Trinity 白皮书

基于 NEO 的链下扩容方案

（披露稿）

目录

1、摘要

面对区块链技术，人们期待其重塑经济和世界的同时，也被区块链当前共识速度慢、交易成本高、匿名性弱等现实问题所苦恼。

Trinity 通过状态通道技术对 NEO 进行链下扩容，通过协议分层、服务可插拔、服务可定制、基础服务免费、激励增值服务提供者等一揽子方案，来帮助用户方便快捷安全的使用区块链服务。

2、背景介绍

区块链的诞生，标志着人类开始构建真正可以信任的互联网。

区块链技术创造了具备价值唯一性和传递性的价值互联网，其实质是实现资产价值的可信流动。

区块链目前正逐渐让我们摆脱对全球各产业内中介机构、结算/清算公司与中心化服务提供商的需求，一步步改变着这个世界。

区块链技术不是一个单一的创新技术，而是一个集成了多方面研究成果的综合性技术系统，其中共识机制为其必不可少的核心技术之一。

由于硬件、带宽、节点数量、节点分布及共识算法自身局限性等客观原因的限制导致链上共识的达成往往需要消耗数十秒甚至数十分钟的时间，如此大的共识时延给区块链的落地商业应用带来了巨大的障碍。

由于区块自身数据结构大小的限制，导致区块中的空间资源是十分稀缺的，也是十分昂贵的，把不必要的指令类操作或者非结算类的中间数据存放到链上，会给区块链上的应用带来高昂的成本，同时也给区块链 P2P 网络的同步带来巨大的负担。

由于区块链上的数据对于所有用户都是公开可见的，把所有的数据和过程都存放在区块链上，也会给用户的隐私带来很大的困扰。

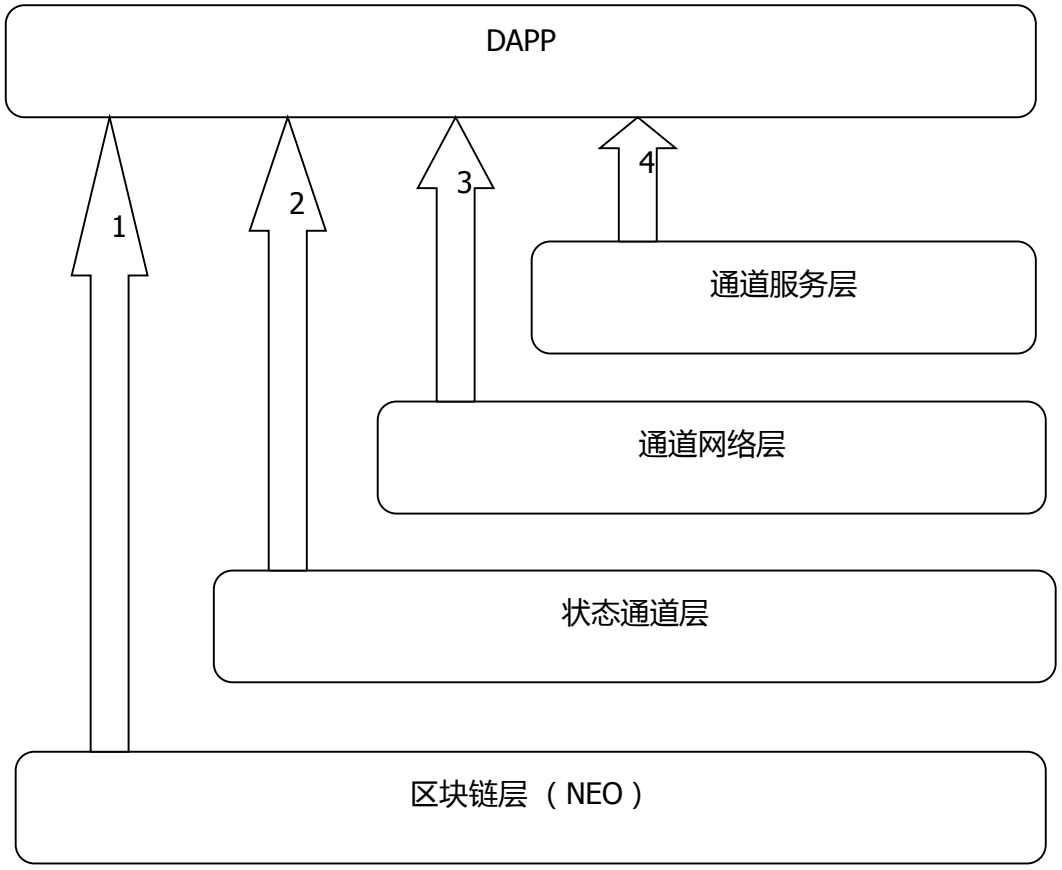
针对以上情况，业内产生了基于 BTC 的闪电网络、基于 ETH 的雷电网络等链下扩容方案；本项目为基于 NEO 的链下扩容方案。

3、项目概述

Trinity 是基于 NEO 的链下扩容方案，适用于 NEO 全局资产和 NEP-5 标准代币的区块链转账，通过资产证明进行链上信用背书、状态通道进行链下交易进而达成 NEO 链上资产的即时支付、低交易费用、可扩展以及隐私保护。

Trinity 致力于通过提供快速安全的链下支付通道，来帮助用户方便快捷安全的使用区块链服务。

Trinity 整体架构介绍如下：



Trinity 与区块链及 Trinity 各逻辑层之间都是完全解耦的，都可以独立为 DAPP 提供服务。部署在 Trinity 上的 DAPP 可根据自身业务需要调用 Trinity 的任意逻辑层的 API 获取 Trinity 各层对应的服务（如图中 2、3、4），也可以绕过 Trinity 服务直接进行链上交易（如图中 1）。

状态通道层为 Trinity 提供最基础的 P2P 状态通道服务，状态通道的建立过程即交易双方在区块链上进行资产抵押并建立智能合约为后续的链下交易作信用背书的过程。交易双方通过该层提供的状态通道服务就可以进行即时交易，零等待。该层服务适合 C2C 即时支付、个人高频数据采集等场景的 DAPP 使用。

