约类java小程序源码，可被加密

14）单元数据写长度如果超出原包长度，则自动扩展重新追加到大数据块文件尾，原数据块自动以空格替换标识删除块，并标记已删除pk。

2.2 AFS 节点扩展裂变逻辑图



2.3 SMG-AFS 架构

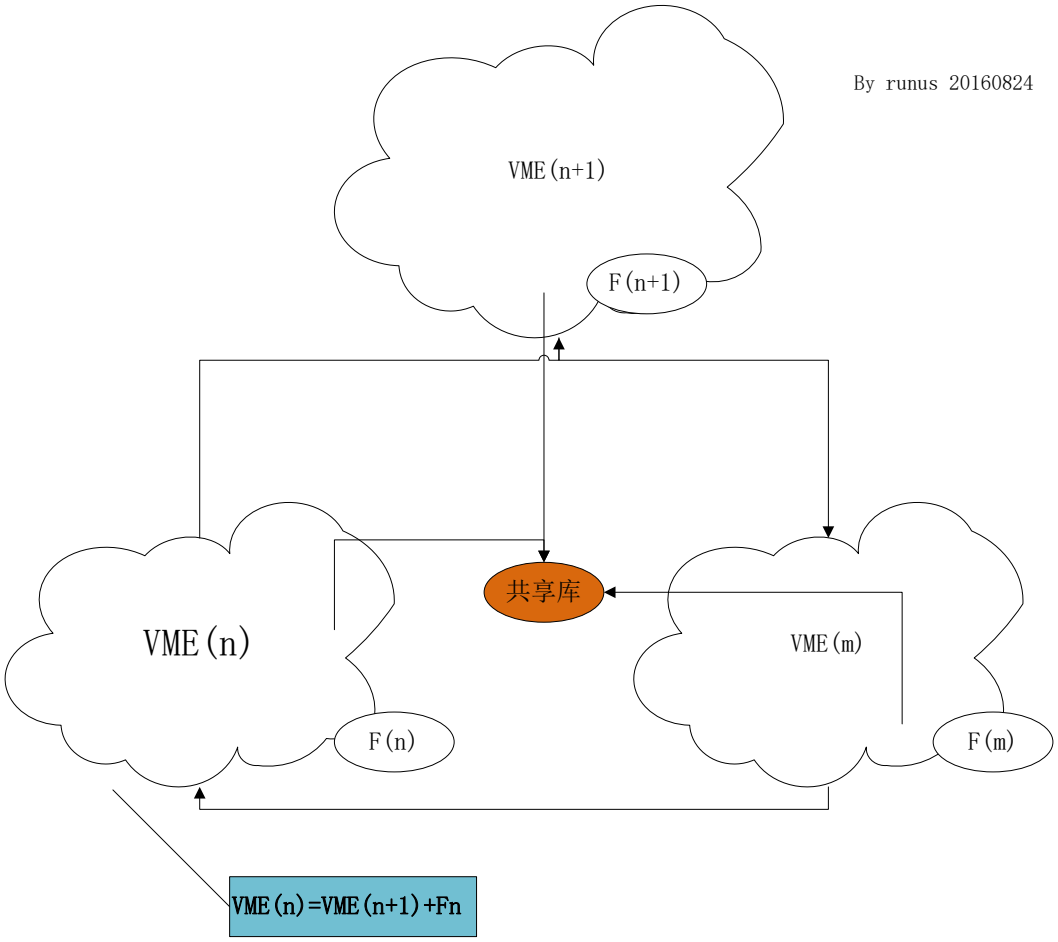


分布式数据库,架构可实现数据的无限扩展.
采用路由概念.每一个节点上级有 leader 进行管理.每一维度下节点数相同;二级维度下节点数不同.通过扩展维度,节点数实现网络按立体结构进行扩展.每扩展一维度按 2 的 n 次方几何级进行扩展.可扩展维度数不限.所有维度共享 lib 库.支持自我迭代调度.数据执行以异次元结构进行异构调度.

