目录

1、摘要..... 3
2、研发背景..... 3
2.1 发展背景..... 3
2.2 市场现状..... 4
2.3 用户痛点..... 5
2.4 使命和愿景..... 6
3 、技术支持..... 6
3.1、区块链概述和机制..... 7
3.2、COC 设计概要..... 8
3.3、核心思想..... 9
3.4、电子钱包..... 10
3.5、比特币清算中心..... 11
4、生态体系..... 15

4.1、Aanl Cosis 环状拓扑中继技术.....15
4.2、CO-Mbicads 兑换网络.....16
4.3、OnePay 闪电支付网络.....17
4.4、COC 的分布式控制链区块内部结构.....18
5、COC 加密与效率.....19
6、商业模式.....21
6.1、 数字资产消费的 Gas.....21
6.2、 算力费用.....21
6.3、 兑换费用.....22
6.4、手续费用途.....22
6.5、手续费抵扣.....22
6.6、用户激励.....23
7、项目计划.....23
7.1、分配计划.....24
7.2、团队拥有的代币说明.....25
7.3、 产品和运营团队.....25
7.4、 市场和营销费用.....26
8、团队介绍.....26
8.1 主创团队.....26
5.2 顾问团队.....27
9、发展规划.....27
10、风险提示.....28
11、免责声明.....29
12、参考文献.....29

1、摘要

COC 是一个开放的分布式验证节点网络，网络内的验证节点将约束所有参与者的行为，且不属于任何一方。它正在构建一个具备去中心化交易、流动性提供机制、清算信息网络和资产支持的区块链网关，并且使用协议代币机制来创建股权证明区块链，以便在参与者之间实现市场活动。与其他去中心化交易方式不同，这个高性能的分布式网络在无需可信任的网关代币的基础上，允许不同区块链间直接进行去中心化交易,也支持不同资产类别间的交易——无论是由法币支撑的发行方，还是完全去中心化的数字代币（ERC-20 类别以及本地化的加密数字货币）。通过去中心化监管以及市场活动透明度的提高来鼓励市场保障，市场利差将显著下降。配对委托交易账本的正确性可以通过使用智能合约以及协议代币保证。这种新型历史交易数据的结构是由太坊担保清算活动以及通过使用以太坊智能合约来保证的。

2、研发背景

2.1 发展背景

从 2017 年初开始，各类代币持续升温，以纯区块链资产交易平台的代表币安为例，注册用户已经达到 400 万的规模，单日交易额达到 100 亿美金（参考 Coinmarketcap.com 的 2018 年 1 月 4 日数据）。即使以单边交易手续费 0.1%计算，日均收入也能达到 2000 万美金。而且市场还在迅速扩大。 以 Coinmarketcap 的数据统计来看，目前全球区块链资产的总市值已经超过 7000 亿美金，单日交易规模超过 600 亿美金，其中比特币的交易占比从之前的 90%已经下降到 33%。 另外，根据不完全统计，全球区块链资产的拥有者大约在 2000 万左右，这个数字相对于区块链资产的用户规模也将有巨大的发展空间。 从最近半年的发展趋势来看，总体区块链资产市场无论是从

总市值，单日交易规模，还是从用户基数来看，这个市场目前在一个快速发展的通道，其典型的特点是人口在净流入，资金在净流入。

当然，随着区块链资产的迅猛发展，各国态度也大不一样。日本是全球第一个给区块链资产交易所发布牌照的国家， 目前有 16 家交易所拿到牌照。其它国家和地区例如新加坡，迪拜，以色列，瑞士等地方对于区块链资产总体上也持相对开放态度。区块链资产从总体上来讲，从争议到逐渐步入普通人的生活，这个大趋势已经很难阻挡。

2.2 市场现状

区块链的主要作用是解决网络参与者间的多边协议之间的协调问题。通过确保透明度，保障以及执行，我们可以有效达成多方共识，而这在以前是不可能实现的。当网络内参与各方发现业务不仅透明化，而且运行机制无法轻易改变，那么它们会更愿意进行协调。参与者显然更能确保，任意一方很难通过改变业务流程或利用信息不对称来强行收取暴利益租金。换句话说，任何单个参与者都更乐意使用业务流程和机制本身不属于任何其他单个参与者所拥有的系统。支付处理商，网关和金融机构之间存在着基本的协调问题。例如，银行的客户希望在另一个网络上支付商家。过去，建设一个在支付网络和机构之间兼容的支付系统是一项浩大的工程。这个过程通常是通过建立一个管理交易的交换所，即使用与中央交易对手清算中心或者银行往来帐户的通信网络，例如 FedWire，CHIPS，SWIFT，消费者支付网络，NSCC / DTCC，OCC 和 ACH。这些网络服务于不同的角色和功能，包括本地/国家支付，国际支付，信贷，股票/资产交割和衍生工具。这些中心化网络允许控制实体随意更改机制，在信息成本，尽职调查和所有各方之间的合同执行的过程中导致交易成本大幅度上升。我们认为，目前使用新型支付平台来颠覆数字支付存在着广阔的新兴市场（例如Venmo，支付宝等） 。这些网络对于跨网络的交易具有重

大的意义，因为它们通常需要承担显著的与交换设施相互信任的间接成本。缔约方不愿意使用中央交易对手，因为任何一方都不希望听从对方，并且使用银行往来帐户需要参与者之间制定合约。虽然较大的网络有足够的动力保护自身的网络影响，但我们相信大多数机构都希望能够提供电子钱包服务，并且这些服务需要多方参与者之间进行更多的协调。这些中等规模的参与者将能够实现网际价值交换，以便在可用性方面有足够的网络影响。这些基础设施和参考前端使网络效应被编码到这个网络中使得新的电子钱包用户可以立即创建高级网络设施。区块链允许社会将全世界的业务流程从单中心公司转化为开放的、去中心化的计算网络。COC 是一个将市场流动性，交易委托账本配对执行、清算中心保管以及可扩展支付去中心化的网络。这将有助于解决新兴电子钱包支付网络间进行支付的问题。通过将这些传统上放在一个单一公司中的商业流程进行转化，我们有可能在一个高性能的开放网络中为电子钱包提供商提供一个完全的交换方法。

