新生比特币

Newborn Bitcoin

系统白皮书

版本号：1.1

二〇一八年九月七日

目录

1. 概述 3

1.1 问题的提出 3

1.1.1 无节制算力竞争带来高成本 3
1.1.2 每秒交易数过低 4
1.1.3 一次交易等待确认时间太长 4

1.2 技术要点 4

1.2.1 设计理念 4
1.2.2 关键措施 5

2. 技术方案 6

2.1 分布式时钟 6

2.1.1 PoET 答题过程 7
2.1.2 答题证明 9
2.1.3 可信矿工身份 9
2.1.4 连续记帐间隔 10
2.1.5 PoET 共识的安全强度 11

2.2 用并行链提高 TPS 12

2.2.1 单链如何提高 TPS 12
2.2.2 分配矿工到指定的链上工作 13
2.2.3 账号归属 14
2.2.4 安全漂流瓶 15
2.2.5 并行链扩容 15

2.3 秒级确认与可信转账 16

2.3.1 秒级确认 16
2.3.2 可信转账 17
2.3.3 链上治理 18
2.3.4 系统安全性 19

3. 价值体系 19

1. 概述

自 2008 年中本聪提出比特币电子现金的概念以来，比特币（BTC）已展现了巨大的生命力和稳健性， 但是随着比特币网络规模扩大和技术的发展，现在的比特币系统已经偏离中本聪最初的设计理念。

为了进一步推动发端于比特币的区块链系统向前发展，我们团队针对比特币现有问题，提出了一整套改进方案，既继承了原比特币系统的优点，又针对性解决了若干严重缺陷，还拓展了一些新的技术应用，我们把这套系统叫做 Newborn Bitcoin，简称 NBC，中文名为新生比特币，简称新生币或新比特币。

1.1 问题的提出

比特币系统作为一个去中心化的点对点电子现金系统，核心设计是完美的。但是同中心化的金融系统相比，在实际应用上还存在很大的差距。

这些差距集中表现为三个问题：无节制算力竞争带来高成本、算力集中的问题；每秒交易数 TPS 过低、网络经常阻塞的问题；一次交易等待时间过长、无法真正商用的问题。

1.1.1 无节制算力竞争带来高成本

我们评估当前比特币系统尚未广泛应用，首先遇到的障碍是使用中的高成本，当购买一杯 5 美金的咖啡要支持 20 美金转账费时，BTC 是很难走向现实应用的。而高昂转账费背后的逻辑是高币价，高币价由无节制算力竞争推动起来的，当比特币全网算力达到一定级别时，降低算力意味着降低系统安全性，而安全性对于比特币至关重要。所以，现实中 BTC 在一定程度上表现出算力锚定的效果，币价涨涨跌跌，基础算力相对稳定，常有波动但不会出现数倍乃至十倍的短期震荡。

比特币采用 PoW 共识算法，虽然提供了一个非常可靠且经得起时间考验的去中心化共识方案，但是也把比特币挖矿引向了算力竞争。经过将近 10 余年的发展，比特币已经从 普通电脑

CPU 挖矿、GPU 挖矿、FPGA 挖矿，最终发展到现在专用 ASIC 挖矿。在 PoW 算法牵引下，比特币网络的挖矿门槛已经很高，普通电脑已经无法参与到挖矿活动中来，大型矿池的出现更是让挖矿开始呈现中心化态势，有违去中心化理念，也在事实上，与中本聪倡导的 “人人可挖矿” 理念已背道而驰。

同时，PoW 共识算法采用毫无意义的哈希碰撞，也导致电力过度消耗，带来了一些环境问题。

1.1.2 每秒交易数过低

比特币对区块的大小限制是 1M ，在区块中平均记录每笔交易要占用 0.25K 字节，按 10 分钟出一块计算，10 分钟约容纳交易数为 4096 ，可计算出每秒交易数（Transaction Per Second，TPS）为 6.8 ，即，每秒约处理 7 笔交易。这种处理能力与信用卡每秒数万笔，以及支付宝峰值每秒 10 万笔以上相比，差距很远。

不只比特币存在 TPS 太低的问题，目前市面上主流加密数字货币普遍存在相同问题，某些币种的 TPS 或许能提高一些，但并未达到数个量级的提升。按一般经验，TPS 值要达到 1000 以上才可能让区块链系统支撑常规商业应用。

1.1.3 一次交易等待确认时间太长

比特币的区块链系统，平均每隔 10 分钟产生一个新区块，出于安全需要，一项交易要经过 6 次确认才算最终交易成功。 所以，一次比特币交易，在网络不拥堵情况下，要等上 60 分钟（即 6 个平均耗用 10 分钟的出块时间）才能得到转账是否成功的确认。这样的交易确认时间太长，带来直接后果是：它将无法用作日常支付手段。如果希望区块链真正进入到实际的商用场景，交易确认需要缩短到 10 秒以内才行。

1.2 技术要点

1.2.1 设计理念

从本质上讲，比特币系统是通过技术手段解决了信任的问题，让每个节点相信在没有中心化机构存在的情况下，点对点的现金转账也是安全的。但是事实上，安全也是相对的，比特币系统

只是实现了在 2008 年计算机技术水平基础上的安全。随着比特币系统将近十年的发展， 相关技术更新换代，尤其是专用 ASIC 矿机的出现，比特币系统开始出现中心化趋势，原有安全壁垒已开始降低。