通道网络层为 Trinity 提供状态通道的路由服务，该层为未建立状态通道的交易双方全自动智能选路。所有的状态通道都对应于链上的一个智能合约，一份资产抵押，由于资产抵押的成本问题用户不可能跟所有的交易方都建立状态通道，此时就需要借助 Trinity 的路由服务，完全无感知的进行状态通道选路，保障无直接状态通道的交易双发也可以进行即时交易，零等待。该层服务适合 B2B/B2C 即时支付、全网数据采集、去中心化交易所、即时币币兑换、IoT 规模互联等场景的 DAPP 使用。

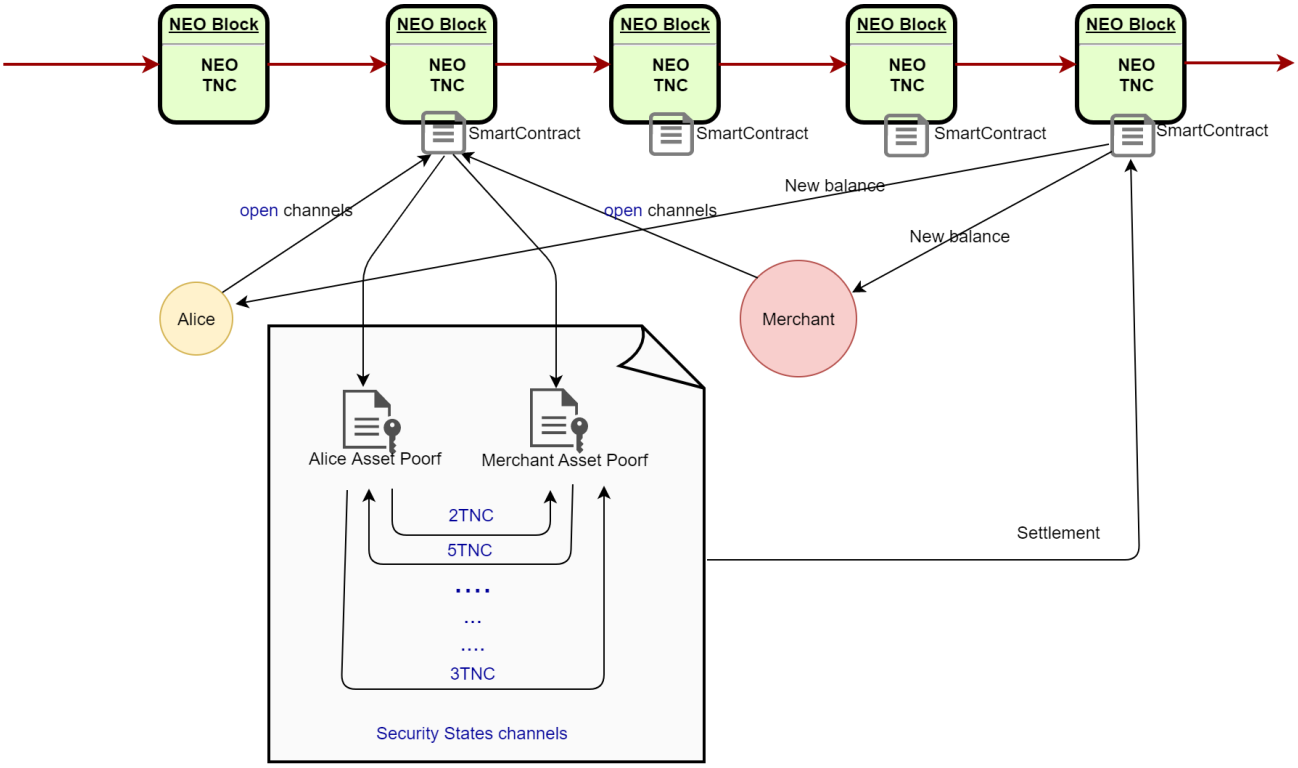
通道服务层为 Trinity 提供插件化、可定制的链下交易服务。通道原子层和通道网络层达成了让链上资产在链下快速流动起来的目标，Trinity 不仅要做到快，而且要做到又好又快。通道服务层就是为了改善交易体验而设置，不同的行业、资产、权益有不同的交易诉求，DAPP 可通过通道服务层进行自定义实现或者向 Trinity 定制个性化服务。该层的常见有：提供轻客户端的网关服务、提供隐私保护的混币交易服务、提供高优先级的状态通道路由服务（QoS）、提供端到端的面向连接的状态通道路由服务、提供通道检测代理服务等。

Trinity 与区块链层的完全解耦，也为 Trinity 后续的区块链移植及跨链交易服务奠定了良好的基础。如后续的本体网络移植及跨 NEO 和本体的资产即时交易服务等。

4、技术实现

4.1资产证明

链下扩展方案中，资产证明是一个关键因素，等同于结算准备金，它通过使用数字签名和哈希锁定传输来实现，也就是说它把主链上的数字资产进行了抵押后进行交易。



在上图中，假设两个交易参与者，一个是 Alice，一个是 Merchant。资产证明是指 Alice 和 Merchant 需要把主链上的代币资产进行抵押锁定，最终产生资产证明。比如 Alice 拥有 1000 某个 NEO NEP-5 资产，Merchant 拥有 1000 个 NEO NEP-5 资产，在链下交易转账之前，两者的这些代币可以按需要的数量被抵押冻结当作资产证明。如果产生不了资产证明，就无法进行代币转账。资产证明是由 NEO 区块链上执行的有约束力的协议。通过数字签名，确保交易双方不能随意退出价值转移。另外，由于链外的交易中，只有交易双方才能访问存在支付通道的智能合约中代币，这意味着 Trinity 资产证明跟主链交易一样具有约束力。