3 QOS-VME 量子迭代微操作系统

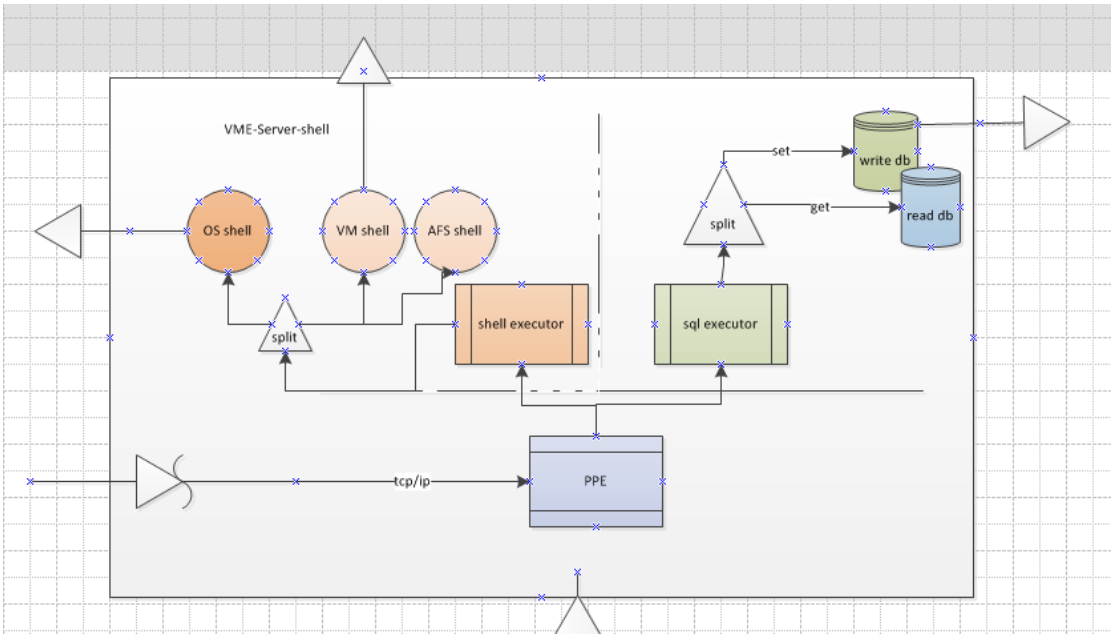
节点直接共享操作系统 系统模式系统(PPG) +业务逻辑系统（ PPE ）

任何系统由这两部分组成，组成千变万化的子系统



一个引擎的数据输出送给第二引擎的数据输入. 引擎之间共享一组程序库.

3.1 PPE SHELL



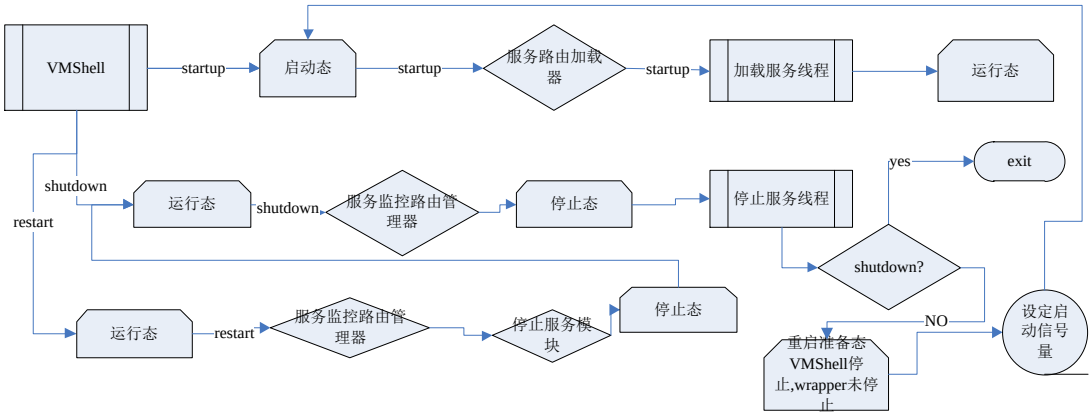
规则描述：

1） PPE 接收来自用户的请求
2） 请求识别指令为 shell mode,sql mode 分别交给 shell 执行器,sql 执行器,AFS 引擎进行处理
3） 如果是 sql 执行器 分离读写指令 ，将写数据发送到写数据库 ， 读数据直接读数据执行操作返回
4） 如果是 AFS 模式则发送指令给 AFS 进行处理.
5） 如果 shell 指令 则进一步分离 vmshell ， 如果不是则执行 OS shell 返回

vmshell :包含用户增加，删除，权限修改 ， 密码修改 ,连接池状态查看等命令 包含基本的认证服务以及操作系统 shell 扩展服务。用户调用授权服务；授权用户可通过 vmshell 进行 telnet 远程登录执行服务器的 shell 权限，必然查看日志权限，查找分析统计日志。通过 shell 可对服务器进程进行 kill 杀。并可对服务器重启，关机

通过 OS shell 可操作底层操作系统 ,通过 sql shell 可操作底层数据库
通过 AFS Shell 可间接操作底层 afs 大数据的基本查询.以及核心数据的计算分析.