2.3 用户痛点

2.31 数字货币管理不便：

数字货币的存储和管理仍困难重重，数字货币市场的快速发展将受到掣肘。现如今在用户面前的一大拦路虎就是如何安全备份一种数字货币的地址秘钥。随着越来越多的数字货币种类开始涌现，用户在管理不同资产的难度进一步增加。当下用户的选择不外乎两种——一是使用不同的去中心化钱包来管理对应类型的数字货币；二是让中心机构通过交易所代为管理。前者给用户管理和体验带来诸多不便，后者存在的安全隐患又使人望而却步（中心机构被攻击，或经营不善倒闭等情况将带来资产损失）。因此，该领域服务商一直努力的方向是：如何更好的兼顾安全性和便利性。

2.32 交易和兑换门槛高：

非专业用户注册交易所需要严格的实名身份认证，而当下数字货币的流通不能绕过交易所，这对于参与者与缔约者体验非常不利。数字货币的交易通常还会有一定限制，用户有必要读懂相关流程和操作步骤；且数字货币间的兑换一般需要以法币为媒介。第二种是类似 localBitcoins 提供中心化的交易方式，只要交易双方之间认可，可进行一对一交易。但这又带来了另一隐患，交易双方的数字货币将不得不被平台方托管，网络攻击、监守自盗等难以监管的手段将再次死灰复燃。

2.33 区块链开发成本高、算力浪费大、连接现实世界难：

区块链技术的发展潮流将势不可挡，未来的众多企业将不得不张开双臂拥抱区块链技术，而开发区块链所必须的高昂成本将使得企业望而却步；由于众多缔约者相互之间的竞争极为激烈，使得在 POW 的挖矿模式下，算力低下的矿机将会被淘汰，资源无法被有效利用。而 POS 机制缺失了 POW 的去中心化优势；现实社会的数据很难被区块链技术获取，比如股市变动、职位升迁、天气如何等等数据，现实世界数据量如汪洋大海一样不可描述。显而易见，矿工不可能提供企业任何想要的数据，而区块链连接现实世界难在于企业如果完全自己提供这些数据，又做不到去中心化的特性，很难让人信服。

2.4 使命和愿景

COC 致力于为大众提供一个安全、便捷、高效的数字资产平台，通过打通数字货币与实体世界的连接，让每一个人随时随地便捷的使用你的数字资产，丰富区块链技术和数字货币的应用场景，推动其服务于商业进步和社会发展。

3 、技术支持

3.1、区块链概述和机制

我们正在建立一个挂钩到其他区块链来进行跨代币/资产类别的交易。这个过程主要由以太币来支持。从任何单一链条的角度来看，我们正在建立一个可扩展的区块链，其合约状态由 COC 链本身的活动绑定。其他链条的活动可以通过类似与 BTC 中继的形式以跨链提交证明的形式进行链间连接，这个过程可以提交到以太坊处。COC 链验证了该活动所有参与者的行为（包括其他链条上的活动） 。换句话说，COC 代币的作用是提供计算和执行。代币本身作为其在该区块链上的活动的保证金，不正确的活动将导致代币/保证金在 COC 链上销毁。通过创建一个具有深度执行力的定制链，我们可以构建一个系统，在这个系统中，其共识规则对于高性能活动是最优的。该设计优化了快速执行和清算，但是结算速度会较慢。未来的迭代可能包括 COC 链的分片技术，但是对于初始迭代，我们将假设具备高吞吐的区块传播量。拥有 COC 代币，实际上是依照协商一致的规则，购买验证此区块链的权利。交易费用，包括（但不限于）用于支付，交换，清算和结算所的资金，将给予无故障的验证节点执行保证金抵押的合约状态。这些代币将根据从网络中导出的费用获取价值，也意味着承担向链上用户提供验证的义务和成本。这些代币必须具有价值以防止低成本攻击，并且对于推动网络的执行时非常必要的。

在我们的路线图上，我们可能允许将验证授权委托给第三方，而在需要重新授权之前，每一次可以减少有限的数量（该安全模型的完整机制尚未确定） 。因为这将被设计为一个高性能的系统，因此我们需要一条证明连接区块链。我们期望这个系统能够处理大量的交易，这样我们只要把最终的结果传输到以太坊就可以了。清算和结算都在 COC 区块链上发生。共识规则将通过股权证明网络执行。作为网络共识规则的一部分，我们要求所有 COC 验证节点也同时运行以太坊网络来并

行验证，从而使以太坊成为区块链间验证的首要保障。我们同时假设存在如以太坊/ ERC-20 来进行担保或者退款的机制，BLS 签名方案（或 Schnorr）将在不久的将来用于以太坊。对于加密数字货币，这些代币是非监管的，而是锁定在智能合约中（不像其他交换平台，比如 Ripple，需要可信的网关来代表底层）。它也不依赖于所谓的集中验证集合（例如 Ripple）。COC 区块链负责管理在以太坊上的执行顺序的匹配和管理执行。OMG 上活动确保验证节点的活动也可以通过本地以太坊智能合约在以太坊区块链执行。对于比特币和类比特币系统，我们允许通过闪电网络上的清算网络来进交易。区块链通过提交证明在该网络上执行活动。虽然不如以太坊网络那么强大，但它允许在无需全节点验证的情况下协调 OMG 链上的几近即时的动。为了安全性，我们期望在未来让不允许区块链重组的节点进行持重组的区块链上的简单的 SPV 验证不允许在此网络中执行。

3.2、COC 设计概要

COC 初始版本包含两类区块：（1）分布式控制链区块，该区块包含标准参数区块表头、数据块链格式定义、公共 AI 模型参数列表、AI 参数扩展数据块指示、用户 AI 模型参数列表；（2）数据链区块，该区块结构与以太坊类似，包含标准的数据区块头、交易列表、叔父列表。