一旦主链代币资产被冻结，交易双方产生资产证明，双方可立即通过支付通道进行链外转账交易，且不受次数限制。当双方完成交易，可以把资产转回主链，并在

主链上进行登记资产余额变化，链外的交易不会留下记录，也就是说，交易了多少次，交易的数量等信息，都不会向全网广播，保护了用户隐私。

4.2智能合约

部署在链上的智能合约主要提供如下功能：

1) 为交易双方参与者提供一个共享的双方同时认定的交易规则

2) 发放认证交易令牌为链下支付提供保障

3) 智能仲裁，若交易双方有一方毁约，智能合约能公正裁决惩罚毁约者

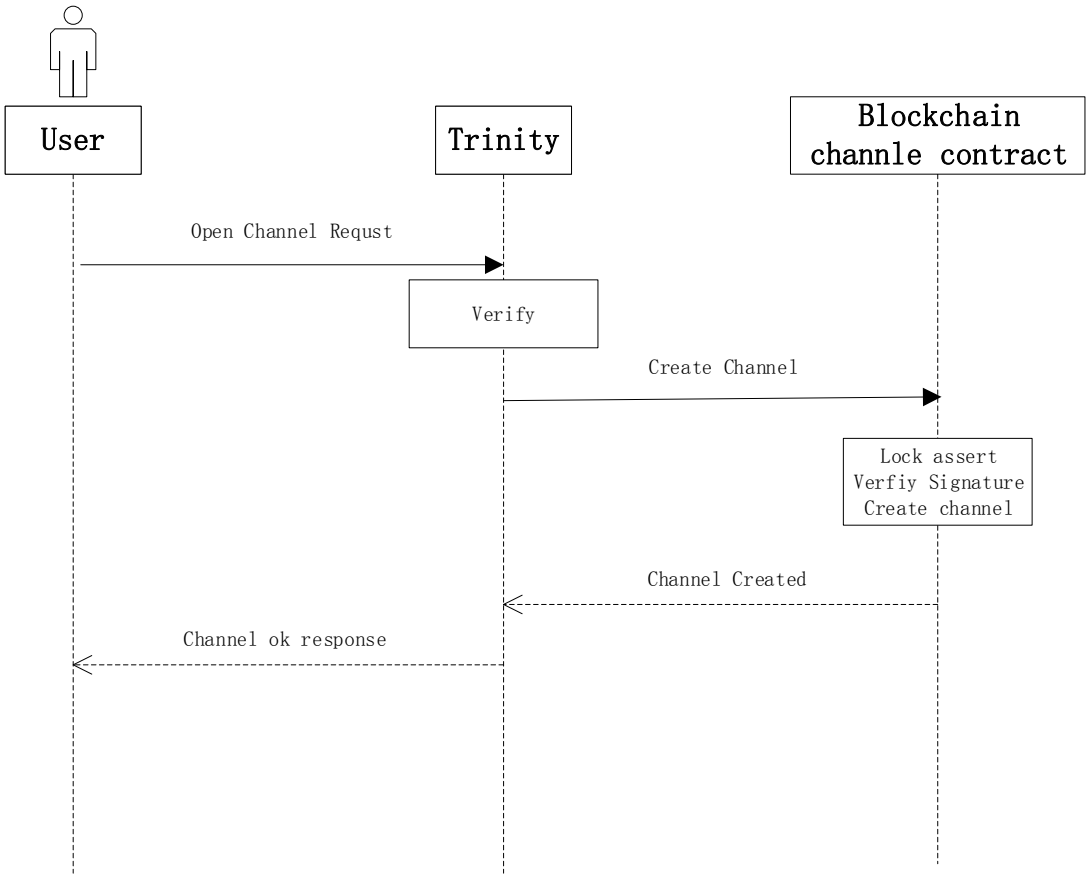
4) 通道管理，关闭通道，将链下交易进行结算然后链上发布

通道智能合同是一种可执行代码，它包含了操作一个链下支付通道的共享规则。当使用通道时，每个参与者都隐含地同意这些规则。通道允许：

1) 在通道参与者中有大量的双向值传输

2) 具有过期和预定义规则的条件值传输

3) 决定转让顺序的规则



每个通道都支持双向的链下支付通道。每个都有自己的结算周期配置。任何两个参与者可以存放任意次数，任意数量的押金。

交易可能有条件地完成，这意味着在任何时间点可能有多个正在等待完成的快速交易。 这些交易由包含交易数值，到期时间和散列锁的锁结构表示。所有还没有执行交易的集合由一个梅克尔树进行编码，并在每次交易中以其根表示。

通道容量等于两位参与者的存款总额。 容量既是交易可能具有的最大值，也是未交易中的资产总量。 容量分为每个参与者的可用和锁定余额。可用余额根据已完成交易的方向和价值在通道的整个生命周期内变化，可以通过参与者的存款或交易对手的支付来增加。 锁定余额取决于未交易锁定转账的方向和值，随着每次锁定转账而增加，并在转账支付成功或以其他方式减少。