让比特币重新变安全、可信，已成必然趋势。

技术是不断向前发展的，任何技术都不是一成不变的，如果不与时俱进，任何技术都会面临被淘汰的风险。NBC 团队认为技术才是比特币系统生存的基石，只有技术才能再次筑高比特币的安全壁垒， 让比特币能够真正的走入到每个人的生活中来。

1.2.2 关键措施

针对上述 BTC 三大问题，NBC 团队针对性的提出了三项解决措施：

更换共识算法：改用 PoET （Proof of Elapsed Time）从根本上克服无节制算力竞争；

提升每秒交易数：将单链串行交易方式更改为多链并行，使系统的每秒交易数能按链数实现线性增长；

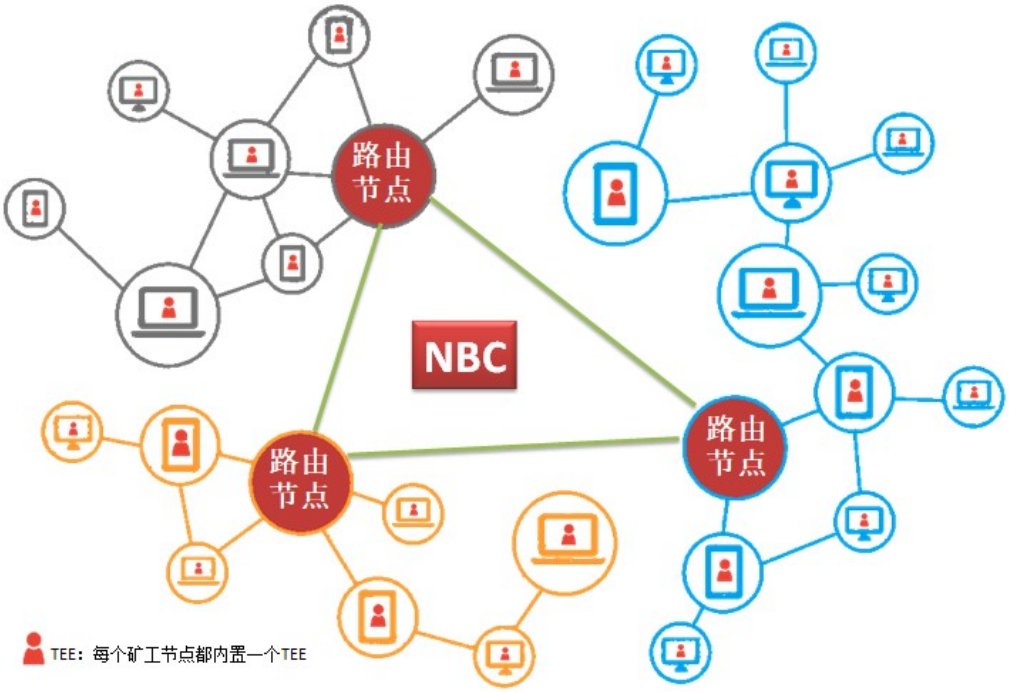
缩短交易确认时间：拆分单次交易，提出一种 “出账即交易” 的解决方案，实现秒级确认。

基于这三项关键措施，NBC 将实现一个具有低耗能、高吞吐率，且支持秒确认的点对点电子现金系统。



2. 技术方案

NBC 系统在 BTC 系统的基础上，从底层架构对比特币进行重新设计。主要做了三方面优化：改换共识算法、支持并行多链、实现秒级确认。其中，共识算法与并行多链的改进依赖于引入一种可信执行环境（Trusted Execution Environment，TEE），并行多链与秒确认的改进依赖于引入一种路由节点（Router Node）。



2.1 分布式时钟

在分布式系统实现多方记帐，首先要克服一个难题，引入一套可信赖的时钟系统。只有时钟可信，记账的先后顺序才能保障，比如某账号要先收款，才有余额对另一项交易付款；也只有时钟可信后，同一笔账款才能保证不会重复花费。比特币系统是去中心化的，所以不能用一个中心节点提供统一的时钟，现有 BTC 记账的时钟以 PoW 算法为基础构建起来，其思路是：系统区分难度来出题，当前抢答的人多出题就难些，否则容易些；各矿工节点独立答题，答题要消耗算力，必然占用一段时间，BTC 系统尝试用难度目标值（即源代码区块头的 bits 字段），来控制每次从出题到答题成功的平均时长接近 10 分钟。

NBC 采用与之对等的机制，也用 bits 字段指示难度目标值，出题则更直接：是否允许本设备以累计的时间资源换取记账权？答题由可信执行环境 TEE 执行，每个参与挖矿的矿工节点都配置一个同款或功能兼容的 TEE 设备。TEE 提供一种高度安全的程序执行环境，TEE 中的程序只在授权后才可运行，其数据也只在授权后才可读取或修改，TEE 还内建一套无法伪造的时钟系统。