COC 中的分布式控制链区块按照固定速率生成，自身行为独立，不依赖于其它数据链；而数据区块链则需要对最新生成的控制链区块进行解析，从而确认新的数据区块更新频率以及对应的参数设置。常规情况下，每个数据区块链参数在较长时间内处于稳定状态，除非 COC 区块参数的 AI 模型，判断现有的数据区块链需要及时优 MATRIX 直接定义了创世控制区块和第一个数据区块，然后按照定义的时间顺序，依次创造后续的控制区块与数据区块。

3.3、核心思想

最终状态要求是拥有法币价值的电子钱包平台去中心化机制的一个架构。电子钱包代币将能够在去中心化、公共的以太坊区块链上使用以太币（或者其它去中心化加密数字货币）作为交换媒介以达到最大效率。我们相信这将为去中心化加密数字货币赋予更多的价值和使用意义，因为它为许多电子钱包平台提供了用处。由于该网络的一个核心功能是实现电子钱包间的交易。COC 必须拥有一个区块链账本，以保持每个电子钱包服务（或任何用户/节点）的总体资金余额。这个账本必须能够跨多类资产/商品记录资金。但是，仅仅拿着一个账本对于交换来说是不够的。这种机制还必须允许这些资产/商品进行交易。为了进行交换，它需要在公开公共市场上的交易者间放置一个命令。这需要一个去中心化的交易委托账本和交易引擎。这个交易引擎内置于 COC 区块链中。当匹配的订单获得了大多数验证节点的确认，订单将被发布并进行匹配。该流程将作为每个区块的一部分来执行。这产生了一个单方拥有的非监管的去中心化交易，其中，此电子钱包平台可以在无需信任某一中心化实体的前提下，与其他电子钱包平台进行交易。然而，直接进行电子钱包代币交换并不可取的，因为这会很复杂。在没有单一偏好的情况下，我们有必要在流动市场使用加密数字货币。通过将以太坊与智能合约绑定（或将类比特币代币绑定清算中心），我们可以将以太币锁定到COC区块链的活动上，以便基于以太坊或其他加密货币的电子钱包创建一个流动市场（如果每一对都与 ETH 进行交叉，在低货币波动的情况下，差价将小得多）。对于需要非常小的差价的活动，可能会出现一些电子钱包代币将被用作交叉；然而，由于程序裁决相关的协调和信任优势，我们有必要使用去中心化代币，如果有必要，也可以使用其他电子钱包代币。但为了不影响短期的智能合约交易率浮动比率，我们主要使用 ETH（例如

HTLC 清算所，流动性供应和 COC 链执行）。通过允许加密数字货币支撑电子钱包平台，所有电子钱包间的交易活动都是公平的。
这意味着锁定的资金需要更大的流动性，而对于低价值的交易活动（例如大量的小额支付），COC 去中心化交易可能不太可取。两个不同电子钱包之间的每一笔付款不是必须使用去中心化交易来执行。我们可以设想，电子钱包将储备一些其他电子钱包的代币，用于流行方向的小额转帐。诸如闪电网络等架构允许在电子钱包记录余额以促进快速支付的前提下发生链下支付。我们允许跨比特币和以太坊付款，因为这些过程都可以轻松地移植到 COC 链上，对电子钱包余额进行记录。借助去中心化交易，加密数字货币（例如 ETH）匹配，交易委托账本和没有全面监管的清算所的信任，COC 区块链架构允许电子钱包间进行交换。

3.4、电子钱包

电子钱包代币将能够使用去中心化加密数字货币（如在以太坊区块链上使用以太币）作为交换媒介以达到最大效益，其终状态要求是拥有法币价值（以电子交易平台为基础）的去中心化机制的一个架构。它为电子钱包平台提供了用处，去中心化加密货币的使用意义和价值得以体现，也是该网络的核心功能所在。COC 拥有保持每个电子钱包服务（或任何用户/节点）的总体资金余额的一个区块链账本，它能够跨多类资产/商品记录资金。值得注意的是，仅仅拿着一个账本对于交换来说是不够的。这种机制还必须允许这些资产/商品进行交易。COC 区块链中的去中心化交易引擎和委托账本放置着交易者之间在公开市场上的命令，以便进行交换。电子钱包平台可以在无需信任某一中心化实体的前提下，与其他电子钱包平台进行交易。当匹配的订单获得了大多数验证节点的确认，订单将被发布并进行匹配。该流程将作为每个区块的一部分来执行。这产生了一个单方拥有的非监管的去中心

化交易，在没有单一偏好的情况下，我们有必要在流动市场使用加密数字货币。通过将以太坊与智能合约绑定（或将类比特币代币绑定清算中心），我们可以将以太币锁定到COC区块链的活动上，以便基于以太坊或其他加密货币的电子钱包创建一个流动市场（如果每一对都与 ETH 进行交叉，在低货币波动的情况下，差价将小得多）。对于需要非常小的差价的活动，可能会出现一些电子钱包代币将被用作交叉；然而，在复杂情况下直接进行电子钱包代币交换并不可取。我们有必要使用去中心化代币来程序裁决相关的协调和信任优势，使用其他电子钱包代币也无妨。为了稳定智能合约交易率浮动比率，我们主要使用 COC 链执行 （例如 HTLC 清算所，流动性供应）。通过允许加密数字货币支撑电子钱包平台，所有电子钱包间的交易活动都是公平的。

COC 去中心化交易对于大量的小额支付（例如低价值的交易活动）可能不太可取，这代表着锁定资金需要更大的流动性。两个不同电子钱包之间的交易可以不使用去中心化交易来执行。在用于小额转帐方面，电子钱包也可以通过储备一些其他电子钱包的代币。诸如闪电网络等架构推动了快速支付，且允许在电子钱包记录余额以发生链下支付。我们 COC 链可以快速移植跨比特币和以太坊付款的记录和过程，对电子钱包余额进行全方位跟踪记录。COC 区块链架构借助去中心化交易，加密数字货币（例如 ETH）匹配，交易委托账本和没有全面监管的清算所的信任，使得电子钱包间的交换成为现实。