参与者的余额 = 参与者的押金 + 收到的交易金额 − 付出的交易金额

$$Bn=Pd+Pr-Ps$$

锁定余额 = 锁定未交易的总和

$$Bl=\Sigma_{k=0}^{n-1}Tp$$

部署后，通道可能会收到来自任何参与者的多笔押金。 一旦交易对方确认，存款人可以用可用的余额进行转账。

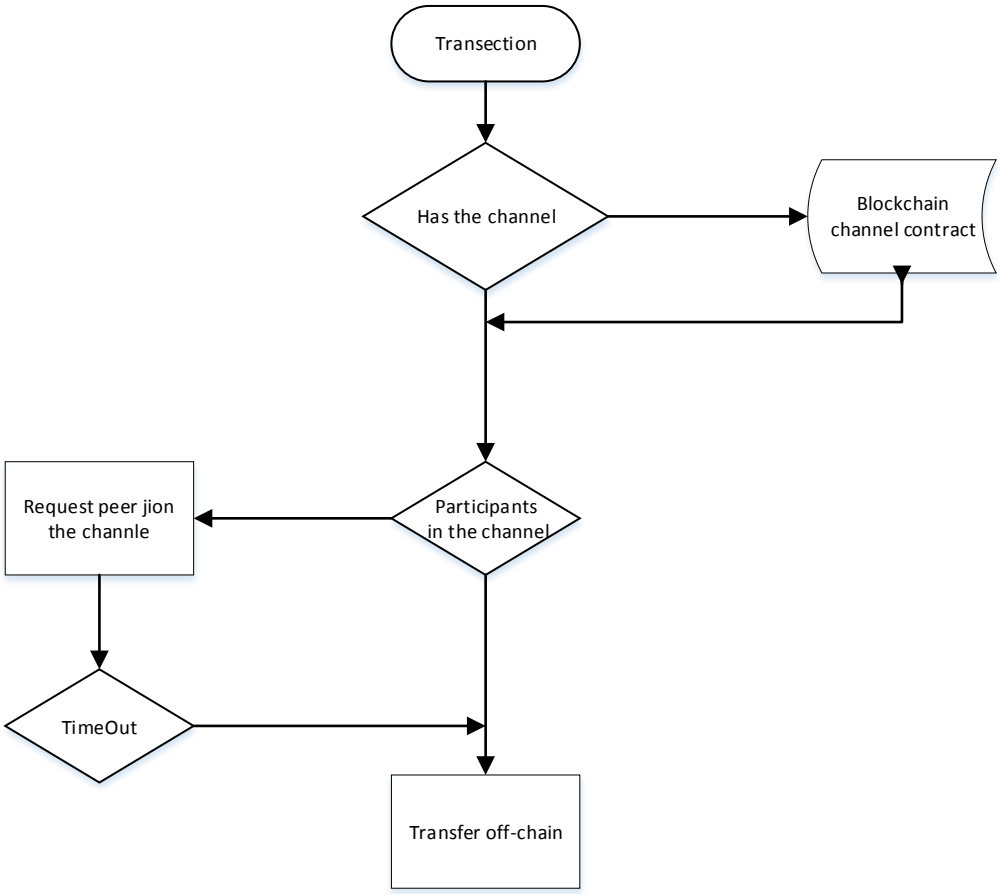
一旦任何一方想要撤销他们交易或发生争议，通道必须关闭。在关闭功能被调用后，结算窗口打开。 在结算窗口中，参与者必须更新交易对方的状态并撤销解锁的锁。 一方不能只执行部分撤销。

交易更新操作接收一个签名的资产证明，其中包含一个含有通道特定数据，包括梅克尔树根，交易金额以及一个交易序列的数据包。由于节点只能提供来自对方的签名消息，所以我们知道数据没有被篡改，并且是有效的。为了阻止节点提供旧的消息，提取的余额从传输的金额中扣除，这是一个单调递增的值。 因此，没有值为负的交易，那这样如果参与者提供了一个较老的消息，那么违规者的净额结余将会变小。

另一个通道操作是锁定撤销。 它接收一个由锁数据结构组成的解锁证明，来证明这个锁被包含在梅克尔树中以及有解锁它的密码。 通道通过重新计算梅克尔树根和校验密码来验证这把锁。 如果所有验证都通过，交易对手的转移金额就会增加。

4.3状态通道

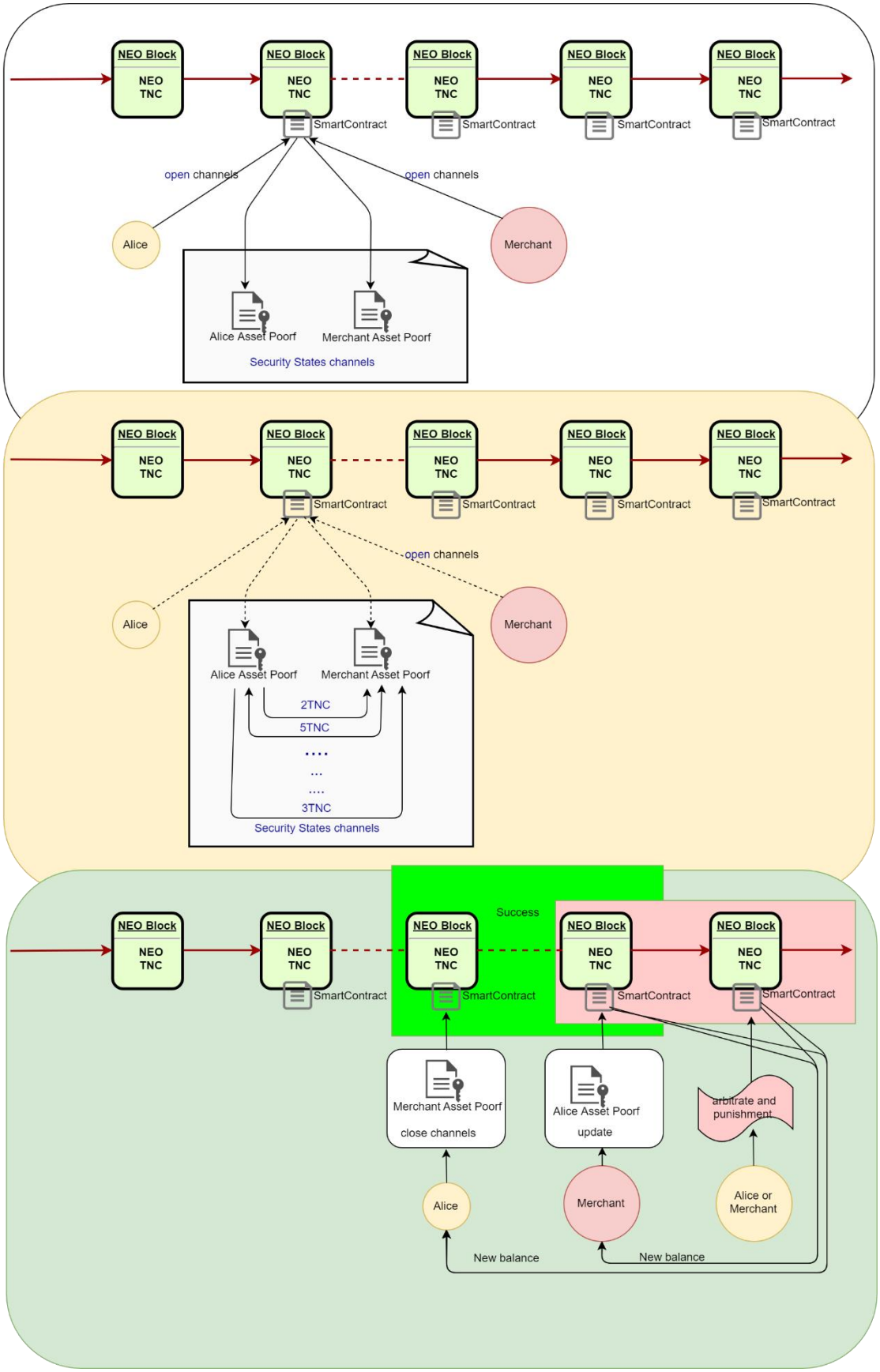
Trinity 通过链上的智能合约鉴权参与者，锁定/解锁保证金，裁决纠纷来管理状态通道，通过 Trinity 链下协议实现链下的交易。