3.2 VME 运行结构图



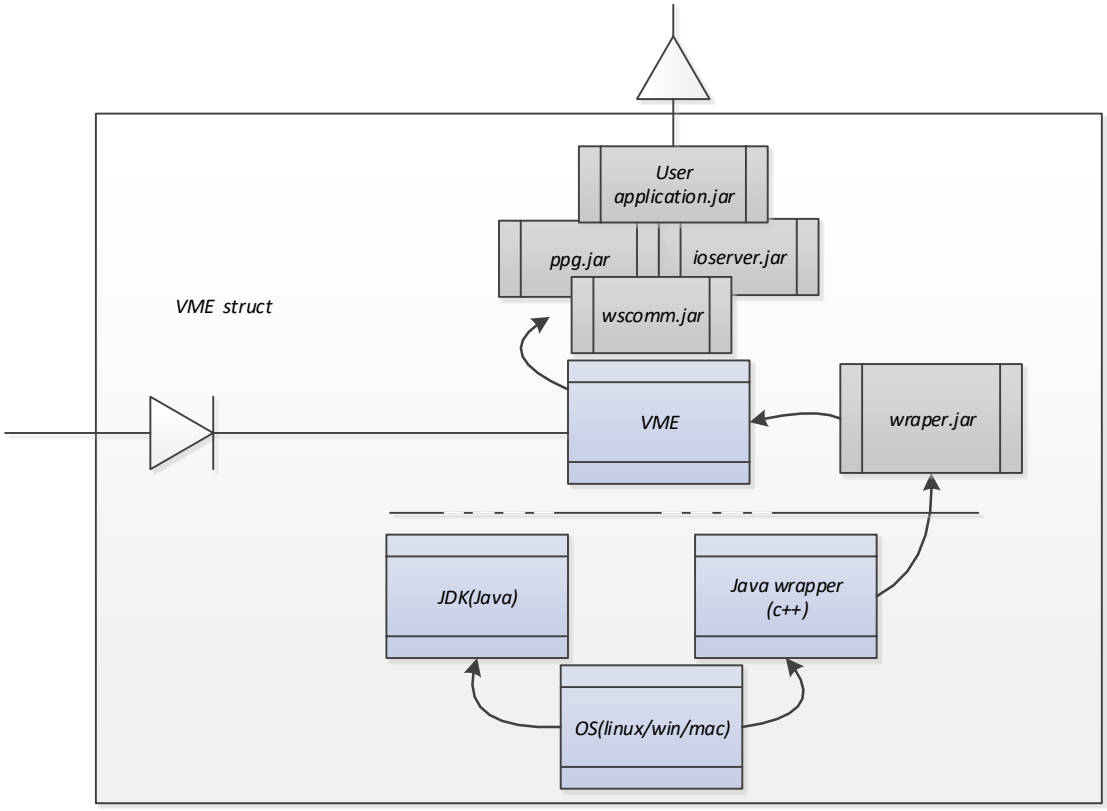
描述：

1） VMShell 开机自加载 启动 ，系统进入启动态 ，挂接服务表加载服务线程 ，进入运行态

2） 进入运行态可对其发送 重启，停止，关机指令
发送 restart/shutdown 指令 VME 进入服务停止态，VME 向所有运行的服务 发送停止指令； 根据服务挂载表依次卸载服务服务.所有服务停止，判断 shutdown ？ 如果是 exit wrapper 服务，VME 退出操作系统 ；否则进入重启服务，设定重启信号量系统进入 1 ）自加载启动态，完成服务重启。