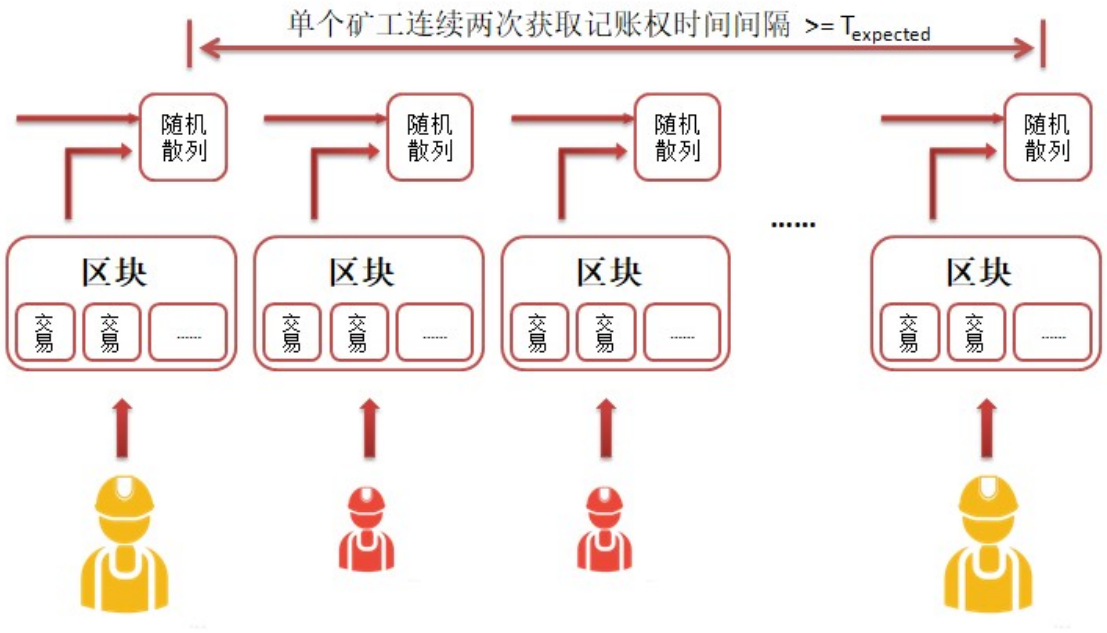
2.1.1 PoET 答题过程

PoET（Proof of Elapsed Time）是一种直接以流逝时间为证明的共识算法，系统按难度目标值 bits 出题，答题的第 1 步，TEE 中的程序先按如下公式计算预期等待时长 $T_{expected}$。

$$T_{expected} = K / bits$$

其中， K 是常量，取值为 $30,000,000$ ，当前难度目标 bits 取值范围是 $20 \sim 10,000$ ，取值越小表示挖矿难度越大。计算所得 $T_{expected}$ 是以秒为单位的预期等待时长。

答题第 2 步，TEE 判断当前设备的累计时间资源是否超过 $T_{expected}$，如果超过，答题将成功，TEE 将扣除刚耗用 $T_{expected}$ 值，这个值保存在 TEE 环境中，在设备启动工作后即自动累加当前流逝时间。如果答题成功，将进入第 3 步，TEE 为答题结果给出一份加盖签名的证明字串。



与 PoW 答题类似，某矿工如果答题成功，意味着他获得一次记账权，然后他可以创建并发布一个新区块，含签名的证明字串也随同新区块的内容一起广播到其它矿工节点。其它矿工可用这份证明验证该区块的创建者答题结果是否属实。

由于分布式系统在各节点间传播消息存在时延，上述基于 PoET 共识的答题过程并不保证同一时间只有一个矿工成功答题。这与采用 PoW 答题的 BTC 类似，同一时刻如果有多人同时获得记账权，系统将临时产生软分叉，软分叉将由后续新挖出区块时始终取最长链进行消除。NBC 消除软分叉的过程与 BTC 相同，但 NBC 更严格，采用 8 次出块作为最终确认，而 BTC 以 6 次确认为准。

NBC 的难度目标值在每出 504 个区块时作调整，按 5 分钟出块间隔计算，大约每 1.75 天调整一次，调整时按下面公式重新计算新的难度目标值。

```
new_bits = bits * (actual_period_time / standard_period_time)
```

这里，actual_period_time 是刚过去一个周期实际经历了多少秒时间，standard_period_time 是一个周期的标准时长，在 5 分钟上下，具体取值与当前挖矿难度相关。如果实际经历时长小

于标准时长，新的难度目标值将变小，由“K / bits”计算的预期等待时长 $T_{expected}$ 将变大，反之，实际经历时长如果大于标准时长，新的 bits 变大，$T_{expected}$ 则变小。

BTC 固定指定难度目标调整周期的值，即 2016 次出块乘以每块间隔 600 秒，NBC 则让这个周期与挖矿难度关联，挖矿越难出块就越快，当前的难度调整周期就越短，这意味着攻击者永远无法在低算力情况下，通过人为制造分支来培养最长链。standard_period_time 的计算公式如下：

```
Standard_period_time = 504 * (240 + (bits / 42))
```

其中，bits 表达当前挖矿难度，其值从最近两个周期的难度目标值推导而来，因 bits 在 20 ~ 10,000 之间取值，上述 standard_period_time 将在 504*240 与 504*478 之间取值。换一句话说，标准出块间隔会在 4 至 8 分钟之间，就挖矿人数较多的典型情况而言，NBC 各链平均每隔 5 分钟挖出一个新区块。

2.1.2 答题证明

TEE 已预驻留一对用来代表答题公证人的公私钥，可信设备有机制保证其私钥永远不会在 TEE 之外出现，而公钥则全网公开。上面步骤中给出的答题证明，将包含如下内容：