4.3.1 通道的生命周期

生命周期时间，代币会被锁定，确保代币只能在通道中发送和接收，直至交易通道关闭，这样可以防止双重支付给其他人。一旦一个渠道创建，参与者可以发起认证检查。每个对等交易方无需查看所有记录，只需跟踪最新部分。资产证明包含了所有 Trinity 网络转账中发送给参与者的最终总额，由发送人进行数字签名。

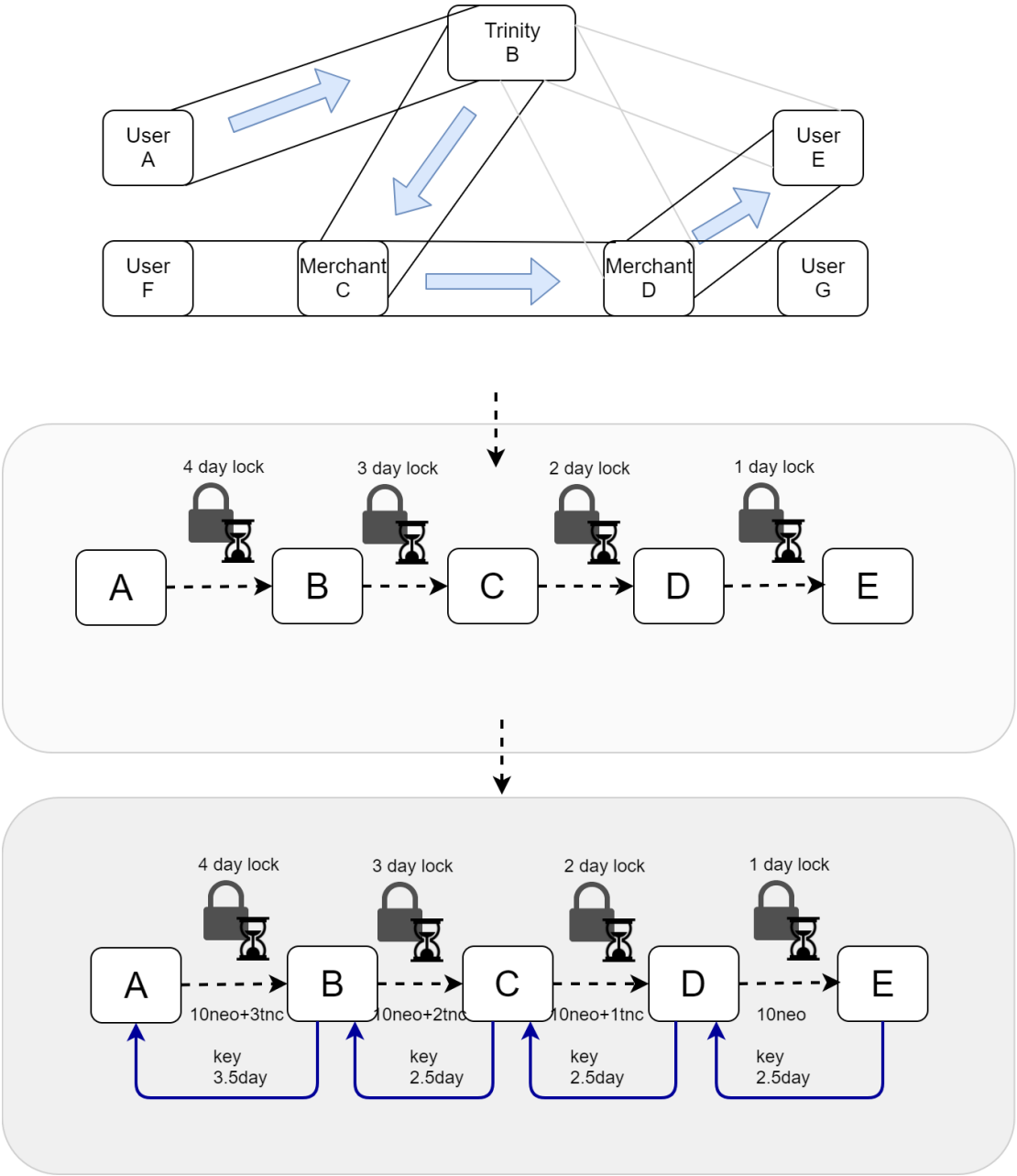
当一方决定在区块链上结算资产，可以要求对方付款也可以支付未付资产，交易者可以随时通过向智能合约提交供其选择资产证明关闭支付通道。另一方没有关闭通道，必须提交资产证明，如果没有转账则无需操作。在双方提交资产证明后，就可提取存款。如果有一方没有及时提交资产证明，资产会根据结束者的证明来确定资产。



上图是关于 Trinity 网络支付通道整个生命周期的示意图。

4.3.2 通道网络

支付通道的创建和结算必须在区块链上执行。因此，为每个潜在目标创建新的通道显然是不可行的。Trinity 则通过创建支付通道网络来解决这个问题，每个参与者通过支付通道网络都能彼此连接。



如图，A 想把加密代币发给 E。A 必须先找到一条连接到 E 的网络通道。连接路径的每个参与者需要合作让 A 能顺利把代币转到 E。参与者通过支付转发到下一个节点，这样把通道租借给了 A。加密哈希锁定防止所有这些中介转账被记入，直到 E 确认收到 A 的代币。一旦 A 决定解锁付款，她把钥匙给到 E 即可。

因为通路上的每位参与者解锁他们的收款都会有激励，密钥很自然通过通道传回 Alice。所有锁定的转账都可以用 Alice 密钥进行链上兑换。但是，参与者最好将锁定的转账价值合并成标准资产证明。包含锁定转账价值的资产证明和让锁本身无效都可以同步到通道状态。这样就完成了多方转账。

