BCS
Technical Yellow Paper

BCS FOUNDATION

目录

1 背景

区块链技术从比特币时代，少数极客们的玩具，到如今的公链的百花齐放，经历了10 年的快速发展。虽然数字货币陷入了熊市，但区块链技术和社群的发展却不曾停滞，依然欣欣向荣。但是，我们也看到了，因为利益的冲突和技术的限制，公链的落地场景迟迟无法实施。尤其是作为区块链核心的共识算法上，不管是 POW，POS，还是 DBFT，PBFT，都没有创新性的发展。

比特币和以太坊采用的 POW 算法，可以保证区块链网络的安全。但因为 TPS 的限制，无法满足实际应用的需求，同时 POW 算法也使人们担忧数字货币对于环境资源的浪费。

而 EOS 等采用的 POS，则陷入了中心化 VS 去中心化的争议中。同时，POS 天然会产生富人更富的经济悖论，不利于区块链经济的发展。

因为有准入的门栏，DBFT/PBFT 等主要的应用场景是联盟链或者私有链。虽然有项目方把 DBFT/PBFT 应用到公链中，但同样也遇到了激励和准入等等的问题。

2 匿名性

2.1 地址和私钥

在所有的区块链特性中，匿名性是最富有特色的。所有的非区块链的金融中，身份认证是第三方托管所必需的。但在区块链中，由于没有第三方托管的存在，个人身份是非常难以认定的。所有的数字货币，都被区块链以共识的方式，记录在每个区块链节点中。同

时，也只有自己所保管的私钥被区块链认同，花费这些数字货币。所有的这一切，都不需要身份。

或者我们可以说，私钥就是身份。

2.2 记录公开

区块链是匿名的，但所有的转账记录却是公开的。通过公开的记录，可以关联出某些地址的相关性，或者某笔数字资产的流通情况。这个特性产生了某些有趣的结果。

有些公链通过特殊的算法隐藏了记录，使得交易双方之外的人无法了解交易的详情。

有些项目期望通过记录公开来提供溯源应用，来解决安全或者不信任问题。

2.3 匿名

有趣的是，并不是人人都喜欢匿名，NAMECOIN 和 ENS 的出现，就是一个很好的例子。某些实体或者个人希望把自己的地址和某些有意义的代号链接起来，这个代号或者是项目的名字，或者是公司的名字。

同时，KYC 和 AML 的出现，也使得区块链的匿名性成为了不可能。或者说，比起区块链的便利性和应用前景，人们并不在意他的匿名性。

3 商业应用的需求

3.1 信用体系

比起区块链和数字货币，在实体世界中已经有一套成熟的信用体系来支撑金融体系的运行。POBC 共识希望引入现实世界的信用体系，来为匿名的区块链网络提供更好的运营和支撑。

3.2TPS

TPS 指的是系统吞度量，也是每秒系统处理的数量。假如 TPS 每秒并发太低，很容易造成网络拥堵严重，从而使得区块链在高价值的高并发业务领域无法落地。比如，由于 TPS 每秒并发太低，比特币和以太坊都存在交易费用高、确认时间长、扩展性差的问题。当前的公链虽然可以存储价值，但过低的 TPS 无法支撑真实落地应用的需求。除非区块链达到百万级用户的支持，否则无法出现有价值的依附应用。

3.3 迁移成本

因为区块链的数据存储方式是链式块结构的，单个的应用难以迁移以及成本过高也成为限制。有研究表明，一个以太坊智能合约的迁移成本大约是每个地址 0.025USD。以 30 万用户 BNB token 为例，单次的迁移成本大约为 7500USD。而且，这只是账户金额信息的迁移，如果想迁移其他信息，成本可能更高。这对于 DAPP 的开发者来说，是一笔巨大的开销。