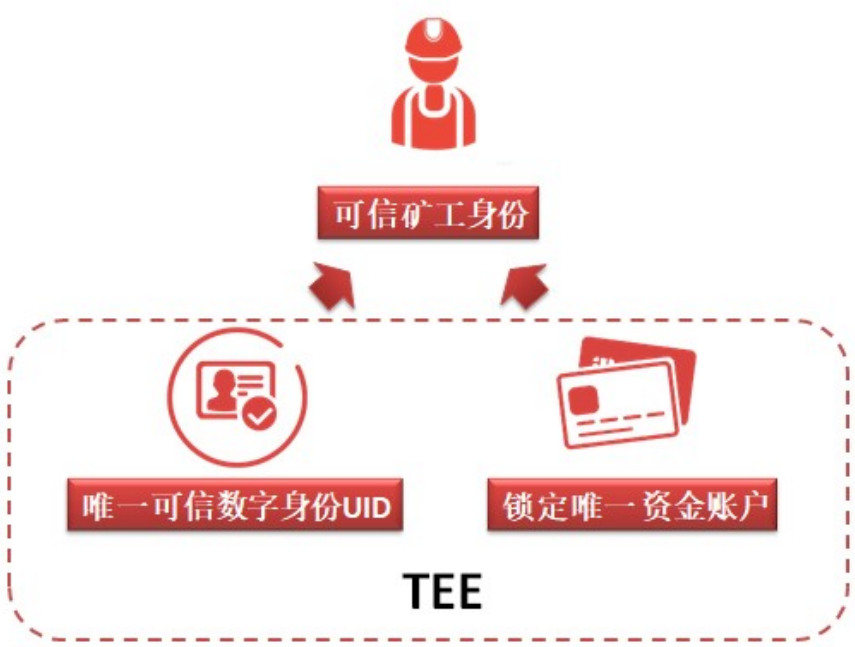
1. 上一区块的 hash 值
2. 当前难度目标值 bits
3. 当前矿工在 TEE 中绑定钱包账号

TEE 中的程序将包含上述内容的字串用答题公证人的私钥做签名。其它矿工则取对应新区块的上述 3 项内容，按相同格式组装字串，再用答题公证人的公钥，验证相应的答题结果证明的签名是否属实。

2.1.3 可信矿工身份

答题证明中包含了当前答题矿工所用 TEE 绑定的账号，这意味着在 PoET 共识算法中，挖矿

者身份是准确不可伪造的。因为，答题证明在 TEE 中生成，外界无从干预，而且，各矿工 TEE 中的钱包账号只允许绑定一次。捆绑账号的操作由 TEE 中的程序负责，该程序会先判断当前 TEE 中是否已保存过一个账号，如果没有，才响应绑定账号的操作请求，将指定账号保存到 TEE 设备中。



在 NBC 系统中，矿工身份是可信的，新挖出区块的矿工可获两个奖励：一是挖矿奖励，二是在该区块打包的所有交易的抽成。两项奖励均记入对应 TEE 设备所绑定的矿工账号，且作为一项特殊交易，永久写入区块链。因为矿工身份可信，他挖矿的频次随时可查验，如果某位矿工有作弊行为，很容易被系统识别出来，并借助可信转账机制被惩罚，有关可信转账的内容将在后文介绍。

2.1.4 连续记帐间隔

为了监督矿工诚实记帐，我们要改造区块头定义，增加两个字段，一个字段记录当前记账矿工的账号，另一个字段保存答题公证人的签名。任何挖矿节点都可以核对签名的真伪，它还可检索全部区块头，把每个区块都由谁开采的信息提取出来导入到数据库，并随时检测一个矿工连续记账的间隔是否正常。比方说，如果某个矿工最近连续 3 次记帐的平均间隔小于某一限度，即判为异常记账，他最后一次记账将不被认可。

这里的最低限度可根据最近 3 次记账所用难度目标值推算出来，只要推算规则是明确的，成为全网共识，所有参与记账的节点都能监督别人是否规范记账，他自己也依据此规则去避嫌，不该自己去记账的时候没必要去竞争记账权。

2.1.5 PoET 共识的安全强度

实践中，NBC 将采用与银行 U 盾同等安全强度的 TEE 硬件，在机制上几乎可杜绝安全措施被破解。基于 PoET 构筑安全性，主要威胁来自 TEE 设备发放后如何被使用，如果攻击者聚集算力，拥有市面上流通的过半 TEE 设备，仍有能力发起 51% 算力攻击。这一点与 PoW 共识相同，只是黑客实施攻击时，每个 TEE 折合算力是对等的，没有强弱之分。所以，我们想保障基于 PoET 共识的区块链的安全性，重点是避免 TEE 设备被恶意聚集。

对于单链区块链系统，我们假定某黑客组织已聚集占总量 1/n 的 TEE 设备，连续 8 次出块黑客均获记账权的几率为 $(1/n)^8$，如果 n 取值为 3，黑客攻击成功的几率为 0.015%，这个几率很低。而同等情况下，比特币在 1/3 算力攻击时，成功率为 $(1/3)^6$，即 0.14%。所以，运营 NBC 系统官方设立的一个安全标准是：避免任何个人或组织拥有全网 1/3 的 TEE 设备。

对于多链系统（下文将介绍 NBC 以多条并行链方案解决 TPS 瓶颈问题），我们将以 TEE 的唯一设备号（UID）为依据，在各条链分配矿工，设备编号唯一且不重复，我们用如下公式计算目标链号：

```
link_no = (MiningMask ^ UID) & (link_num - 1)
```

