



EOS TRANSPORT

一种终端数字资产交换撮合引擎

Version:3.0

Zohar |
2018年10月1日

目录

1.摘要.....	3
2.背景.....	3
2.1 中心化撮合交易现状.....	3
2.2 去中心化数字资产交换的现状.....	4
3. EOS-Transport 终端撮合引擎.....	5
3.1 智能合约管理资产.....	5
3.2 链下终端撮合.....	6
3.3 消息格式.....	7
3.3.1 充值消息.....	7
3.3.2 创建订单消息.....	8
3.3.3 取消订单消息.....	9
3.4 订单撮合.....	10
3.4.1 订单撮合原则.....	10
3.4.2 订单撮合算法.....	11
3.5 EOS-Transport 网络.....	13
4. Token 交换 EOS-TRANSPORT 网络撮合效率提升的潜在方式.....	14
4.1 状态通道.....	14
4.2 楔入式侧链技术.....	15
4.3 分片技术的引入.....	15
4.4 多终端（钱包、Dapp）内挂单撮合引擎.....	16
5. EOS-TRANSPORT 网络规则-社区经济生态.....	16
5.1 Token 添加规则.....	17
5.2 超级节点运行规则.....	17
5.3 其他可能收入.....	17
6. 发展路线图.....	18
7. Token 发行计划.....	18
7.1 EOS-TRANSPORT 网络 Token 功能:	19
7.2 私募细则.....	19
7.3 募集资金用途.....	20
8. 风险提示与免责声明.....	20
9. References.....	25

1. 摘要

EOS-Transport (EOS-T)——一种终端数字资产交换撮合引擎（简称终端撮合引擎）。以构建基础数字资产交换高速撮合引擎为目的，引入智能合约控制的Token 经济模型，同时通过半中心化的撮合模式满足各类 DAPP 等终端间的数字资产高速交换需求，从而实现一个无需信任的数字资产交换撮合引擎。随着区块链技术的发展和公有链平台的增多，对跨链之间的数字资产交换的需求会越来越多，后期扩展为通过多链技术或跨链技术实现链与链之间的数字资产的安全交换。EOS-Transport 在满足当下 DAPP 间的撮合的基础上，与时俱进，不断的融入新的技术和思想。同时通过模块化的组合方式，给整个系统提供了极大的可扩展性和兼容性，初期基于 EOS 实现，未来以太坊以及 BTC 等公链的数字资产交换都将被很好的支持。

2. 背景

2.1 中心化撮合交易现状

随着区块链行业的发展，数字资产的种类越来越多，对数字资产之间的直接交换需求越来越广泛。当前大部分数字资产持有者通过中心化交易所的方式进行交换，虽然当下行业内存在一些去中心化的数字资产交换方式，但是在用户体验和交换效率还无法达到中心化交易所的标准，因此目前中心化交易所在区块链行业里发挥了非常重要的作用。但是，它也存在一些问题，比如遭受黑客攻击、数字资产被盗、交易所内部暗箱操作等问题。同时在区块链的世界里，中心化交易所却处在一个非常重要的地位，对整个行业来说，不得不承认有一些讽刺的味道。因此，提出一种无需信任即去中心化的方式进行数字资产交换的 EOS-TRANSPORT 网络和方法是非常有必要的。

2.2 去中心化数字资产交换的现状

当下区块链行业里最中心化的地方是各个交易所，针对交易所存在的问题，信仰去中心化的极客们都在努力的实现以去中心化的方式进行数字资产交换，提出多种去中心化的解决方案，并一个接一个的进行尝试，不断地进行技术迭代和升级。

0xProject，基于以太坊的去中心化 Token 交换协议。0xProject 已经构建完成了交换协议的基础功能，用去中心化的方式完成了 Token 交换的基本流程操作；由于它是一个基础服务，可以很好的提供一种去中心化交易服务以便和其他复杂应用进行有效的组合，扮演一个基础设施的角色。

Kyber Network，一个去信息去中心化的高流动性交易所。Kyber Network 构建了一个高流动性的去中心交易所，通过引入储备库角色提升效率达成即时交易，并实现与现有智能合约的兼容。