3.4 免费使用

用户不应该因为使用平台的功能而支付费用，免费/收费的策略应该是由应用开发者制定。同时，区块链平台的应该激励应用开发者免费自己的应用。比特币和以太坊未使用免费交易的主要原因是为了防止打包进无意义的或者没有真实价值的交易。EOS 虽然交易免费，但设计了 RAM，NET，CPU 来阻止无意义的交易。

对于交易费的问题，有以下两个安全方面的问题：

- 节点激励来保证网络安全。对于节点奖励，BCS 采用永久奖励的方式为记账节点提供激励。

- 防止 DDOS 攻击是主流数字货币未提供免费交易的主要原因。大量的交易发起一方面需要提供大量的基础手续费，在造成系统拥堵的情况下，还会大幅度推高基础手续费，这就形成一种负反馈，一定程度上保障网络的安全运行。BCS 希望引入一种后结算的方式来阻止无意义交易的发生。具体策略是用户在交易的时候，需要按 BC 评分支付一定数量的保证金来确保交易被正常处理。在固定数量区块被打包之后，这部分保证金会被释放出来。

3.5 延时（确认）和未打包

比特币和以太坊的 POW 共识有极大的延时和未打包的风险，这给用户和应用开发造成了极大的风险。

3.6 智能合约

智能合约是区块链 2.0 得以快速发展的主要原因。通过智能合约，区块链应用开发者不需要发行公链平台就可以使用区块链来存储数据，执行合同逻辑。但是，也需要认识到，智能合约不是一种语言，而是一个体系，重新开发一个新的智能合约运行环境是没有必要的。会产生一系列的问题，比如难以搭建生态，资源浪费。EVM 是当前最有完备生态和社区支持的智能合约体系。

4 商业信誉

POBC 的核心共识基础就是商业信誉，这包括三个方面，身份，声明和身誉 [1]。

身份是系统内最基础的角色。身份可以用来证明自己和他人曾发生过一些事，我们把这些事称作声明。随着时间推演，声誉会随着身份体系建立起来。

身份、声明，和声誉的协议，应该通过适当的接口相互交互。这个系统必须是模块化且可扩展的，同时具备以下特性：

- 去中心化（Decentralization）：协议规则应该由网络参与者制定和遵守，而不是由中心化权力机构执行。
- 自治（Self-sovereignty）：用户自行掌控属于自己的身份、声明，和声誉。这与 Web 2 网络形成巨大的反差；在 Web 2 网络中，比如在亚马逊；一个商家的产品积累的声誉，可能会因为亚马逊破产或单方面决定，而被移除。
- 可移植性 & 互操作性（Portability & interoperability）：系统不该扣留用户，而应该允许用户往其他系统上迁移属于自己的数据。
- 抗女巫攻击（Sybil resistance）：设计协议时，必须考虑参与者不能通过发布多个身份获得优势；除此之外，协议中旧身份更换成新身份没有好处。

- 隐私（Privacy）：参与者应该能选择性地与他人共享数据。此外，默认情况下参与者的身份能通过不公开的标识进行验证。

接下来，让我们深入了解这个系统的三个组成：身份、声明、声誉。

4.1 身份

身份能够用于信息签名、数据加密，或是发表关于自己或他人的声明。身份是由私钥完全控制的，所以对于私钥丢失的情况，身份管理应该包含密钥恢复机制。许多机制在这里能够派上用场：社群找回、暂停证明服务，或是通过 Shamir 密钥分享和 Schnorr 签名方法。身份方法必须和其他系统有很好的互操作性，并能适用于 W3C DID（去中心化身份验证者 Decentralized Identifier) 标准。

4.2 声明

声明是指通过区块链平台发布证明用户身份的证明。一个 POBC 用户为了通过认证，可以发布许多条声明，有些声明是必须的，有些声明是可选的。其他的 POBC 用户可以在此基础上提供佐证。