网络中的对等方不会把自己的通道免费被使用。毕竟，转账会带来额外网络流量和支付通道的不平衡。因此，Trinity 网络的参与者因为租用通道而付出费用，费用还可以通过激励来促使支付通道由不平衡向平衡发展。

4.4链下交易

链下的所有交易都要按照资产证明的格式进行编码，来保证了通道的通信一致性和安全，这些信息包括:

1) 交易序列
2) 转移的数量
3) 挂起
4) 交易梅克尔树的根节点
5) 包含上述所有内容的签名

Trinity 提供如下两种 off-chain 的交易方式：

1) 直接交易
2) 路由交易

4.4.1 直接交易

直接交易不依赖于锁来完成。 网络数据包发送完成后自动完成。 由于传输是在异步网络上运行，无法以原子方式完成。 要考虑直接交易的要点如下：

1) 消息没有加锁意味着传输消息的报文数量是会不断增加的，并且这些报文中可能存在撤销交易的报文。这就是说，付方会无条件的支付交易，不管有没有得到服务

2) 付方必须假设当消息报文发送到网络交易就完成了

一个成功的直接交易只需要 2 个消息报文，交易消息和确认消息。举例：Alice 想付给 Bob n 个资产，Alice 首先创建一个新的交易报文。

Alice 签名这笔交易并发给 Bob，这样就认为交易完成了。

4.4.2 路由交易

路由交易往往使用在通道网络中，会有发起人和交易人以及很多的中间节点。为了保证交易的隐私以及不被篡改，中介交易给设计成一个带有哈希锁的交易，这个哈希锁里带有交易的数目，该锁同时用来验证解锁它的密文和锁的期限。

同样来举例 Alice 和 Bob 的例子：

Alice 想付给 Bob n 个资产，Alice 首先创建一个新的交易报文

1) Alice 签名交易并发给 Bob

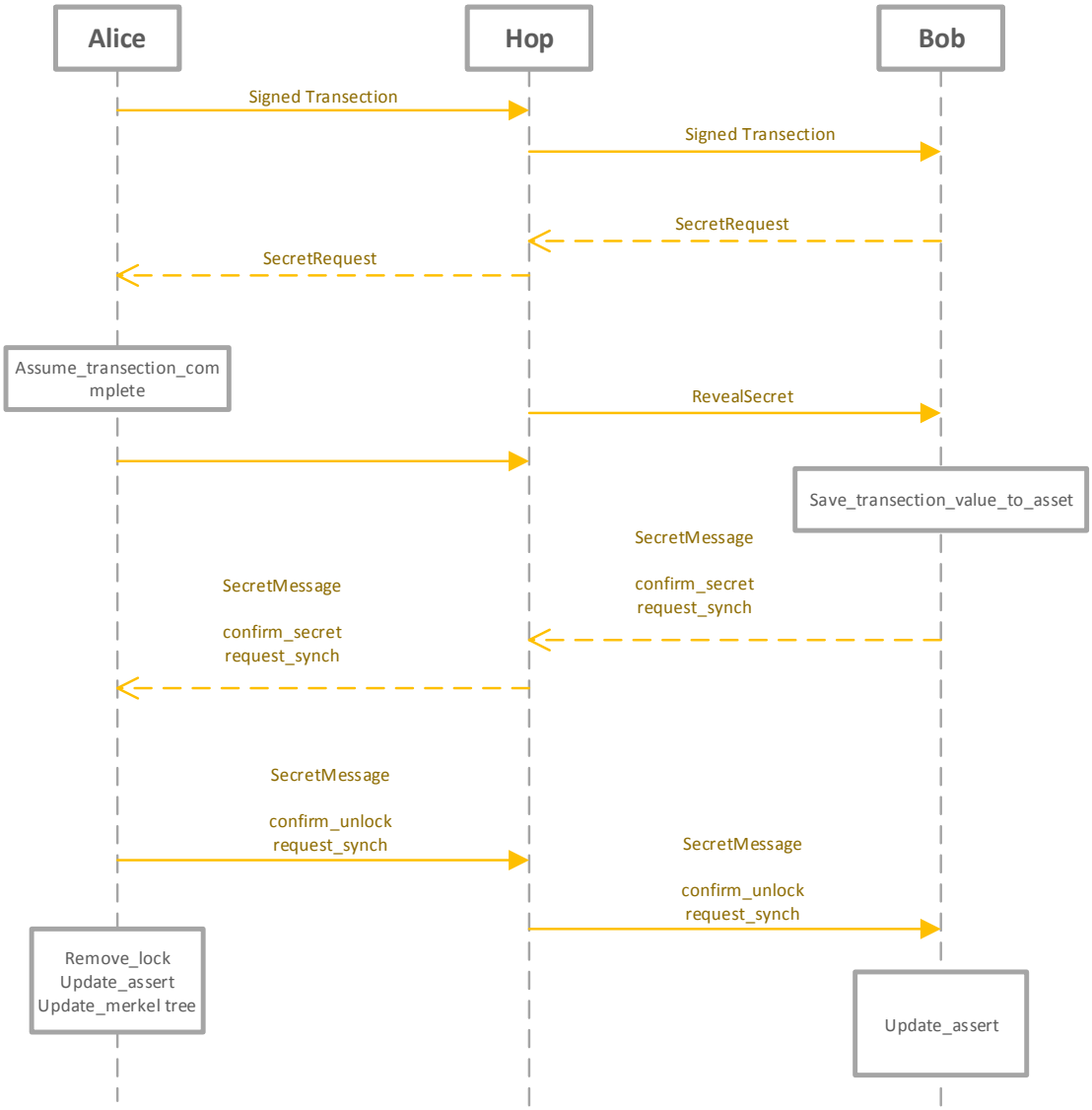
2) Bob 发送秘密请求报文给 Alice 用来请求撤销交易使用的秘文

3) Alice 发送密文给 Bob 并且在这个时候她假定交易已经完成

4) Bob 收到密文，此时他已经将 n 个资产交易到自己这一边

5) Bob 发送一个含有密文的报文给 Alice，来声明密码已经知晓并请求链下同步

6) 最终 Alice 发送一个密文给 Bob，该报文同样也是通知 Bob，锁将从梅克尔树删除，并且交易金额和树根将更新



5、Token 介绍

数字代币经济体系的核心是通过 token 的激励让整个生态自运转起来，Trinity 网络的高效运作离不开激励体系。TNC（Trinity Network Credit）--- Trinity 网络积分，是保持 Trinity 网络状态通道平衡性的重要基础。