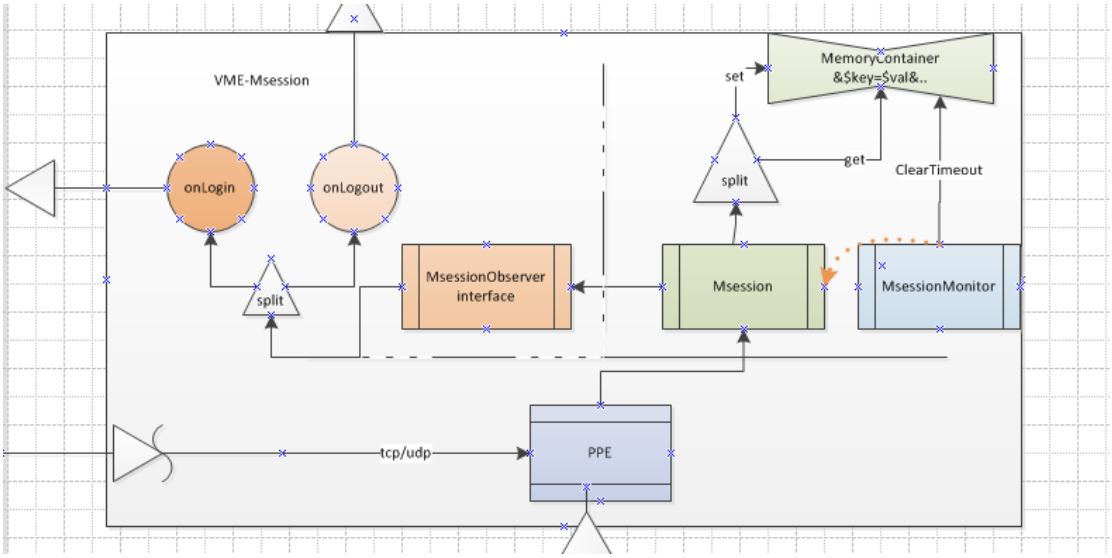
3） VME 运行于 java wrapper 服务框架下 使得开机后立即进入操作系统守候运行态 不必等用户登录桌面，而先运行。

3.3 VME 运行服务结构图



1) VME 需要 jdk ,Java wrapper 服务支撑 wrapper.dll /wrapper.so + wrapper.jar ,wrapper.jar 包含实现的 wrapper 基础接口
2) 通过 jdk 操作底层操作系统
3) 通过 VME 完成协议转换解码 业务逻辑转发存储等服务