4.3 声誉

声誉即 POBC 节点在做为超级节点后的服务信誉，或者 POBC 应用提供者的服务信誉。

4.4 商业信誉和去匿名化

在 BCS 中，节点应该去匿名性。这样就可以和现实世界中的商业信誉体系对接起来，最大限度的降低作恶节点的可能，以及最大限度的提高 BCS 用户和应用开发者对于平台的信任。

大量研究表明，记账节点的健康，和控制实体的现实世界财务状况有很大关系。通过去匿名性，BCS 平台和用户可以更快的发现有可能伤害平台的记账节点。为平台的稳定性（减少分叉和攻击），鲁棒性提供支持。

当然，BCS 中，只有记账节点才需要通过去匿名化认证，和商业信誉认证以达到平台要求。普通用户和平台应用开发者则不需要匿名认证，但可以加入基于隐私保护的身份认证来获得一些特权。

5POBC（商誉证明）共识算法

POBC 将采用类似 DPOS 的轮流记账权算法，但需要记账权竞争机制，期望可以达到 2 秒钟/块的出块速度，并且计划在未来的版本中，将出块速度提高到 500 毫秒。

通过 BC 评分，BCS 将选出 30 个超级节点，来分割每分钟的记账权利。

BCS 将通过一套竞争方法来允许记账权利在记账节点间的竞争，主要评价协议（包括 BC 和质押 BCS 权益）来决定竞争的结果。

这种良性的竞争将提高 BCS 记账节点的公信力和财力，也可以为 BCS 代币市场提供一个良性的流动性市场。我们设想，未来会有一个提供固定 BCS 代币权益租借利率的流动性市场，来服务于记账权利的竞争。同时，公平的记账权利，也防止了矿池走向集中化。

5.1 频繁竞争攻击

记账会产生收益，因此无可避免的会发生频繁竞争攻击。为此，POBC 重新设计了代币权益计算方法，引入时间来计算代币权益。当用户账号中的代币参与权益租借后，该时间会被清零。这样可以有效阻止频繁竞争攻击，保证平台的稳定。

智能合约

BCS 将会重用 EVM 的合约体系，来确保应用开发生态的扩展和移植。

EVM 代码由一系列字节构成，每一个字节代表一种操作。一般而言，代码执行是无限循环，程序计数器每增加一（初始值为零）就执行一次操作，直到代码执行完毕或者遇到错误，STOP 或者 RETURN 指令。操作可以访问三种存储数据的空间：

- 堆栈，一种后进先出的数据存储，32 字节的数值可以入栈，出栈。内存，可无限扩展的字节队列。
- 合约的长期存储，一个秘钥/数值的存储，其中秘钥和数值都是 32 字节大小，与计算结束即重置的堆栈和内存不同，存储内容将长期保持。
- 代码可以像访问区块头数据一样访问数值，发送者和接受到的消息中的数据，代码还可以返回数据的字节队列作为输出。

当以虚拟机运行时，它的完整的计算状态可以由元组(block_state, transaction, message, code, memory, stack, pc, gas)来定义，这里 block_state 是包含所有账户余额和存储的全局状态。每轮执行时，通过调出代码的第 pc（程序计数器）个字节，当前指令被找到，每个指令都有定义自己如何影响元组。

当然，因为 BCS 的没有交易费用，所以用户可以通过虚拟机实现非常复杂的代码逻辑。但是，BCS 也会对有攻击性的合约进行惩罚。

6 发行

BCS 将采用永久线性增长模型，来给予了用户公平的机会去获取货币，同时保持了对获取和持有 BCS 代币的激励，因为长期来看“货币供应增长率”是趋于零的。所有对于 BCS 网络有贡献的节点，将有机会获得记账权利。而记账所产生的收益，将激励节点提供更安全和更高性能的记账服务。

7 综述

BCS 期望实现一个和现实世界有所关联的区块链网络，来提高区块链生态的公信力，促进落地应用的开发，以及加速传统商业机构向区块链转型的步伐。通过引入商业信誉因素，解决了区块链匿名性网络内部的信任危机，并通过这种 POBC 共识协议，来激励商业机构对于区块链生态的投入。