3.5、比特币清算中心

另一方面，对于比特币和类比特币系统而言，我们可以创建一种系统。在这个系统中，我们可以将资产从外部与清算中心系统绑定在一起，由此实现 BTC 和其它类似的区块链进行交易。本质上，这种结构是将清算中心作为一个预言机运行，其中的活动都绑定在 COC 链上

并由 COC 链负责执行，以实现与类比特币区块链的去中心化交易。上述流程参照了 Tier Nolan 在基于外部交易执行工具进行快速去中心化交易的研究。清算中心用于确保支付发生在比特币区块链上。我们使用清算中心而不是

SPV 证明，是为了防止由比特币矿工产生的不符合共识但 SPV 证明有效的区块来攻击外部系统的对抗性激励（对自己的链条进行重组攻击的成本是昂贵的，但外部攻击比较便宜）。对于类比特币系统，该系统要么需要进行可延展性修复（例如隔离见证），要么是仅在透明地址上可用的 P2SH / BIP-66 / CLTV/ CSV 组合。清算中心是必需的。因为目前不可能在比特币上执行复杂的合约状态。这些清算中心负责通过生成原像和哈希值来披露比特币（或类比特币）的链上活动。这些哈希值将被提交至清算中心所负责的活动，并进行绑定。如果他们释放不正确的原像，或拒绝透露 OMG 链的原像，任何人都可以提供渎职证据，此时，清算中心将会被削减。需要注意的是，这要求清算中心既要有比特币资金储备，也要有可用于在 COC 链上进行绑定的资金。至于保证金，其数额只能存留到资金可以在比特币上进行清算和结算，所以理想情况下不需要极高数额的资金。清算中心运营着一个闪电通道，但他们不仅在通道中拥有自己的资金，还有预期在 COC 链上流动的资金的数倍金额的 ETH 储备（例如，3 倍预期流动资金以应对汇率浮动）。

图 1：Alice 和 Bob 有一个闪电网络通道与 Carol，即区块链上的清算中心相连。支付原像 R 由 Carol 生成，并且原像的释放由 OmiseGO 链上的绑定承诺来执行。假设 Alice 希望出售比特币，而 Bob 希望购买比特币，他们都有向 Carol 清算中心开放的通道。这三者都在 COC 链

上，并指定 Carol 为可接受的清算中介。请注意，如果双方均指定某一清算中心为可接受，则可能会在多个清算中心之间进行转账，而且交易只能在交易参与者指定可接受的清算中心的交集中进行。Carol 这一清算中心根据 COC 链以及智能合约中的共识规则将以太坊上的资金锁定在智能合约中。Carol 提供了一个已签名的证明，并对 H（它是由 Carol 的原像 R 生成的，这时只有 Carol 知道）进行哈希。她提供哈希 H，在她负责的 BTC 中具有相应的价值，并签名。这可以用作 COC 链上的证明（如果 Carol 出现故障，则可以使用以太坊智能合约）。当 Alice 想要出售比特币时，她将根据 Carol 提供的 H 值创建一个 HTLC 支付内容。同样地，当 Bob 想要接收比特币时，Carol 根据自己提供给 Bob 的 H 值发布 HTLC 内容。这些 H 值在 COC 链上与特定人物相关联，那么此时，资金就可以进行去中心化交易。当交易在 COC 去中心化交易中心执行时，例如 Alice 要卖出 BTC 兑换 ETH，而 Bob 用 ETH 购买 BTC，该交易现在在 COC 链上进行清算。每个人现在都有履行交易的责任和义务。Carol 负责释放与 Alice 和 Bob 在 COC 链上所执行的交易相关的 H 的原像 R。Bob 可以使用这些信息来提取比特币链上的资金，而 Carol 现在有权从爱丽丝处提取资金。如果 Carol 拒绝在相关时段内将原像 R 释放到 COC 链上，她的资金将被削减，她的 ETH 将转移给 Alice 和/或 Bob。（以惩罚的方式来减轻汇率波动，并防止 Carol 作恶）。如果 Carol 不正确地释放了她不应该释放的 R 值，那么任何一方都可以将证明提交到区块链上，此时 Carol 将被处以罚款，并将交易清算合约锁定的与 H 值相关的资金给予证明提交方。清算中心可能不需要直接与参与者（Alice，Bob）相连，他们可以通过路由网络支付，这样的话，他们可以实现资本效率最大化。清算中心有权为各种使用自身来进行的活动收取费用。我们需要去相信清算中心能够执行支付，但我们可以对他们的活动信任最小化（因为他们的活动都绑定在 COC 链上）。值得注意的是，这种结构对于通过外部化接合的

HTLC 快速超时也十分有用，也是实现以分钟测量的极速超时来构造支付的方式。它不需要清算中心锁定比特币，只需要绑定由清算中心所执行的信息的释放过程。这个结构的进一步解释将在另一份单独的文件中进行阐释。请注意，这仅仅是可能的。因为 COC 链很大程度上不提倡重组。最终的结果就是我们能够在比特币之外进行去中心化交易。我们相信这是一个新颖的结构，因为比特币网络上的参与者的活动是由一个外部去中心化的交易中心经由以经济激励方式来驱动的建立在比特币上的清算中心来执行的，并且通过外部条件强制释放原像可以让比特币用于协议代币区块链。

3.5、 智能合约实时数据更新

将最近交易执行的 VWAP 定期在 COC 区块链上进行计算和公布作为共识规则。它将允许外部合约使用交易执行价格和数额的 Merkle 树 SPV 证明，甚至可以在智能合约中创造更大的可行性。