2.3 EOS 目前存在的问题和机遇

EOS 作为区块链时代具有代表性的公有链技术平台，随着主网的上线，社区开发者也已在其链上开发了上百款 DApp。随着 DApp 数量的增加和社区的壮大，EOS 存在的一些问题也逐渐暴露出来，比如 CPU 资源面临瓶颈、跨链间的通信问题等等，其中最主要的就是 CPU 的资源问题，随着所有区块链项目都面临着 DApp 运营的高成本。尽管 EOS 通过 BFT-DPOS 实现了高 TPS，但对于超级节点而言，资源问题在可预见的将来仍然是稀缺的。例如 RAM，尽管根据摩尔定律，随着时间的推移区块链应该获得更多的资源，但由于 DApp 需求的快速增长，资源短缺在短期内仍旧是一个问题。在市场投机行为背景下，开发者付出的成本将会显著上升，这将成为 EOS 发展的一种制约。针对 EOS 当前存在的问题，EOS 接下来也有一些方面的考虑，例如：EOSForce 多链架构技术规划

多链体系结构确实为可扩展性和大多数现有区块链难以处理的资源问题提供了有意义的解决方案。有了它，开发人员可以创建自己的链来支持他们的 Dapp，

避免单链模型中存在的资源稀缺和网络拥塞问题。

这预示着未来每个应用程序都有自己的独立区块链，并通过链间通信工具来实现跨链通信。支持多链是 EOSForce 的主要发展方向。通过多链架构，可以在保证当前区块链安全性的同时为 DApp 开发人员提供丰富的功能。另一方面，交叉链可以允许社区启动不同的公有链或私有链，以获得 DApps 的最佳运行环境

随着区块链技术不断更新和迭代，数字资产交换撮合引擎也会跟进。尤其是在 EOS 的 CPU 资源、跨链之间的通讯技术等提高区块链信息计算之后，同一链内之间的数字资产交换效率也会得到相应的提高，而不同链之间的数字资产交换还需要借助其它技术（如跨链技术）来实现，随着技术和行业的不断的发展，相信很快就许多方案最终都会被提出。

3. EOS-Transport 终端撮合引擎

3.1 智能合约管理资产

EOS 智能合约中执行的交易是对外公开的，只有在开通 EOS 帐户时需要提交一定的账户费用，用户间的交易是免手续费的，并且所有的 DApp 都可以接入其中。凡是构建在这套 EOS-TRANSPORT 网络上的 DApps 都可以访问流动的公共池或者创建他们自己的流动池，并且根据数额收取手续费。这套 EOS-TRANSPORT 网络是开放的：它不会将成本加在用户身上，也不会将其他价值从一组用户转移到另一组用户。去中心化的管理是基于容器的持续集成管理，并且支持安全地更新升级，不会影响到 DApps 和用户。终端撮合引擎通过智能合约来存储和管理用户的资产，在未经用户的同意下，没有权威机构或者中心化机构可以操作资产，从而保障用户资产的安全。

3.2 链下终端撮合

终端撮合引擎的规则是通过智能合约管理用户的资产，包括充值、提现等等。虽然目前通过智能合约在链上完成交易，但由于当前公有链平台（包括比特币、EOS、以太坊等）的吞吐量还无法达到中心化交易所的要求，因此需要其它方式来提高资产交换和撮合的效率。终端撮合引擎通过类似链中继的方式将资产撮合放到了链下进行处理，从而提高交换效率。以下是终端撮合引擎交易处理模拟展示：