8BCS 线路图

Phobos 2019.7	BCS Beta 主网上线
Deimos 2019.8	智能合约平台发布、POBC 共识协议发布
Mars 2019.9	BCS 主网上线
Jupiter 2019.12	认证机制模块开发完成、POBC 共识协议模块开发完成、BCS Solar TestNet 上线
Saturn 2020.6	BCS Solar 主网上线、BCS 区块链浏览器发布、基于 Solar 主链的钱包发布、智能合约 2.0 平台发布
Uranus 2020.12	BCS2.0 主网上线、BCS 开发者生态圈建设

BCS 技术团队

附 1:

以太坊的身份证明

ERC 725/735

ERC 725 是个关于智能合约身份的提案，实现了一个管理身份声明的标准化接口，部署编号为 ERC 735。用户需要批准所有与他们相关的声明，而且能随时删除。因为这个系统不需要多方协同，所以是可以升级的。

这个提案也有一些问题。因为每个身份都要自己部署声明合约，因此无法保证都遵守 ERC 735 中的规范。因此当验证者与这些身份打交道时，首先得检查他们的源代码；这会带来很大不便。更糟的是，允许用户直接删除关于他们的声明，阻碍整个系统发布负面声明。

最后，涉及隐私保护，ERC 725 需要搭配一个链下系统，因为它将所有声明都存储在链上。

ERC 780

ERC 780 提出在以太坊上建立一个全局的注册表，来存放以太坊上的所有声明。uPort 便是将注册表当作构建一个去中心化 PKI 系统的基础，目标是将大多数声明转移至链下。注册表不会区别声明者是账户或是合约；又因为只存在一份合约，所有验证者可以相信它的逻辑。

这份提案的问题在于声明的表达性有限。因为要求所有声明遵守同样的数据结构，这就直接带来使用上的局限。进行升级时也会遇到麻烦，因为它需要广泛的利益相关者的支持。

Zeppelin TPL

Zeppelin TPL（ Transaction Processing Layer ，交易处理层）被设计用于 ERC20 代币的许可交易。在这个方案给每个“司法管辖区”部署了不同的合约。“司法管辖区”的管理集群们选出证书颁发者，这些证书颁发者有权将声明写进该管辖区的声明注册表。

这是个比较实用的设计。验证者更加信任司法管辖区的声明，因为他们知道这些声明者是经过认证的。但另一方面，只允许部分用户发表声明，必然导致系统灵活性降低。

这样的系统也可能遇到难以扩展的问题。没有一个管辖区会提供完整的相关声明列表（因为管理、地理位置，或用例的不同），因此验证者必须检查多个注册表，或是声明对象必须在不同管辖区反复进行声明。

基于 NFT 的身份

我们能以 NFT（Non-Fungible Token，非同质代币）的形式，将许可进行编码，一组权威节点可以为用户生产 NFT，验证后供用户使用。这里的问题是用户能够交易他们的 NFT，而设计里并没有提到使用 NFT 比使用声明的优势在哪。

附 2:

女巫攻击

女巫攻击是在 P2P 网络中，因为节点随时加入退出等原因，为了维持网络稳定，同一份数据通常需要备份到多个分布式节点上，这就是数据冗余机制。女巫攻击是攻击数据冗余机制的一种有效手段。

引用：

1. 身份，声明，声誉：https://sinahab.com/2018/09/identity-and-reputation-in-web-3/
2. 智能合约：https://en.bitcoin.it/wiki/Contracts
3. 比特币白皮书：http://bitcoin.org/bitcoin.pdf
4. 以太坊白皮书：https://github.com/ethereum/wiki/wiki/White-Paper
5. 以太坊 EVM：https://ethereum.stackexchange.com/questions/268/ethereum-block-architecture/6413#6413
6. How contract migration works：https://blog.trailofbits.com/2018/10/29/how-contract-migration-work