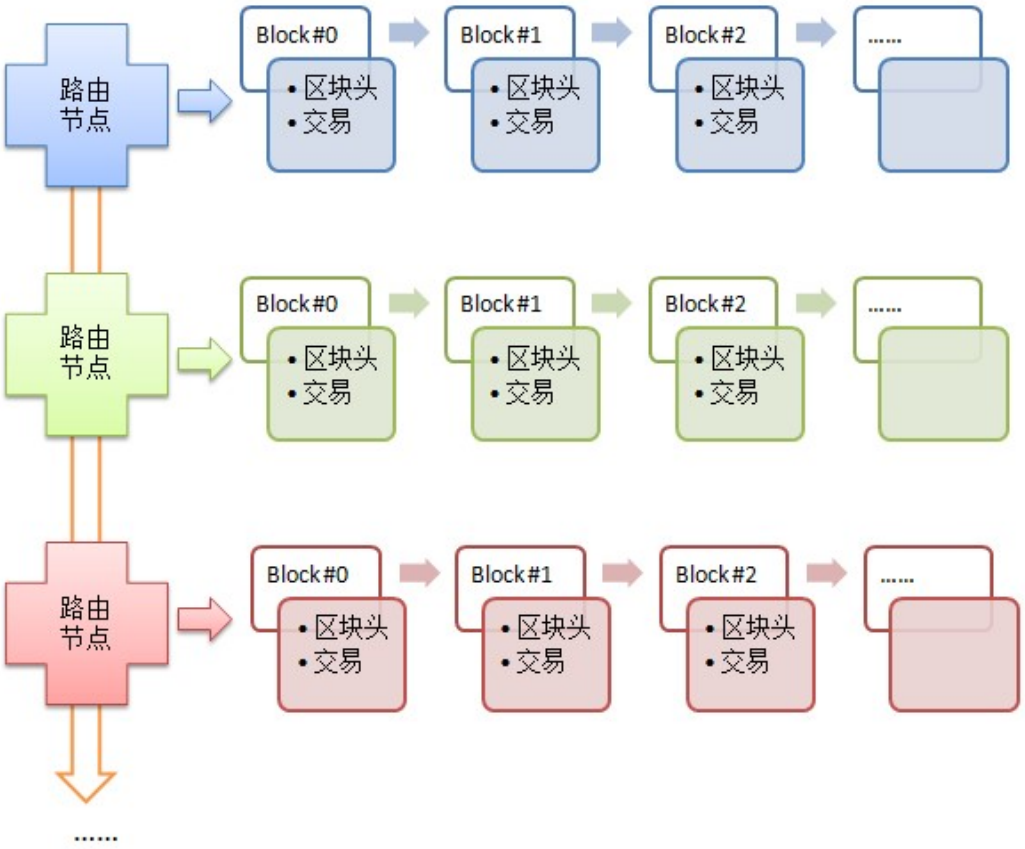
其中，link_num 为当前并行链总数（取 2 的 n 次方），MiningMask 是一个可配置的常量，称为链号掩码，链号掩码在一个时期内固定不变，但如有必要，只要本区块链社区达成共识，需要变换这个掩码来提高安全性时，这个 MiningMask 取值就可以变化。有了链号掩码设计，攻击者将难以通过收购具有特定规律 UID 的 TEE 来聚集算力，因为本区块链的维护团队一旦发现市场有定向收购情况出来，可随时变换 MiningMask 值，而从让攻击者的收购行为变得无意义。

从某种意义上说，NBC 的安全性高过 BTC。如果将 BTC 排名前 3 的矿池合并，哈希算力将经常超过 51%，他们要是合谋发起攻击，BTC 体系将岌岌可危。而在 NBC 系统想发动算

力攻击极其困难，一方面因为它的算力分布更加分散，另一方面，NBC 中的矿工身份是可信的，一个时期内实际参与挖矿的设备数目，可从区块数据统计出来，攻击者是否在某条链聚集算力可以识别，也能预警。而且，必要的时候，NBC 全网还可紧急切换至更安全的工作模式，即：只允许可信转账。

2.2 用并行链提高 TPS

并行链是现实中区块链系统切实提高 TPS 的有效途径，而且，也是近乎唯一的途径。NBC 系统中各个并行链直接由一个独立的路由节点负责跨链协调和通信。



2.2.1 单链如何提高 TPS

单链系统提高 TPS 只有通过调整三个变量来实现：区块大小、出块间隔和交易字节大小。

增大区块大小，虽然可以提升 TPS，但账本在各节点之间的同步时间变长，当有大量节点跟不

上同步节奏而不能及时获取最新区块时，系统软分叉将变频繁，安全性也变脆弱。在 P2P 组网中，每个矿工节点可与 M 个相邻节点建立通信连接，账本数据全网广播依赖于各相邻节点之间的通信，降低相邻节点间的连接数 M，虽然同样能提升传播效率，但同样也有限度，M 值变小后，数据及组网的冗余度也降低，系统稳健性跟随下降。

降低出块间隔时间，可以有效的提升 TPS，并且还可以提升交易确认的效率，但是出块速度是不能无限制提升的，节点间数据需同步，如果保持区块大小不变，出块越快，账本数据就越大，本系统出现软分叉与孤块的几率就越高，系统安全性会降低。

减少一次交易占用字节数，比如隔离见证（SegWit）方案，隔离见证确实在不增加区块大小的前提下实现了 TPS 提升，但是由于交易字节的大小不能无限制减少下去，最多只能减少 50% 左右，TPS 只能提升一倍多一点，从应用角度看，这个交易性能与支付宝相比还是相距甚远。

从理论分析和实践验证来看，在单链提高 TPS 十分受限。但是如果将单链的业务处理分配到多链进行，就能轻松实现处理能力的线性扩容。多链方案有主从链与并行链两种，主从链是一条主链加若干条辅链，并行链是多链并列，没有主导链，NBC 采用并行链解决方案。