3.4 PPE Msession 中间件

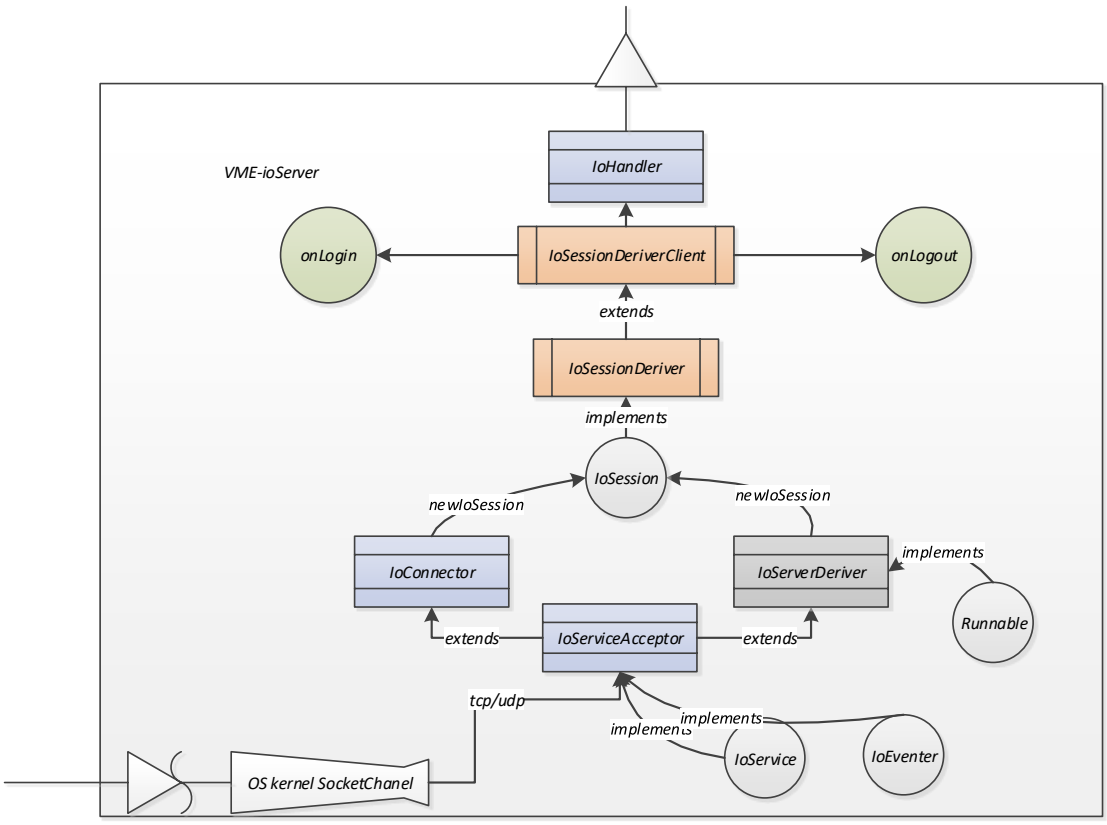


描述：

1) Msession 基于内存存储适合于 session 类会话服务 支持后台 session,前端 web session .可代替 memcache,redis.组件内置在 wscomm.jar 随项目发布自动嵌入无需单独部署.多节点可通过 ioServer 框架进行通讯
2) Msession 内含 MessionMonitor 负责对超时 session 及时清理。多个 Msession 可共享会话服务
3) MsessionObserver 为观察者模式接口 含 onLogin,onLogout 事件 可在外部服务实现该接口来实现登入、登出消息类会话服务。

Msession 支持前后端共享会话 后端可接入 tcp/ip 协议;前端可接入 jsp web

3.5 PPE IoServer 节点通讯框架架构图



描述：

1) IoServiceAcceptor 通过 NIO 模式绑定底层 SocketChanel ，自身实现了 IoService,IoEventer ;实现了 socket connector 功能。
2) IoConnector 扩展了 IoServiceAcceptor 通过建立连接返回一个 IoSession IoServerDeriver 一样扩展了 IoServiceAcceptor 可通过连接返回 IoSesssion 但它实现了 Runnable 接口 因此支持多线程。
3) IoSessionDeriver 实现了 IoSession 接口
4) IoSessionDeriverClient 扩展了 IoSessionDervier 为 IoSession 的逻辑实体。同时在连接建立过程 IoSession 实体内部用到了 Msession 缓存，通过 MsessionObserver 观察者模式执行 onLogin,onLogout 业务逻辑 。

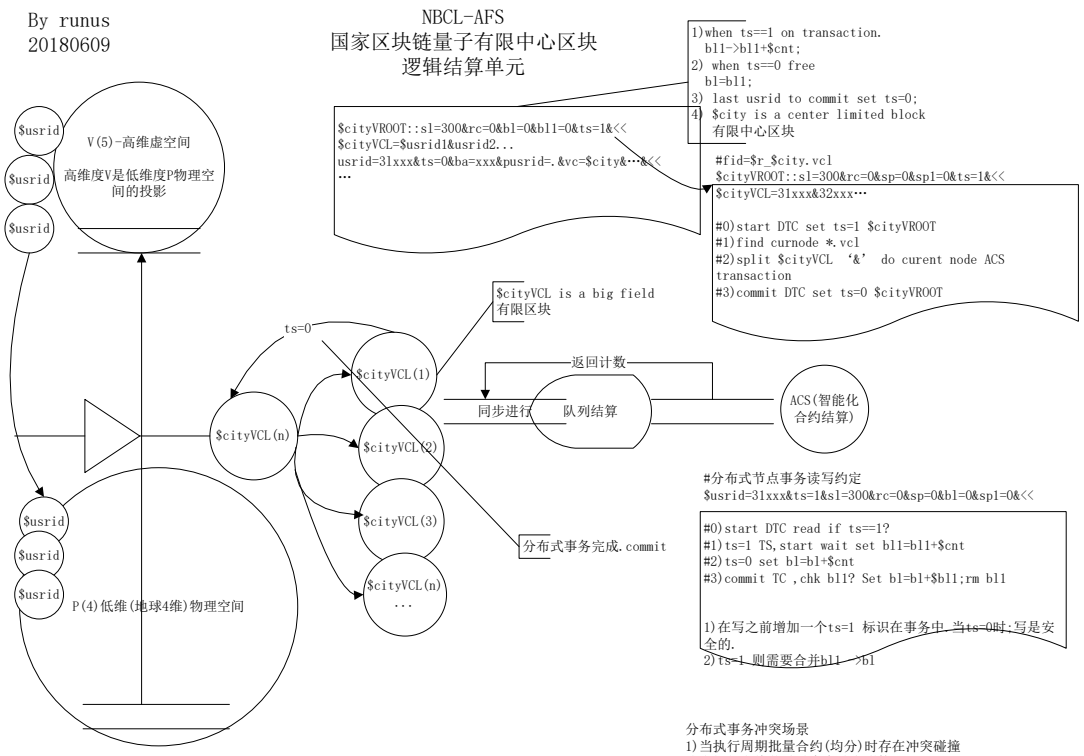
   小结：通过上面的设计实现了业务逻辑与设计模式独立 。通过实现 MsessionObserver 将业务逻辑可扩展实现。采用延后加载技术实现逻辑分离。IoServer 支持协议独立，可扩展协议解码。适合建立复杂场景模型服务