5.1Token 的功能及价值

Trinity 的核心是状态通道，为了让状态通道被更多的用户使用起来，以便构建整个微支付的生态习惯，使用状态通道本身是免费的。即不持有任何 TNC，也是可以 Trinity 提供的基本状态通道服务的。

Trinity 为了保证状态通道的可用性，需要很多参与者共同协作，TNC 可以起到重要的激励和平衡作用。

TNC 的使用场景：

1) 统一的网络结算资产

在通道建立的时候，使用 TNC 作为资产抵押，这样不仅能提供易用的统一的结算方式，对于一些不希望也不具备同步整个链上资源的中小型节点或用户来说，使用 TNC 是最直接和方便的一种方式。统一结算机制为链下和链上交易减轻了不必要的兑换开销。

2) Trinity 网络的构建奖励金

Trinity 提供状态通道的路由来增强整个网络的交易便捷性，由于通道路由的存在，可以有效的使通道在多用户或节点间进行状态交互和价值传输，也就给 Trinity 网络提供了更高的灵活性和便捷性，TNC 作为一种网络积分，能有效的奖励通道路由经过的中间状态通道，使更多的节点或用户乐于参与到网络的通道中来，为更高效的资产流通提供保障。

3) Trinity 网络的增值服务

Trinity 是一个重视隐私保护的网络，在 Trinity 中使用了包括零知识证明、混币交易等多项技术保障数据的安全，增强用户的隐私保护，在 Trinity 网络中，TNC 可以用来支付更隐私的保护服务。

Trinity 网络节点还提供了如状态通道的 QoS、面向连接的通道路由、轻客户端的网关服务、通道状态检测代理服务等增值服务，这些节点可以通过收取 TNC 来获取提供增值服务的报酬。

DAPP 开发者也可基于 Trinity 的通道服务层自定义开发增值服务，这些增值服务可以提供给 Trinity 网络的用户进行直接使用，DAPP 开发者可以通过收取 TNC 来获取报酬。

4) 网络服务费用

Trinity 网络致力于为中小型企业提供数字化资产的服务，对于使用 Trinity 网络来发布或管理数字资产的中小企业，TNC 可以用来支付所需的服务费用。

5) 企业定制服务费

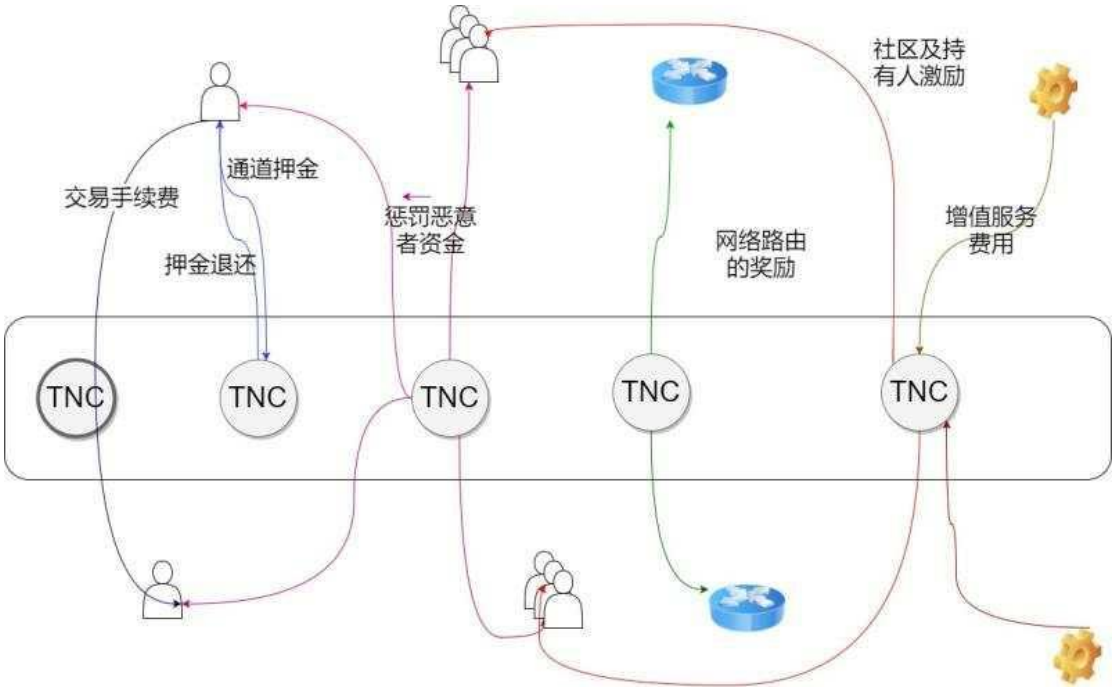
如果某些企业需要定制化的服务，比如自己独立的状态通道节点，高度定制化的钱包，这些定制费用需要以 TNC 的方式提供。

6) TNC 持有人和社区开发者的激励

对于持续关注和支持 Trinity 社区的开发者，Trinity 将通过 TNC 代币的方式奖励以吸引更多优秀的开发者加入到 Trinity 的社区开发中来，来不断的完善和优化 Trinity 协议。

对于持有 TNC 的用户来说，Trinity 会不定期的将 TNC 以奖励的方式下发给 TNC 持有人，来激励更多人参与到 Trinity 的网络构建当中。

随着 Trinity 整个网络的不断发展，参与进来的协作者不断增多，TNC 的使用场景及价值会不断增加。



5.2Token 的分配比例

总发行量	**1 Billion**
第一部分 非公开捐赠	**111, 111, 111**
第二部分 公开捐赠	**222, 222, 222**
第三部分 运营分配	**152, 663, 333**
第四部分 ESOP （锁定3年，1年后每年解锁33%；2019年2月首次解锁）	**180, 670, 000**
第五部分 基金会锁定 （锁定3年，1年后每年解锁33%；2019年2月首次解锁）	**333, 333, 333**