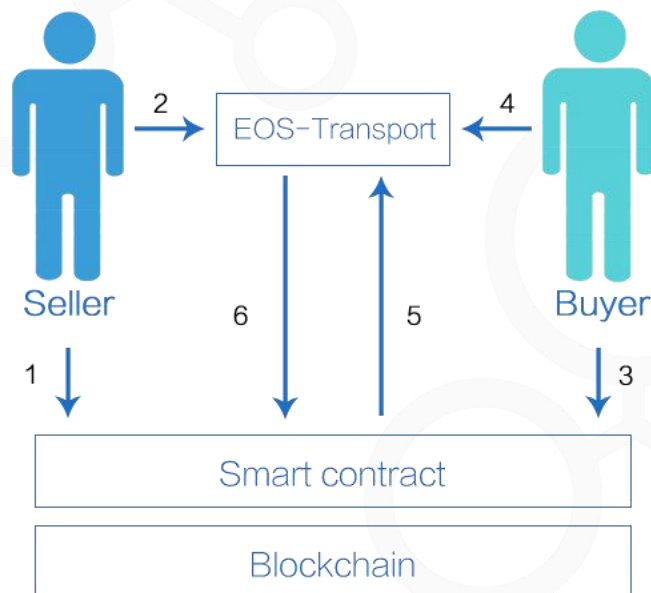


图 1 终端撮合引擎处理模拟展示

终端撮合引擎处理顺序如下：

1. 用户 Seller 将需要交换出去的资产充值到智能合约中，除了用户 Seller 以外，其它用户无法操作充值到智能合约中的资产；
2. 用户 Seller 将资产成功充值到智能合约之后，可以发送消息 MakeOrder 到终端撮合引擎的网络中，消息的内容包括换出和换入的资产标识和数量等，同时还需要包含消息发送者的签名；

3. 用户 Buyer 的操作跟步骤 1 类似, 将 Buyer 需要换出的资产充值到智能合约中;

4. 用户 Buyer 发送 MakeOrder 消息;

5. 终端撮合引擎获取用户的操作事件, 包括充值、提现等;

6. EOS-Transport 将最终的交换结果写入到智能合约中, 同时在用户在智能合约中最终提取资产时, EOS-TRANSPORT 网络可以发送确认消息, 以防止恶意用户的非法操作。

3.3 消息格式

EOS-Transport 与主链之间通过消息进行通信, 同时用户与 EOS-Transport 之间也是通过消息机制进行通信, 每个消息通过 keccak 产生 32 字节的散列值, 消息发送者使用私钥对该散列值进行 ECDSA 签名, 并同消息一起发送给接收者。

3.3.1 充值消息

充值消息是用户将需要交换的数字资产充值到智能合约, 充值成功之后才可以创建订单, 充值消息包括以下内容:

表 1 充值消息内容

名称	类型	说明
version	uint16	EOS-TRANSPORT 网络版本号
to	name	资产的接收者, 即 EOS 帐户
token	symbol_code	资产标识
value	asset	资产充值的金额
sign	bytes32	通过私钥签名生成的参数

充值消息中的参数 Token 代表了资产的标识，针对不同的区块链平台 Token 的类型可能会不一样。在 EOS 上，Token 的类型需要 Token 创建者的帐户名和 Token 名称共同确定，在以太坊等其它平台上可能会有所不同，但不会影响 EOS-TRANSPORT 网络的设计。

3.3.2 创建订单消息

用户将资产成功充值到管理资产的智能合约之后，便可以创建订单以交换资产，创建订单的消息内容如下：

表 2 创建订单的消息格式

名称	类型	说明
version	uint16	EOS-TRANSPORT 网络版本号
orderId	uint256	订单号，以区分不同的订单
tokenA	name	用户需要出售的资产 A 标识
amountA	asset	用户需要出售的资产 A 总量
tokenB	name	用户需要购买的资产 B 标识
amountB	asset	用户需要购买的资产 B 总量
expiration	int	该订单的过期时间，单位为秒
fee	asset	订单手续费
account	name	订单创建者
nonce	uint256	交易计数，表示到目前为止发送的消息总量，包括创建创建和取消订单

sign	bytes32	通过私钥签名生成的参数
------	---------	-------------

创建订单消息里包含两个资产的标识 tokenA 和 tokenB, 其中 tokenA 是需要出售的资产, tokenB 是将要购买的资产。同时, 用户可用的 tokenA 总量必须大于等于 amountA, 否则该消息无效。expiration 是订单的过期时间 (时间为秒), 通过设置过期时间, 防止订单未成交造成订单堆积。

amountA、amountB 分别表示出售和购买的资产总量。如果将该订单视为了一个买单, 那么购买 tokenB 的价格可以通过公式 1 获得:

$$\text{TokenB price} = \frac{\text{amountB}}{\text{amountA}} \text{ tokenB/tokenA} \quad (1)$$

同时, 该订单也可以视作一个卖单, 以 tokenB 为标的卖出资产 tokenA, 相应的卖出价格由公式 2 获得:

$$\text{TokenA price} = \frac{\text{amountA}}{\text{amountB}} \text{ tokenA/tokenB} \quad (2)$$