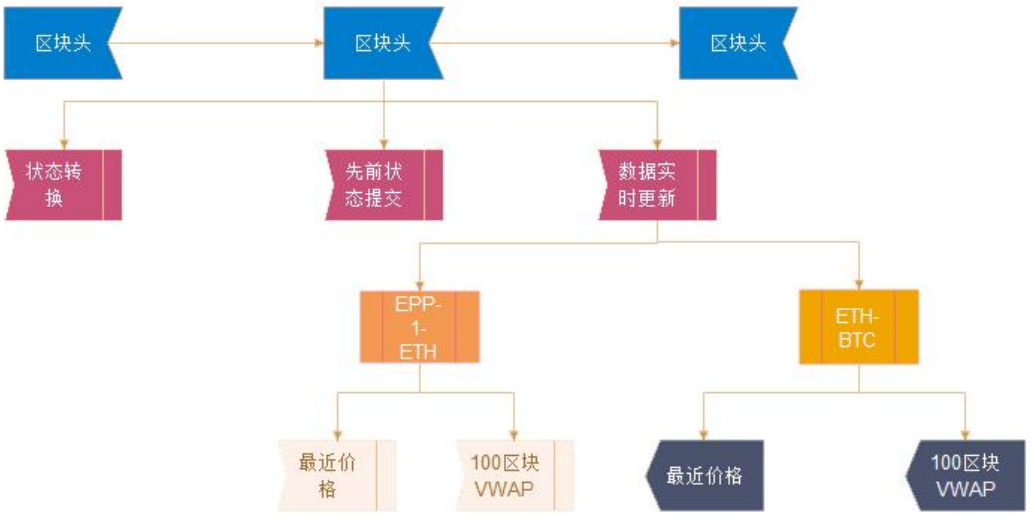


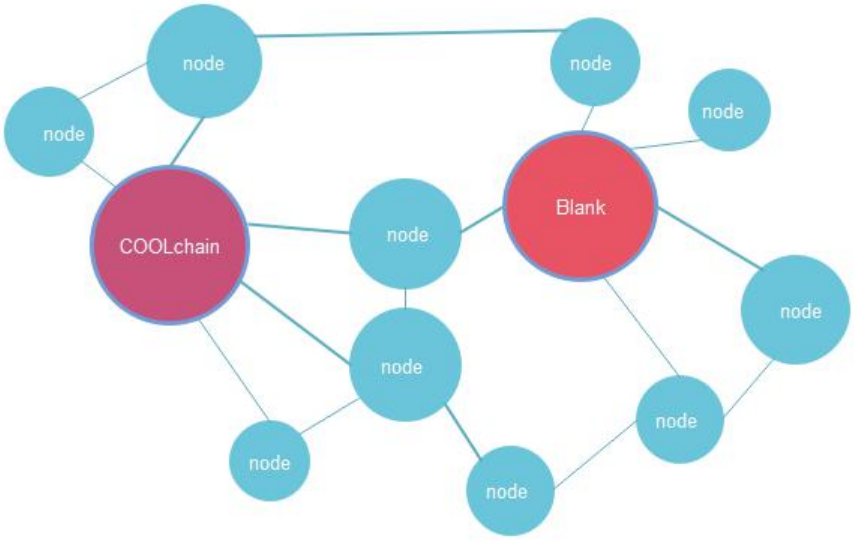
图 2：实时数据的定期提交将在 COC 区块链中记录。人们可以通过区块链头中的 merkle 根提交信息来进行外部验证。交易数据来源包

含最近交易价格，交易量和各种 VWAP 条件（各种时间和/或区块数）等常用交易对。任何交易所的主要功能都不仅是管理交易委托账本和执行，而且还有一个供第三方系统使用的数据供应。它允许第三方系统使用这些信息，并让参与者在一个地点上净化活动。由于汇率/定价机制的基础对于所有（智能）合约来说都是必要的，因此访问该系统可以让这些外部合约的参与者使用交易中心作为实时数据更新的途径，从而在执行中有更大的保证和透明度。合约参与者将被允许基于行为认知创建合约，并获得去中心化合约服务。如果参与者使用 COC 链上的价格预言机供应作为智能合约定价的基础，他们可以通过在 COC 链上下订单获得更好的执行保证。这将为 COC 链创造更卓著的网络效应以彰显其对智能合约更好的应用。

4、生态体系

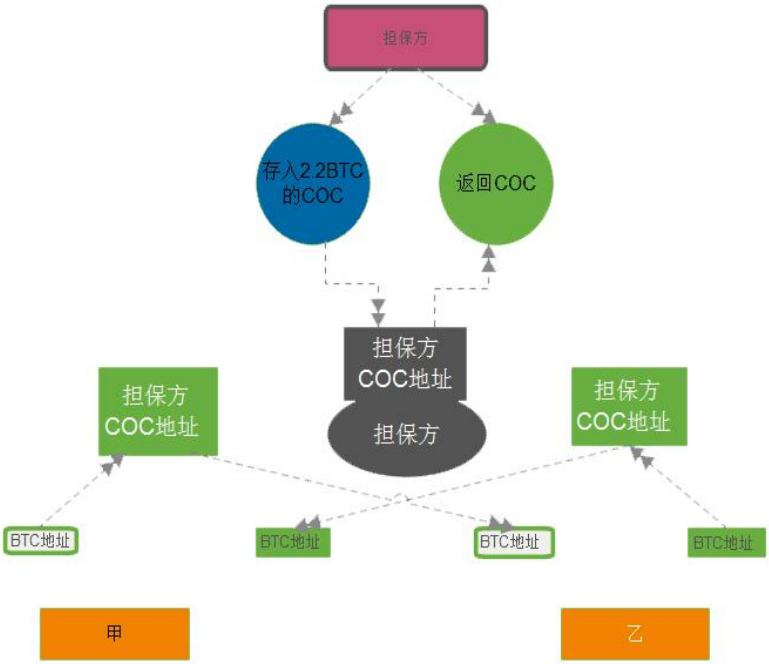
4.1、Aanl Cosis 环状拓扑中继技术

COC 的 Aanl Cosis 技术将多条链连接到一个 Hub 上，让数字资产终端轻松实现一键跨链和转换。环状的优势在于拓扑结构对资源的消耗比星型、树形要小很多。节点少、距离近可能不明显，但是距离远、节点多，环网的这一优势会很明显。大体的设计结构如图所示：