4 智能化合约 ACS(闪电合约)

智能化合约将双方、多方达成的法律协议程序化写入各自底层 AFS 区块绑定 key 值。一旦写

入不可更改，直到协议退出。因为未来人人绑定了法币的区块链数字货币，使得跨境转账极其方便与便宜。闪电合约支持秒级操作执行比如每分钟进行小额度转账，这样使得交易双方成本极低，违约带来的成本损失也更小。使得贸易更容易集中在双方资源优势有利于促成双方达成交易。我们的智能化合约支持秒分润。

4 .1NBCS-AFS 区块链秒分润设计实现手稿草图



网站需求
0)buy $vcode(数字id)
1)任何人可上传产品到主站
2)任何人可交易主站商品
3)商家获取报价$price*80%
4)$price * 10%=>pusrid (buy)
5)$price * 10%=>$city.VROOT.bl+=$price*10%
6)$city.operator.bl*5%=>$city.VROOT.bl
7)SVIP商城,HVIP商城,VIP商城
8)商城生成二维码
9)用户可扫描分享的二维码 含(pusrid)
10)$cityVROOT 为部落虚拟根节点可存储智能化合约

分布式事务冲突场景
1)当执行周期批量合约(均分)时存在冲突碰撞
2)当执行上线奖励时存在冲突碰撞

解决方案:
1)如果批量操作因为每月累积触发.引发冲突概率小.

2)单一用户冲突 每用户执行一个lock{$city.usrid}xxx.l ,如果发现存在用户id锁,说明正在执行队列锁.继续追加一个队列修改锁.去更改它的状态.则前后顺序执行队列锁操作.完成数据写

注:因为系统是队列顺序时间执行所有写操作.故不存在冲突.

改进算法.
需求:效率低,大数据尽量避免遍历存储.上面算法在数据量少的情况下可行上到几百千万秒结算实现不了.因为单用户的合约不同,执行需要加锁只能一条条计算.转存.无法有效使用块闪写技术.效率低下是必然的.
方案:
1)采用共享账号模式利用股本公积金模式.智能化合约计算读写只对每个city大区块的VROOT根节点进行读写.在单一用户提取股息时进行单一用户操作.采用分时法读写.因为所有用户不会在同一时间提取股息.在提取那一刻对该用户进行读写操作.
2)在读取用户资金账号时,账号余款动态计算方程式$bl=p.bl+(p.$xdc-p.xdc)*$sprate
注:
p.$xdc =区块派息次数 ,
p.xdc = 用户提取次数 (<=p.$xdc)
$sprate=1 每股派息面值 恒定1RMB 当累积到 1 时系统自动派息.
p.$xdbl=区块已派息账号总额
VROOT 区块虚根节点.总账本账号.记录着区块总股本,元信息.共享账号收入情况.不可提现.

以上设计可实现不限用户量的区块总账本秒级结算.采用的是共享公积金账本模式.每次操作只对总账本进行管理一次.完成利润分配.单一用户分时提现.完成单一用户账本记录分配以及总账本进行修改2次key hash操作.秒级可以实现.
每用户必须持有相应的股份stka=1 or stkb=1 才可享有利益分配.