在 NBC 系统中，单链处理能力约为 20 TPS， 区块大小设为 2M，一个区块可容纳 8 K 交易，平均每 5 分钟出一块，理论上 TPS 为 8K / 300 秒（即，每秒 26 笔交易，我们取 20 TPS 做计算），最多有 65536 条并行链，NBC 全网每秒可处理 131 万笔交易。这个量级基本上超过了支付宝等主流支付手段的吞吐量，更是远远超越了比特币系统每秒 7 笔的速度，可以满足当前各种应用场景的需求。

2.2.2 分配矿工到指定的链上工作

并行多链系统架构下，矿工节点不能自主选择在那一条链上工作，否则，攻击者只要持有一定数量矿机，集中到一条链上，很容易实现 51% 算力攻击。

NBC 系统通过三个步骤来限定矿工在哪条链上挖矿：

第一步，我们引入了一个 MiningMask 值，这个值是一个全局常量，系统升级时，如有必要可调整该常量，矿工节点挖矿所在的链号将由 MiningMask 值和矿工节点内 TEE 中固定唯一身份识别码 UID 推导而得。这个机制保证了 NBC 中的矿工以实在身份参与挖矿，虽然矿工不必

经过实名认证，但 TEE 保证他的身份不可伪造。这也让系统对矿工节点在各链的分布能实时监控，潜在算力攻击不仅可以预警，还能有针对性实施防御。

第二步，矿工节点只能捆绑一次钱包。这样，矿工节点所有收益将会固定到与 TEE 已绑定的钱包上，如果矿工节点作恶，系统将在第一时间阻断该矿工账号，让作恶意节点难以兑现他的收益。NBC 中矿工账号较为特殊，其一，它的 UTXO 未必在挖矿所在的链中维护；其二，从矿工账号转出资金只能以可信转账方式进行，其交易过程会被监督。

第三步，将当前链号配置的相关信息作为密钥，采用对称加密的方式将链内关键通信信息加密，如非本链矿机将无法进行正常通信，更无法参与挖矿。

通过这种机制，一台矿机在确定时段内，只能在指定的链上工作。至于具体该跑在哪条链上，源头决定因素是官方在 TEE 硬件发货前就预设过的 UID 值，此值不可改，攻击者更难以通过大量囤货（指 TEE 硬件），预谋在某条链上聚集算力。

2.2.3 账号归属

将矿工分配到各条并行链工作后，交易相关的各个账号的 UTXO 数据维护也要分配到各条并链上。因为转账的结果是更新各账号的 UTXO，让 UTXO 修改权分散到各链，实际也将交易处理的工作量分散出去了。

我们规定，任一账号的 UTXO 数据要归属到某条指定的链上，目标链号 link_no 计算公式如下:

```
link_no = VCN & (link_num - 1)
```

其中，link_num 为当前总链数，VCN（Virtual Chain Number）为虚拟链号，取值为 0～65535，这个值由钱包软件在生成一个账号时随机分配。

NBC 的账号地址与 BTC 的格式稍有差异，NBC 要在全网已唯一的地址基础上，再添加 2 字节的 VCN，因为 VCN 取随机值，各账号的 UTXO 数据将平均分散到各条并行链去维护。

2.2.4 安全漂流瓶

对于交易双方同处一链的交易，本链矿工将在本链内更新双方账号的 UTXO，其处理过程与常规单链系统没多少差别。如果交易双方的账号归属于不同的并行链，他们之间发生的交易就是跨链交易，为支持跨链交易我们引入了安全漂流瓶机制。

发起跨链交易时，系统将按一种中间地址格式在单链内处理转出或转入操作，比如，在转出操作完成后路由节点会自动拎取需做转入操作的交易，转发到另一条链上让交易继续。这种转发环节并不每次只针对一项跨链交易，而是自动合并同目的地的交易，一起打包后传送。这好比将若干交易集中起来塞到同一个瓶子，贴上目标地址后寄出，因为我们还额外设计安全传送、校验核实、异常恢复等机制，所以称之为安全漂流瓶。

2.2.5 并行链扩容

当 NBC 系统平均单链节点达到一定数量时，将启动扩容操作。

NBC 系统要求以倍增方式支持并行链扩容，初始总链数定为 2 的 m 次方，比如，全网初始设计 16 条（即 2^4）并行链，随着业务量上升，16 条链可扩大到 32 条，当 32 条处理能力不足时，再扩大到 64 条，如此倍增，直至 65536 条。

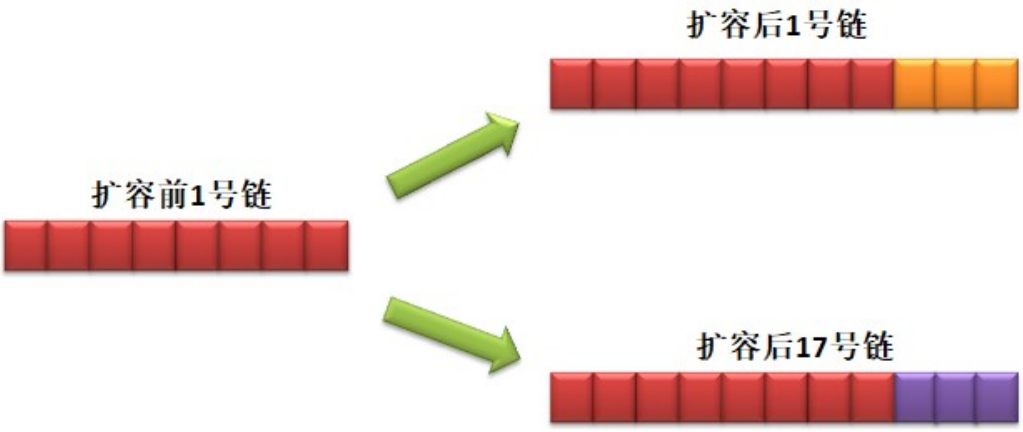
下面用公式表达扩容后的映射关系，假定扩容前全网总链数为 N：

```
Link_No = VCN & (2 * N - 1)
```