4.2、CO-Mbicads 兑换网络

CO-Mbicads 兑换网络是基于 COC 区块链平台通过定制智能合约和 CO-Mbicads 跨链网关技术，实现无风险数字货币兑换。COC 平台或持有 COC 代币的用户都可以创建兑换智能合约，通过创建合约提供担保服务，以合约机制来规避各方违约，避免中心化托管机构的仲裁偏颇，让参与三方都没有损失风险。合约创建者促成兑换交易后，获取相应比例的担保回报。整体流程示意如下：



4.3、OnePay 闪电支付网络

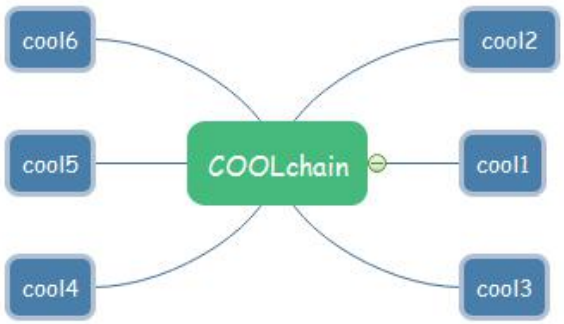
区块链的去中心化会带来支付效率不高的问题。我们通过以下技术实现 COC 闪电支付网络（本质是基于现有区块链网络构建 COC 的 VPN 子网），转账秒级确认，保证实时刷卡消费不受区块链的影响，技术设计重点如下：

（1）定制移动客户端，COC 用户的区块链转账做 SHA512-ZERO 加密标志；

（2）开发企业级区块链节点，随时检测 COC 用户的区块链活动，进行合法性校验、流量分析等。企业级节点 7X24 小时不间断检测，提供给服务器用户的余额变化分析，并上报给 COC 服务端

（3）COC 服务端接收企业级区块链节点分析结果，用户发起刷卡请求时，已经能实时明确用户是否已经真实发起区块链转账请求，防止恶意双花。

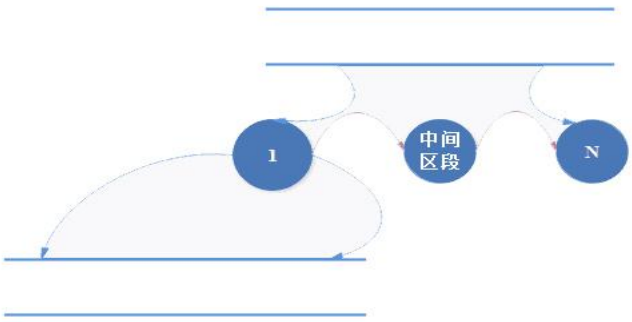
图例（蓝色的节点是我们在全球部署的嗅探节点）：



4.4、COC 的分布式控制链区块内部结构

COC 的控制区块单个区块链的结构提由两部分组成：

1. 控制链区块头；
2. 控制链参数与模型列表。



其中：

COC 控制区块，将尽可能的容纳多条数据链的参数配置。当某个区块存在容量

问题时，将采用 Round Robin 算法，保证每个数据链参数配置的

公平性。

目前的参数配置方式如下：

DataChainParameter_list = [

DataChainParameter 1,

DataChainParameter 2,

...

]

而对应的每条数据链的参数配置，则采用如下方式定义：

DataChainParameter=[

SystemAIParameterList

SystemTransModelList

UserAIParameterList

UserTransModelList

]

另外，考虑减少数据链的参数解析运算量，促进新加入用户快速进入挖矿进程，COC 将周期性的提供每一条数据链的完整参数，并设定对应的标志。

5、COC 加密与效率

区块链的价值锚点在于链条自身的消耗与产出。当区块链选择 PoW 作为共识机制时，每一次区块的生成消耗的算力都将成为其价值的基石。另外，在 COC 上，每个节点都具备解决现实环境问题的能力，并能对外提供各种 AI 服务。如果 COC 上的节点能够参与实际问题的解算，整个区块链条就具备了现实的产出价值。因此，为保证区块链自身价值最大化，COC 控制链与每一条数据链将默认选择基于 PoW 的共识机制。 但由于 PoW 具备交易速度较慢等显性缺陷，因此在 COC 中，除初始的数据链与控制链强制采用 PoW 外，后续的数据

链，其共识机制将被设计成模块化的，可以通过控制链参数进行配置，能够动态适用公链和私链的不同应用场景。 目前，COC 对后续数据链共识机制，支持 PoW、POS、DPOS、BFT 等。COC 链的 AI 优化系统将针对数据链本身的应用场景和交易情况，选择合适的共识机制，确保各个分布式节点通过算法取得数据的一致性。

COC 链的安全加密算法，是基于采用传统的比特币加密方式上的改进。COC 链涉及的安全加密算法及相关定义如下：

对称加密：对称加密是最快速、最简单的一种加密方式，加密（encryption）与解密（decryption）用的是同样的密钥（secret key）。对称加密通常使用的是相对较小的密钥，一般小于 256 bit。密钥的大小既要照顾到安全性，也要照顾到效率，是一个 trade-off。非对称加密：非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公钥（public key）和私钥（private key）。私钥只能由一方安全保管，不能外泄，而公钥则可以发给任何请求它的人。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。

私钥（private key）：非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

公钥（public key）：可公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括： secp256r1（国际通用标准）、 secp256k1（比特币标准）和 SM2（中国国标）。MATRIX 控制链与初始数据链选择 secp256r1 作为密钥方案。

Hash 算法：通常 Hash 算法是指安全散列算法 SHA（Secure Hash Algorithm），该算法是美国国家安全局 （NSA） 设计，美国

国家标准与技术研究院（NIST） 发布的一系列密码散列函数，包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 等变体。目前比特币采用 SHA-256 算法。MATRIX 除 PoW 外，其余 Hash 算法均指 SHA-256。

COC 链的随机数产生包含两种方式：

（1） 基于共识的随机数

（2） 二阶段产生的随机数

其中，基于共识的随机数将当前区块的 Nonce 作为种子之一，与未来某个区块的 Nonce 共同组成随机数种子（Random Seed），通过随机数发生器，获得真正的随机数。