对经常查询操作,可将区块节点账本缓存.任何节点对账本更新.需要实时通知其它节点更新缓存.

$20180727 by ws

4.2 NBCS 区块链智能化合约代码实例

ACS 智能化合约 用例 以下配置实例代码都会在我们的引擎下完好的工作

以下代码 置入商城注册 配置文件{$port}fos.properties 下. 用户注册时自动无缝绑定注入 AFS 分布式 NOSQL 存储引擎节点数据按区块存储。

OP:operator 运营商,holder 终端 user (持币者) 这里的币同时具有股权分红除息价值

4.2.1 OP 定义 (Operator)

智能化合约定义了原始区块的总币数 a 类币 100 万,b 类币 400 万。一个 op 部落相当于一个大部落区块，一个部落相当于一个行业。
以下 op 代码约定了 a 类币：享有该部落 op 利润的 20%分红派息率。B 类币法币价格 9900RMB.
如果 op 注册用户序数前 10 万 a 类币法币价格=3300RMB
如果 op 注册用户序数>10 万 a 类币法币价格=6600RMB

动态求的$eps =p.bl / p.rc 即 op 的总余额 除 部落注册成员数，当$eps > p.sprate 即收益率大于运营商约定的分红比 这里是 20% 即开始分红派息。运营商的余额发生变化。派息资金转移到公积金账号。p.w.xdbl = p.xdbl + $axd 计算运营商公积金余款并写回 op. 同时更新写 计算器+1，标识派息次数。 否则条件不满足 不派息。

实例：

```
#when ebs>=1 trigger=onStart commitACS
afs.nbcs.max.eps=1.00
afs.nbcs.profit.rate=0.05
#acs automatic contract service
afs.nbcs.acs.operator={$rate = p.rate;$sprate = p.sprate; p.w.rgstka
= 1000000; p.w.stkasp = 0.20; p.w.rgstkb = 4000000; p.w.stkbv = 9900;
$axd = $sprate * p.rc ; if (p.rc <= 100000){p.w.stkav = 3300;} else
{p.w.stkav = 6600;} $eps = p.bl / p.rc ; if( $eps >= $sprate ) {p.w.bl = p.bl -
$axd ; p.w.xdbl = p.xdbl + $axd; p.w.xdc = p.xdc + 1;}else{ $axd = 0; }}
```

注：
p.sprate 派息阀门 当 $eps 每股收益率 大于 p.sprate 时即开始派息 通常为 1
p.rate 税率 0.05 （按高科技享受低税率政策调整）
p.bl 账号余额
p.xdbl 除息余额（公积金累积余额）

4.2.2 用户定义 User(holder)

如果无 a 币，也无 b 币 则退出
p.$rate 读取 op 的 派息率
p.$sprate 读取 op 的派息阀
$axdc = p.$xdc – p.xdc ; 未派息计数 = op 派息计数 – 当前用户派息计数
$axd = $axdc * $sprate * (1 - $rate); 当前用户累积 派息额 = 未派息计数 * 派息阀 * (1 – 税率) ； 这里系统自动代扣税。
如果累积派息额大于 0 则写 派息计数 + 未派息计数 并写回 当前用户 xdc 计数；同时当前用户余额 = 余额 + 派息额 ；(这里相当于公积金提现，本次操作同时会修改 OP 计数) 同时写当前 账号余额。

实例：

```
#stock holder
afs.nbcs.acs.holder={if(p.stka == 0 && p.stkb == 0) { return; } $rate =
p.$rate;$sprate = p.$sprate; $axdc = p.$xdc - p.xdc; $axd = $axdc * $sprate
* ( 1 - $rate ); if($axdc > 0){ p.w.xdc = p.xdc + $axdc ;p.w.bl = p.bl +
$axd ; }else{ $axd = 0; }}
```

4.2.3 bl 动态计算账号余额

用户调用账号余款 ：动态计算 类函数功能
如果 op 的派息数>大于当前用户的已派息数 则返回当前资金+当前用户持币（股）数* (op 派息总数-当前用户派息数) * op 的派息阀 * （1- 税率）
否则直接返回当前用户的 余额.