这种映射规则可以保证每次扩容都是一分二，而且从原有一条链去分叉，不会交叉乱序重新组合。倍增之前编号为 K 的链，将分裂为 K 与 N+K 两条链。这个方案的好处是，让扩容过程变得更平滑。以 16 条链扩容到 32 链为例，已有 R0～R15 路由节点，扩容后变成 32 条链，各链的路由节点分别是 R0 ～ R31。

并行链的裂变规则类似于细胞分裂，或者说是两兄弟分家，链内各节点持有的信息也一分为二，比如对于数据库，裂变后，各矿工节点只需将本地数据库中不属于自己管理的那一半记录删掉即可。扩容后账本数据将由分解后的各链独立维护，比如，1 号链分裂为 1 号与 17 号链后，

两条链将独立维护自己的区块链数据，下图不同颜色表示区块内容不同：



一分为二后，原有区块数据被两条新链原封不动继承过来，扩容后随时间推移，两条链将各自独立增加区块，而继承过来的前面部分数据是一样的，这相当于两条链拥有一份共同的记账历史。

扩容升级涉及并行链总数变更，由于安全原因每条并行链在升级中不能暂停区块生产，各链独立运行，升级须在跨越难度调整周期时启动，但各链跨周期所在时间点并不一致。所以，扩容中我们必然要空出一段时间让全网暂停交易，各链空转，等全网所有并行链都一分为二完成升级后，才重新启动交易。

2.3 秒级确认与可信转账

2.3.1 秒级确认

一次交易的等待确认时间是影响比特币系统在实际交易场景中落体的重要指标。比特币系统单次交易约需 1 个小时的等待时间，在实际商业应用中是无法容忍的。

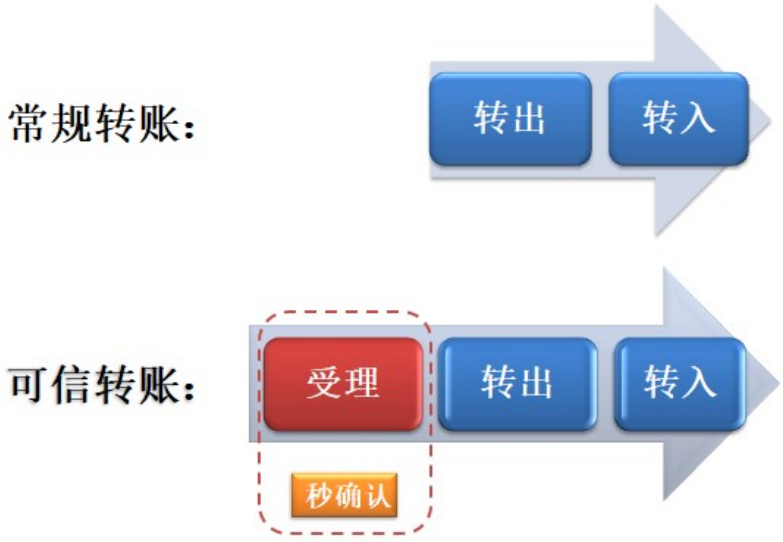
NBC 系统提供了一种快速确认交易机制，可以将单次交易等待时间缩小到数秒级别。其实现原理是，NBC 将交易过程划分为受理、出账、入账三个环节，路由节点用来保障 3 个操作环节的事务完整性。即：凡由路由节点受理的转账请求，都会纳入可信转账的处理流程，可信转账在交易受理后便进入不可逆状态，预设的转账金额一定会被转出。所以，这种交易在数秒内

路由节点即给出“已受理”的确认通知。

秒确认机制基于一个前提假设，交易是分级别的，有大额交易，也有小额交易，如果两者没有区分，小额交易也像目前比特币目前采用的方式，都等上 1 个小时才予确认，显然无法支持现实中商业应用的。NBC 系统的钱包软件允许用户指定当前账户是否缺省按可信转账方式去处理，因此，NBC 的用户通常会开设两个账户，一个用于大额支付，一个用于小额支付。

2.3.2 可信转账

NBC 系统支持两种转账模式：常规转账与可信转账。前者对应于 BTC 中 SPV（Simplified Payment Verification，简单支付验证）节点所承担的转账功能，NBC 继承了这种转账方式，即，将轻钱包应用接入到区块链的 P2P 网络，成为 SPV 节点。SPV 不挖矿，不必同步完整的区块链数据，在 SPV 发起的转账不必由其它节点代理，所以，常规转账没有受理环节，只有转出与转入两个环节。



可信转帐则由路由节点代理转账的发起，以及其后流程各环节。各路由节点拥有独立身份，用它的私钥对受理的交易加盖签名，以此实现交易授权；验证授权则用路由节点的公钥，公钥是公开的，各个矿工节点能用它验证交易是否已授权。可信转账机制要求各链所有矿工都遵循一项共识：只有本链路由节点已签名的本类交易，才能纳入处理，才能记录到新挖出的区块，其它矿工验证新区块内各项交易时，也会检验可信转账的签名是否正确。

NBC 全网共识授予路由节点对可信转账拥有阻断权，而对于常规转帐，路由节点则无此特权。在区分常规转帐与可信转账后，NBC 系统发展出两种运行模式：常规模式与安全模式。在常规模式下，常规转账与可信转帐均支持，而在安全模式下，全系统只支持可信转账。