一般情况下, EOS-TRANSPORT 网络只需按照一种标准解析订单消息, 同时算出订单的单价, 以撮合不同的订单完成资产交换。

3.3.3 取消订单消息

当订单在过期之前未完全成交或者部分成交, 用户想以其它价格交换资产时, 可以发送消息以取消订单。取消订单的消息内容如下:

表 3 取消订单的消息格式

名称	类型	说明
version	uint16	EOS-TRANSPORT 网络版本号
orderId	uint256	被取消的订单号
nonce	uint256	交易计数, 表示到目前为止发送的消息总量, 包括创建创建和取消订单

account	name	消息发送者地址
sign	bytes32	通过私钥签名生成的参数

用户发送消息以取消订单时，该订单可能还未与任何其它订单匹配交易，此情况下取消订单就比较简单，直接将订单从撮合队列中一移除即可。另外一种是比较复杂的情况，如该订单已经有部分成交，需要将未成交的部分取消，这时需要将原始订单进行拆分成已成交部分和未成交部分，已成交部分不能再被取消，未成交部分取消即可。

3.4 订单撮合

3.4.1 订单撮合原则

订单撮合是指卖方在 EOS-TRANSPORT 网络上委托销售订单，买方在 EOS-TRANSPORT 网络上购买订单，EOS-TRANSPORT 按照一定的原则确定双方成交的价格，完成交易。

撮合价格的计算建立在买入价格 PB(Price Buy)必须大于或者等于卖出价格 PS(Price sell)的基础上：

1. 当 PB 等于 PS 时，成交价格即按照 PB(PS)指定
2. 当 PB 大于等于 PS 时，若前一笔成交价 PP 小于 PS 则按照 PS 定价；若 PP 大于 PB 则按照 PB 定价。

EOS-TRANSPORT 基于内存的撮合系统架构如图 2 所示。



图 2 EOS-TRANSPORT 内存撮合系统架构图

基于对区块链中币币交易的研究，EOS-TRANSPORT 采用一种基于内存状态机复制技术的撮合引擎集群方式，基于内存的撮合方式可以大大提高撮合效率，撮合引擎集群解决实际环境中宕机情况的出现。同时，EOS-TRANSPORT 网络节点会使用订单筛选算法，对订单进行优化处理，提高撮合成功率，每一个节点使用内存状态机复制技术，保证撮合系统的健壮性。

3.4.2 订单撮合算法

在 EOS-TRANSPORT 上，撮合引擎的重要组成部分是用户的买卖订单，通过对买卖订单进行撮合形成交易记录。但是在实际情况中，会出现订单无法立即完成撮合的情况。根据这种情况，EOS-TRANSPORT 设计买入队列和卖出队列保存订单。队列遵循“价格优先、同价格下时间优先”规则。买入队列按照委托价格从低到高顺序，卖出队列按照委托价格从低到高顺序，如图 3 所示。

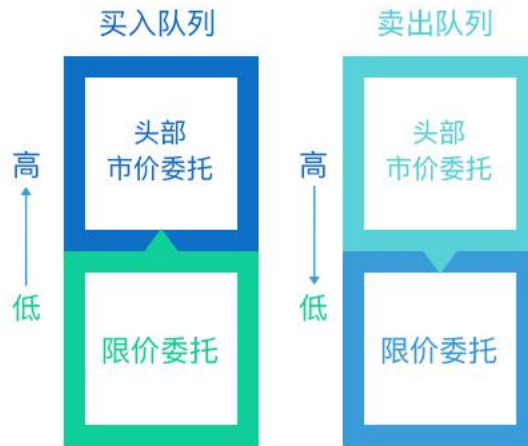


图 3 订单队列示意图

如图 4 所示，撮合引擎接收到新的买入订单，会在卖出队列的头部查找是否存在符合价格规则的卖出订单，如果存在卖出价格小于或等于买入价格的订单，则从队列中取出此订单并撮合成一笔交易；若卖出队列为空或者队列头部不满足价格关系，则将买入订单插入买入队列中，因为买入队列按照价格和时间先后顺序排序，所以新插入的订单会经过一次排序插入到买入队列的相应位置。