第一年流通供应	485,996,666（2018年2月 – 2019年2月）
第二年流通供应	657,331,110（2019年2月 – 2020年2月）
第三年流通供应	828,665,554（2020年2月 – 2021年2月）
第四年流通供应	999,999,998（2021年2月 – 以后）

注 1：首次向捐赠者发放 TNC 时，TNC Neo 智能合约富豪地址排行将列出第 4 部分和第 5 部分，以便社区监督。

注 2：所有捐赠者，无论通过公开或非公开捐赠，按同样的兑价计算 neo 捐赠额。私人捐赠者不享受折扣。

注 3：第五部分的分配将在以后的文件中详细解释。截至目前，Trinity 基金会正考虑将 TNC 自动分配给状态通道运营商、支持者和社区贡献者。但是，绝对不可能将第五部分发放给所有现任的 Trinity 基金会董事或团队成员。

6、团队展示

6.1 创始人及团队

李一灵

创始人

前小蚁(Neo)海外经理，负责 16 年小蚁的全球代币众售及其后续的社区建设、商业合作、生态建设等。FourierPR 联合创始人，中国顶尖的加密经济项目 PR 与咨询企业，Fourier 的客户主宰了 coinmarketcap 前一百的列表；与 FBG 合作。垒石科技创始人，媒体网站 inwecrypto.com, 多资产钱包 InWeWallet

张广峰

联合创始人

密钥安全及区块链领域专家，拥有 15 年以上的技术开发经验。曾就职捷德（中国），中钞区块链研究院，从事银联 PBOC2.0/3.0 规范的制定及推广，基于数字货币和区块链技术的数字票据系统的设计与开发。

易锋平

联合创始人

区块链行业政府事务专家，具有丰富的政府从业背景和资深的区块链项目渠道拓展经验。2015 年底进入以太坊爱好者社区，一直负责区块链应用和技术在社会及政府领域的拓展。曾经有政府商务工作背景，有出色的团队管理能力和过硬的执行力。先后任上海分布信息科技公司政府事务总监和同济金融科技区块链研究院副院长，推进公司参与工信部区块链参考架构和政府相关区块链政策的编写工作，参加贵阳市政府在国内第一个诚信农民项目在当地的合作和落地。

李扬

核心开发人员

软件交付专家/咨询师，成都地区颇具影响 力的软件架构意见领袖。专注于互联网初创公司技术咨询、团队孵化以及初始产品交付，帮助建立的初创团队/公司涵盖了数 码艺术资产交易、数据挖掘、智能农贸等众多领域。在此之前长期服务于电信相关行业，是电信 AAA 技术领域专家，多个省级电信千万级宽带接入服务系统的创建者。毕业于国防科学技术大学。

吴伟

核心开发人员

从事软件开发测试 10 年，曾就职 NOKIA，从事软件开发，I&V 专家，测试自动化教练等职务 基于自然语言处理的自动化自动测试工具项目发起人 区块链技术爱好者，Hyperledger Fabric 的中文 gitbook 文档译者

刘源

产品经理

网络传输协议专家，软件架构师，拥有 11 年无线通信、云计算等产品研发经验，曾就职于中国电信新媒体事业部、诺基亚 WCDMA 部门、华为 2012 实验室。多年来一直专注于互联网基础设施领域的产品研发，先后推动基于 100GE 包交换的数据中心产品、基于 3GPPWCDMA 的无线通信产品、基于 kvm 的云计算产品的商用落地，有幸和业界同仁一起通过革命性基础设施产品的商业应用落地先后开创了数据中心的 100GE 时代、移动互联网时代及云计算时代。

田梦楠

社区经理

区块链行业爱好者，曾就职中国最早的比特币交易所比特币中国，从事区块链数据分析，区块链交易所运营以及交易所产品设计等工作，对区块链各项目及交易所有较深的行业经验。拥有丰富的线上营销及项目管理经验，早期曾就职于谷歌（上海）及哈佛上海中心。

6.2 项目顾问

徐敬程

数字货币基金 Badwater Capital 联合创始人，RPX, CPX, VEN, REQ, ZRX 等项目的早期支持者。曾就职于位于硅谷和中国知名早期风险投资基金 DFJ Dragon Fund,从事 TMT 领域的风险投资。从事投资之前，创业项目曾获得 IDG 资本风险投资并于 2016 年收购退出。

季宙栋

本体首席战略官，资深区块链专家 前 500 强集团区块链负责人，担任工信部区块链产业发展论坛副秘书长，先后参与工信部白皮书编写和有关标准发布，撰写有《区块链开发指南》等专业书籍

李彦博

NKN 创始人 & Onchain 联合创始人 历任美国高通，红点科技高级研发工程师及技术总监 Linux Kernel 网络层核心代码贡献者， 专长于分布式网络系统架构设计， Mesh 网络协议实现 现负责 Onchain 北京分公司管理及开源区块链平台 DNA（Distributed Networks Architecture）开发 曾于斯坦福大学师从 Dan Boneh 学习，良好的应用密码学背景。

7、风险及免责

1) 本文档只用于向主动要求了解项目信息的特定对象传达信息使用，并不构成未来任何投资指导意见，也不是任何形式上的合约或承诺。

2) 参与者一旦参与 TOKEN 分发计划，即表示了解并接受该项目风险，并愿意个人为此承担一切相应后果。

3) 项目团队明确表示不承诺任何回报，不承担任何项目造成的直接或间接损失。

4) 本项目涉及的 TOKEN 是一个在交易环节中使用的加密数字编码，不代表项目股权、收益权或控制权。

5) 由于数字货币本身存在很多不确定性(包括但不限于：各国对待数字货币监管的大环境、行业激励竞争, 数字货币本身的技术漏洞)，我们无法保证项目一定能够成功，项目有一定的失败风险，本项目的 TOKEN 也有归零的风险。

6) 虽然团队会努力解决项目推进过程中可能遇到的问题，但未来依然存在政策的不确定性，大家务必在支持之前了解区块链的方方面面，在充分了解风险的前提下理性参与。

8、联系我们

联系人：Mona Tian

微信：M0n9mmm

邮箱：better.mona@gmail.com