2.3.3 链上治理

社区治理是促进区块链良性发展不可或缺的部分，十余年区块链发展历史也反映了这一点。与常规区块链系统不同，NBC 将常规的链上治理功能内置，把在线治理视作社区管理在链上的自然延伸。NBC 社区治理委员会（简称治委会）在线上系统中以一对公私钥表达身份，一条指令如果用治委会的私钥加盖签名，表明该指令从治委会发出，本系统所有节点都可以用治委会的公钥对签名是否真实做验证。治委会的公钥在产品源码中给出，用作一种可信源头，路由节点的公钥在网络中广播时，需由治委会私钥做签名，各节点用治委会公钥做验证，从而保障大家收到路由节点的公钥也可信。

经治委会签名的链上治理指令主要有以下几种：

1. 指示矿机节点设置所属链的路由节点公钥
2. 指示路由节点设置指定帐号阻断
3. 指示路由节点解除指定帐号阻断
4. 指示路由节点广播本系统即将进入安全运行模式
5. 指示路由节点广播本系统即将退出安全运行模式

值得注意的是，由治委会签发的指令都不必实时响应，而且，发布这些指令之前治委会都会对即将签发的操作发布公告，公示后才发出指令。而路由节点针对可信转账交易中涉及的帐号实施阻断却是实时响应的，当有矿工恶意记帐，尤其是制造双花攻击时，路由节点会立即阻断恶意记账后受益的帐号，同时也阻断恶意记帐矿工的帐号。路由节点从紧行使阻断权，可疑交易中受益账号先阻断，被阻帐号或许是无辜的，当治委会介入仲裁后，视实际情况有权解除针对特定账号的阻断设置。

虽然 NBC 的设计让路由节点拥有阻断权，但路由节点不参与挖矿，没有记账权。这实际在区块链中实践了分权制衡思想，并非挑战去中心化机制，NBC 仍按无中心方式实施记帐。

2.3.4 系统安全性

NBC 使用的 PoET 共识算法，从本质上看也采用了分权制衡思想。

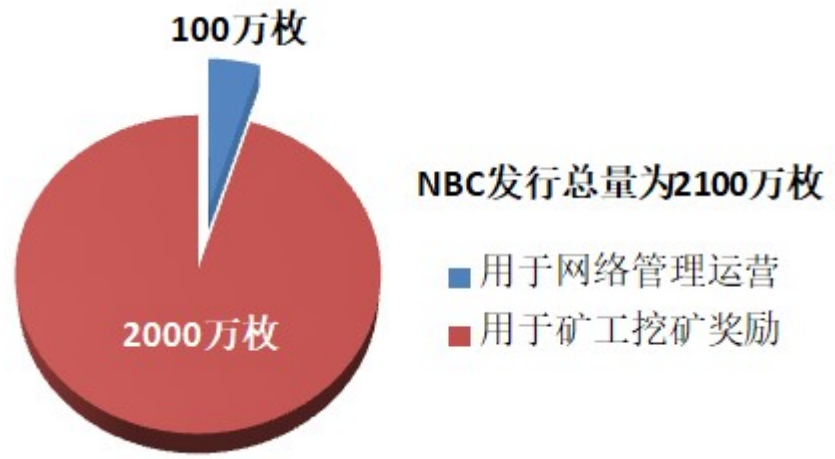
TEE 既保证矿工身份唯一且可信，还保证所有参与者挖矿机会在时间上平等分配，同时，NBC 设计全员监督机制，借助挖矿间隔实现一种便利的监督手段，计算同一矿工连续多次记帐的时间差，即可验证。如果有人作弊了其他矿工马上能识别，大家都不认可他生产的区块，所以作弊不会成功，即便是 TEE 生产商，对这种用出块时间差的验证方式也是无从作弊的。这里，TEE 控制单个矿工在哪条链如何获得记帐权，其它矿工则监督 TEE 的控制结果是否公平性，类似于行政与司法分离了，互相制衡。

普通运行与安全运行两种模式中，后者是 NBC 系统的高阶目标。在只支持可信转账的安全运行模式下，双花攻击虽可实现，但不再具备价值，因为即便攻击成功，获利也无法转出。不过因为路由节点由 NBC 团队负责运营，运营方需向公众证明他们不会作恶。最关键的证明措施就一条：识别所有双花攻击，阻断所有涉嫌双花攻击的账号，并让管控措施全程公开。做到这一点并不困难，因为分布式账本原本就是公开透明的，谁都可以查验。

3. 价值体系

NBC 系统采用 NBC 币作为一切费用和价值交换的标准价值单位。发行采用定量制，固定 2100 万枚，可以细分到小数点后 8 位，最小单位依然以聪 Satoshi 为单位，即，1 NBC = 10^8 Satoshi。

NBC 总发行方式分为两个部分，其中预留 100 万枚用于网络管理运营，2000 万枚用于矿工挖矿奖励具体分配如下图：



NBC 挖矿奖励同比特币保持一致，每 20 万个区块，奖励即自动减半。NBC 系统设置第一个 20 万个区块挖矿奖励为每区块 “50 NBC / 并行链数”，第二个 20 万个区块每区块矿工奖励为 “25 NBC / 并行链数”，依次递减，直到挖矿奖励趋近于零。

当 NBC 供应量趋近于零时，矿工的收益将主要以交易费为主。由于 NBC 系统改进了共识算法，矿工的挖矿成本将远低于比特币矿工的挖矿成本，只要 NBC 网络有足够的交易量，靠收取交易手续费依然有利可图。