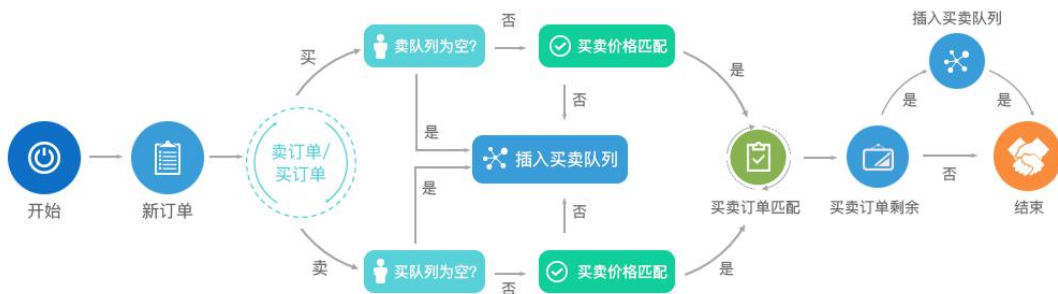


图 4 订单撮合流程图

同样，撮合引擎接受到新的卖出订单，则会到买入队列的头部查找是否存在符合价格规则的买入订单，如果存在买入价格大于等于卖出价格的订单，则从订单队列中取出此订单并撮合成一笔交易；若买入队列为空或者队列头部不满足价格关系，则将卖出订单插入到卖出队列中，由于卖出队列也是按照价格与时间先

后进行排序，所以新插入的订单会经过一次排序插入到卖出队列的相应位置。

3.5 EOS-Transport 网络

社区有一定条件的成员可以申请运行 EOS-Transport 网络节点。

EOS-Transport 网络节点接收用户的挂单、撤单等请求，并将请求广播给网络中的其它节点，同时通过路由层的路由算法将请求路由给相应的撮合引擎。撮合引擎根据撮合算法对用户的订单进行撮合，完成买单和卖单的匹配，其网络架构图如图 5 所示。

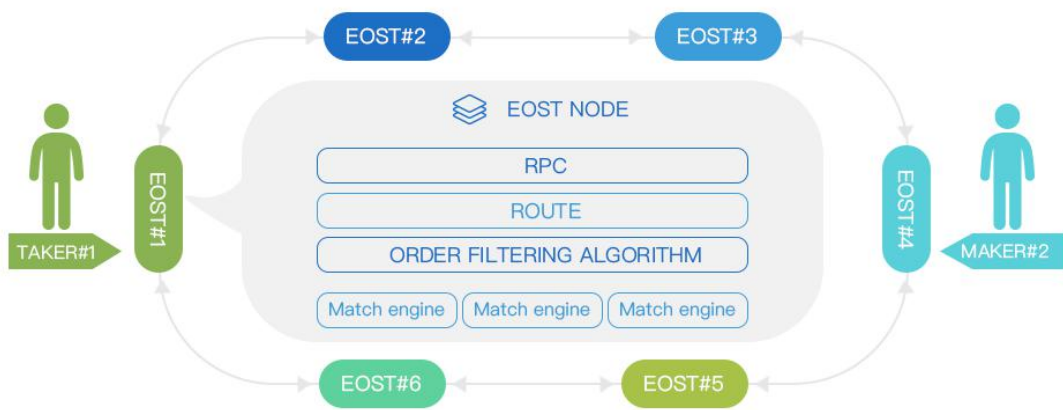


图 5 EOS-TRANSPORT 网络架构图

EOS-TRANSPORT 网络节点之间可以通过广播的方式将订单广播到网络中的其它节点，由于每个节点的处理能力不同，节点可以自行选择优先撮合的交易对。比如某个项目方运行了一个 EOS-TRANSPORT 网络节点，那么这个节点可以优先撮合这个项目发行的代币，从而提高代币的流通速度。同时作为 EOS-TRANSPORT 网络中的节点，撮合订单交易可以获得交易手续费，从而鼓励社区中的成员运行网络节点。