二阶段随机数，则将随机数的产生分为两个阶段，核心是避免矿工由于自身利益，隐藏当前区块的 Nonce 作为随机数种子。因此，第一阶段先随机抽取一个在线第三方，第三方可以与当前区块的 Hash 有关联，并确定未来某个区块的 Nonce 作为随机种子之一。这个第三方也可以直接选择可信第三方。第三方生成一对公钥与私钥，并公布随机种子的区块公布公钥，并在后续的一个区块公布私钥。私钥与随机种子的区块 Nonce 共同组成了随机数发生器的种子，并由此产生基于全网共识的随机数。

6、商业模式

6.1、 数字资产消费的 Gas

在 COC 上，任意数字资产的创建和转账需要消费掉 COC 代币作为 Gas 矿工工费。

6.2、 算力费用

在 COC 上，如果项目方需要快速的生成一条侧链，他们需要往配置合约资产的合约里存入一定的 COC 代币，以吸引矿工为其提供算

力。同样，如果项目方需要用户提供去中心化的算力、数据支持和挖矿服务，项目方也需要预先支付一定的 COC 代币。

6.3、 兑换费用

用户要完成不同数字资产之间的兑换功能，需要支付一定的兑换费用以获得去中心化的兑换服务。

6.4、手续费用途

用户通过 COC 绑定在商家消费，VISA 或 Master 等服务商会向商家收取相应的交易手续费（这笔费用会受到消费地区、消费类型、消费金额等因素的影响而不同），然后再分配一定比例给 COC 作为分润收入，我们预估平均交易手续费分成后收益为 1%左右（实际情况可能会有变化）。假设，COC 用户 100 万，平均每个用户每月消费 100 美元，一年交易总金额 12 亿美元，手续费分润收入 1200 万美元。 用户通过COC绑定在商家消费，VISA 或 Master 等服务商会向商家收取相应的交易手续费（这笔费用会受到消费地区、消费类型、消费金额等因素的影响而不同），然后再分配一定比例给 COC 作为分润收入，我们预估平均交易手续费分成后收益为 1%左右（实际情况可能会有变化）。假设，COC 用户 100 万，平均每个用户每月消费 100 美元，一年交易总金额 12 亿美元，手续费分润收入 1200 万美元。 COC 团队会每月拿出上述交易分润的不少于 35%部分用于购买 COC 代币，回购代币存入发展基金地址，用于后续项目开发和产品生态建设。

6.5、手续费抵扣

当用户通过 COC 进行数字货币兑换交易时，可以根据 COC 当前市场价值，使用其进行手续费的抵扣。后期，COC 团队将通过和交易

所合作，尽可能让 COC 可以部分抵扣数字货币交易手续费。

6.6、用户激励

持有 COC 代币的用户，都可以在 COC 的货币兑换服务里，担任合约创建者的角色，通过促成兑换交易来获取手续费收入（具体机制参见 NO-LOCALCOIN 兑换网络描述）。 通过 COC 钱包绑定的用户，每次消费都将获得本次交易手续费 10%的返现，COC 自动以 COC 代币的形式发放到用户钱包里。这样不仅让用户获得了返现折扣，也进一步拓展了 COC 代币的用户群

7、项目计划

COC 基金会发行基于 ERC-20 标准的 COC，COC 作为网络中的核心要素，将在点对点加密消息，， 去中心化交易，COC 商家支付等场景中有大量的应用。

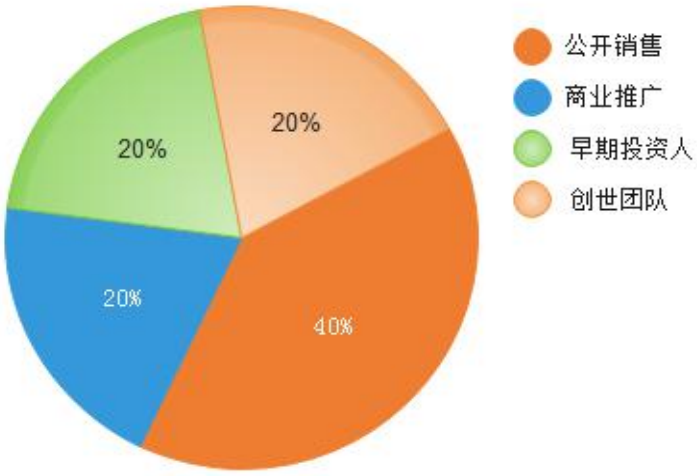
COC 总量为 3000 万，按如下方式分配:

创始团队：持有 600 万枚 COC，占总量的 20%；

早期投资人：持有 600 万枚 COC，占总量的 20%；

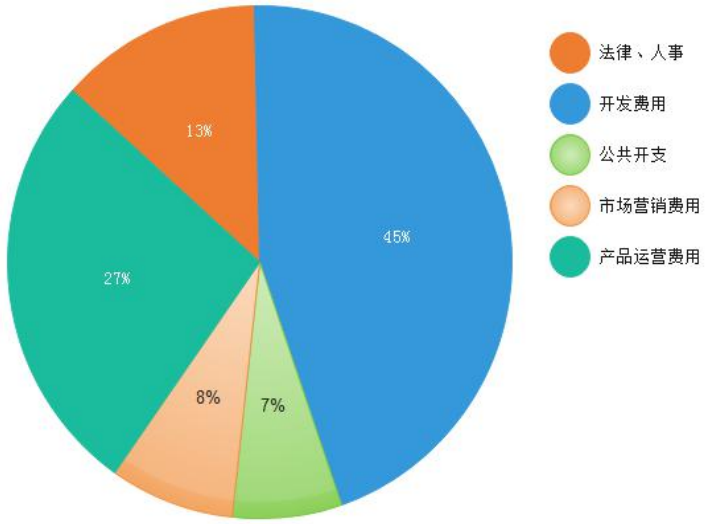
商业推广：持有 600 万枚 COC，占总量的 20%；

公开销售：1200 万枚 COC，占总量的 40%；



7.1、分配计划

众筹资金的具体分途分配比例见下图。基金会将主要持有众筹所得 COC 和比特币以及以太坊， 资金将按五年规划使用。



7.2、团队拥有的代币说明

1） 团队部分合计 20% COC 将分 3 年逐步解冻，这是为了保障团队在上线交易后，能够持续执行开发。

· 上线交易半年后，释放团队持有量的 5%；

· 一年后，释放团队持有量的 5%；

· 之后的 2 年，每年释放 5%；

2）公募部分在完成上线交易后，立即发放；

3）用于商业推广的 20%，将主要用于促进 COC 社区的应用和成长；

4）将成立 COC 漏洞奖励网站，奖励发现安全漏洞的个人和团体。并和安全服务提供商进行长期合作，保证 COC 的安全性。

7.3、 产品和运营团队

好的产品是靠运营出来的，COC 团队将划分出 20%的资金用来建立专业的产品、运营和客服团队。及时处理客户的问题、积极响应社区的需求、并快速的添加的产品迭代计划中去。从而实践区块链的精髓：拥有于社群，管理于社群，服务于社群 。

7.4、 市场和营销费用

在互联网时代，一个再好的应用也离不开市场的推广、合理的营销和商务合作。因此 COC 团队安排了近 20%资金用于市场和营销工作，致力于持续推动 COC 遍布全国，并走向全世界。 在 COC 社交网络中，我们将支持包括中文简体、中文繁体、等多种语言。后续还将持续不断的添加更多的语言。我们坚信在合理的市场和营销费用安排下，COC 可以在全世界得到广泛的使用进而我们还将积极参加各种区块链活动，在全球推广和营销我们的 COC 产品。帮助大家更好地理解 COC 产品。

7．5、法律、咨询、财务和人事行政费用

这些费用将会为我们整个公司提供有力的支持，尤其是对于我们这样一款国际化产品，这些费用将促使我们的产品走得更稳更快，为更多的人服务。

8、团队介绍

8.1 主创团队

刘朗 CEO：
经济学家，有着多年的金融贸易从业经验，创办了多家公司，在欧洲具有广泛的影响力。
顾章平/COO：

毕业于新西伯利亚国立师范大学，曾任新西伯利亚 Academ Media 公司主要项目经理和 Movements 商务开发经理，带领过多国团队和谈判。

刘成希/CTO：

软件工程师，曾在北京的大型软件和游戏开发公司有 3 年以上的经验。擅长使用 Solidity, Python, C/C++ and C#语言进行编程。

程靖宇：

区块链技术开发者，擅长语言和框架搭建。对各类共识算法 PoW, PoS, DPoS, PBFT, Paxos, Raft等非常熟悉，并参与过目前开源项目。

8.2 顾问团队

Elena bogdanova：（律师） - 俄罗斯联邦高级法律顾问，GROHE 公司俄罗斯联邦，中亚和高加索地区合规主管

Dmitri borovalkin：（协议开发者） - 开发服务器解决方案（后端），智能合约，参与工作项目,Overkings（MMO RPG 浏览器）

9、发展规划

10、风险提示

请务必认真阅读和理解本白皮书中规定的所有权利和限制。除非您接

受本白皮书所列条款，否则您无权下载、阅读或使用本白皮书及其相关资料。您一旦购买、复制、下载或以其它方式使用本白皮书产品，将视为对本声明的接受，即表示您同意接受本声明各项陈述。

11、免责声明

1.本文件不是招募书也不构成任何交易合约，不应视为在任何具有司法管辖权的地区构成证券邀约或招揽购买证券邀约。

2.本文件中提供的信息不是投资建议，不应作为任何投资决策的基础。

3.数字代币可能波动性较大，兑换或持有数字代币属于高风险行为，参与者必须具有足够的判断力、有足够的风险承受力或其他与承受高风险行为有关的必要素质；若兑换或持有数字代币，则视为已全部知晓兑换或持有数字代币带来的全部风险。

4.本白皮书仅为传递信息之用途，不构成任何发行、诱导购买BSTN、投资建议、教唆投资或其他买卖邀约及任何证券行为。没有在此显示的相关信息或分析，有意构成任何投资决策或具体的购买推荐。

5.COC 在此清楚的表述，并不对 （1）依靠本文中包含的信息（2）任何信息错误、疏漏、或不准确 （3）由此导致的后果，造成的直接或间接损失负责。一个完全的交换方法。

12、参考文献

[1] Turing, A. M. Computing Machinery and Intelligence. Mind 49: 433-460, 1950.

[2] Giardina, Carolyn. "*How Artifcial Intelligence Will Make Digital Humans Hollywood's New Stars.*" Hollywood Reporter, 25 August 2017.

[3] Lanier, Jaron. Who Owns The Future?. Simon and Schuster, p. 245, 2014.

[4] Rosenthal, Edward H. The Right of Publicity. American Bar Association. Intellectual Property Literature, p. 1, August 2014.

[5] Jain, Nikhil. "PAI." ObEN Inc, 2017, https://jain.ai/.

[6] Woo, Willy. "*Using Google Trends to Estimate Bitcoin's User Growth.* " Coindesk,12March2014,https://www.coindesk.com/using-google-trends-estimate-bitcoins-user-growth/

[7] Southurst, Jon. " *It's still too hard to get your frst Bitcoin.TheDailyDot,24April2015,https://www.dailydot.com/via/bitcoin-cryptocurrency-adoption-hard/.*

[8] Canada. Kik Interactive Inc. "Kin: a decentralized ecosystem of digital services for daily life." Kik Interactive Inc, Whitepaper, p. 11, May 2017, https://kin.kik.com/#Papers.

[9] Saunders, Philip, and Yonatan Ben Shimon. Israel.

“ Matchpool. ” Matchpool, Whitepaper, p. 2, 14 Jan 2017, https://matchpool.co/.

[10] Merkle, Ralph C. Protocols for public key cryptosystems. 1980 Symposium on Security and Privacy, April 14, 1980, Oakland, CA, IEEE Computer Society, p. 122, April 1980.