实例：

```
afs.nbcs.acs.holder.getvbl={$rate = p.$rate;$sprate = p.$sprate; if( p.$xdc >
p.xdc ) { p.w.return = p.bl + p.stka * ( p.$xdc - p.xdc ) * $sprate * ( 1 - $rate );}
else { p.w.return = p.bl;}}
```

4.2.4 特殊注解

p 是万能微容器 Putter 实例

```
p=putter p.$var: get var=>p.get("$var") ;p.w.$var => p.set("w.$var",$val); will
  write to AFS
$var startWith $ self var
p.*  AFS var
p.w.* AFS set VAR
```

p.w 为写变量 结果会被立即写入 AFS
p.w.return 即完成写并返回结果 写并返回给调用者
$ 用户自定义变量
p.$ 为 OP 变量
p.xx 为 当前用户 Putter 实例变量

小结：

holder 用户持股权益者关心的是资产 bl(blance)净值的变化

上面代码定义了 operator 部落 原始发行多少币（股）比如北京总量限额 2000 万.
holder 定义了每人账户持有的币（股）即账户中股票、币的余额 （这里的币具有交易，与股东分行权益，以及购买时的价格。分 A 类股，B 类股，享有的权益不同。
op:定义了当注册数动态变化购买股的法币（人民币）资金成本会按倍数递增 体现了区块链的激励政策 越早进来成本越低。
p.bl 为用户资金余款（跟法币即人民币按 1：1 挂钩）

区块链的意义

区块链带来技术革命
智能化合约，分布式存储电子钱包。

区块链交易是建立在不可信交易风险之上采用密码学分布式记账交易模式。通过合法的签名技术认证交易，延后交易，智能交易手段，进行交易。

1 房屋租赁与过户

比如业主 A 出租房子给用户 B,约定每月一日交付房租 10000。租期一年。传统时期，签约没约房东来收费或定时打款。如果交不起房租合约解除 B 违约，房子收回。

在区块链智能化合约是这样的。把合约关键信息条例化数字量化。
通过抽象的数学公式经过双方秘钥加密写成智能化合约写入分布式账本。系统会定期扫描。触发执行这些智能化合约。区块链时代所有人都链接了数字钱包。如上例子每月一日智能化合约会被系统自动触发。自动划拨数字货币从 B 转到 A。B 想赖账都没用，数字币即法币。提高了办事效率也避免了坏账。

各行业都接入区块链，交易。批量执行智能化合约，分块存储执行。提高社会经济效益。

2 有价数字资产转让

股票，债券的交易。
区块链是基于 token 认证，未来会接入交易所，工商股权注册通过双方认证授权直接完成资产的过户变更登记。

3 绑定银行法币

区块链货币绑定商业银行法币，人人都可自由兑换。人人在一个大而全的分布式系统登记注册，公开透明。提高社会效率。降低资金转账成本。

4 通证授权

比如自媒体发布原创视频。可以通过区块链存储获得 token 授权认证。区块链有时间记录。不可修改。经过授权的视频链接可转让，获取二次授权认证。区块链支持的数字转移。依次类推包含版权授权，专利授权等数字认证。

5 股权分红，债权还息，公积金发放，微支付

区块链技术结合智能化合约技术可实现微支付秒结算，智能分成。提高交易效率节省交易成本。打破传统比特币交易时间慢(约 15 分钟每笔)时限。

7 区块链可绑定稀缺物品进行拍卖交易，进行资产转移过户。

如名画，玉器，文物。每个商品一个唯一编码一旦生成不会改变。

区块链传递的有价数字资产，这些资产一旦生成不可改变。但数字资产可以完成转移登记，可溯源。

小结

本项目方案中所用到的中间件系统 90%是自主知识产权.有强大的技术壁垒.不会受制于人.被卡脖子。当下正值中美贸易战,美国在芯片领域掐断中兴通讯的事实再一次证明了;自主核心技术的重要性.自主创新核心技术为国之重器.本系统下组件为轻量级架构模式.设计具有优雅先进性.融合了宇宙迭代学进行演变过程.

本项目可以设想,每个人一生下来即存在一个身份 ID,对应在高纬度虚拟的 V 空间,V 空间对应着现实 P 物理空间背后的商家.通过绑定区块链技术实现智能化合约分享利益.厂家,商家,也需要用户的购买力来支撑才能继续投入生产.最终到达人人平等,人人即我,我即人人的未来世界大同;最终实现共产主义.