4. Token 交换 EOS-TRANSPORT 网络撮合效率提升的潜在方式

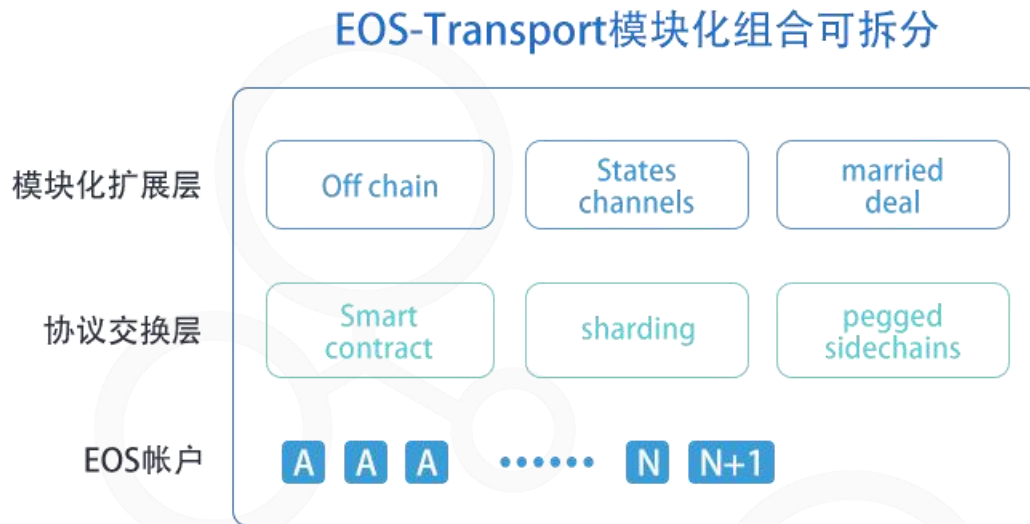


图 6 终端撮合引擎模块化组件

终端撮合引擎的整个架构设计成模块化组件，以增加整个 EOS-TRANSPORT 网络的可扩展性。对当前技术发展来看，提高资产交换的撮合效率的方式有以下几种：

4.1 状态通道

目前，EOS 目前的 TPS 已经到达 1000 以上，相比于比特币（目前 TPS 为 7 左右）、以太坊（目前 TPS 大概在 13 左右）等公有链已经有非常多的提升。但相较于传统中心化服务架构的 TPS 还有一定的距离。比特币、以太坊等公有链在提高 TPS 的方面引入了状态通道技术。状态通道提出是这样的一种策略，虽然它保留底层的区块链网络运作的模式，但改变了网络的具体用法，通过链下完成具体的操作来解决可扩展性的挑战：它不仅仅将区块链作为处理任何形式交易的主要处理层，而是作为一个结算层，只处理一系列互动所产生的最终交易，并只在出现争议的时候执行复杂的运算操作。¹

¹

状态通道在应用的时候可以采用 A->B 的通道，也可以组合通道，还可以加入智能合约，在转账和支付执行过程进行复杂的操作中可以很有效的提高效率。

因此，EOS 在进一步进行提升 TPS 的研究时，也可以使用状态通道技术来达到一定的目的。同时，EOS 的操作目前需要抵押 EOS 来换取 RAW、CPUT 和网络，这无疑约 DAPP 的开发者们增加了运营成本，如果使用状态通道将部分操作放于链下，对整个 EOS 生来说是非常有帮助的。

4.2 楔入式侧链技术

侧链技术可以让用户访问大量新的区块链技术，并且提供安全隔离，在 EOS-TRANSPORT 网络升级时避免不可预知风险，侧链发生灾难性问题时，不影响主链的良好运行。

EOS-TRANSPORT 网络在后期会引入侧链技术，用于尝试提升撮合效率，把体验升级逐渐向中心化交易所方向靠拢，在较好的兼容不同公链的数字资产的同时还能保障用户的资产安全。

4.3 分片技术的引入

目前，在所有区块链网络中，每个节点都存储所有状态（账户余额，合同代码和存储等）并处理所有的交易。在提供了极高安全性的同时，也极大限制了可扩展性：区块链不能处理比单个节点更多的事务。在很大程度上正因为如此，比特币被限制在每秒 3-7 个交易，以太坊到 7-15 等。

将状态分成 $K = O(n/c)$ 分区，称之为“分片”。例如，以太坊的分片方案会将所有以 a 开头的账户放入一个分片中，所有以 b 开头的账户放入另一个分片中等等。在最简单的分片形式中，每个分片也具有自己的交易历史记录，在一些分片 k 中的交易被限制在分片 k 的状态。在更高级的分片中，也包括某种形式的跨分片通信能力，其中一个分片上的事务可以触发其他分片上的事件。

EOS-TRANSPORT 再考虑提高计算效率和存储效率时，也会对分片技术进行研

究,通过引入分片技术为整个区块链世界打造一个高效和无磨擦的多终端撮合引擎系统。

4.4 多终端（钱包、Dapp）内挂单撮合引擎

众多的终端开发团队，项目方开发的 Dapp，都在逐渐的尝试把数字资产的交换内置进自己的应用里，从而方便用户完成资产的交换。如果每个钱包开发团队都去开发一套资产交换程序，不仅给团队增加了开发成本，而且重复造轮子，浪费资源。因此，针对这些问题，EOS-Transport 网络提供了一些解决方法。

EOS-Transport 网络为这些终端（包括钱包、DAPP 等）挂单提供了外部撮合引擎，针对不同的钱包、项目方 Dapp 等终端的挂单提供了精准的撮合，同时为各个终端挂单提供 Api 进行集中撮合。

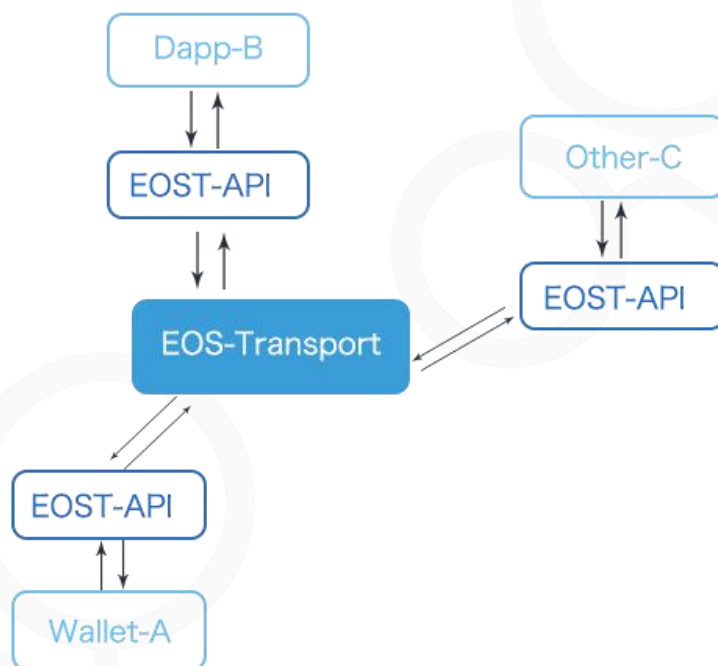


图 7 多终端挂单撮合

5. EOS-TRANSPORT 网络规则-社区经济生态

EOST 作为 EOS-TRANSPORT 网络的 Token 资产添加都是通过提前预设好的智

能合约规则完成，一方面通过燃烧 EOST（终端撮合引擎的 Token），添加 Token 合约地址，另一方面是由社区超级节点投票完成合约地址的添加。

EOST 致力于打造开放式社区，形成一个良性的 Token 经济环境，随着生态的逐渐完善，持有 EOST 将会获得生态发展的红利。

5.1 Token 添加规则

EOST-TRANSPORT 网络添加 EOS Token 资产，需要通过智能合约添加 Token 的合约地址，并且向特定黑洞地址打入特定数量的 EOST Token，然后广播消息，完成合约地址添加。

提交 Token 合约地址，随后生成一个特定不可提现的“黑洞”地址，分批次的向“黑洞”地址转入 EOST Token，合计超过特定数量，合约生效，Token 合约添加完成。

5.2 超级节点运行规则

EOST-TRANSPORT 网络社区的超级节点规则，设定智能合约规则，锁定 50 万 EOST 可以成为社区超级节点，锁定周期固定为 12 个月或者特定数量区块高度。

成为超级节点可以进行 Token 合约地址的添加投票，超级节点投票规则设定为，赞成票大于反对票，且赞成票大于 10 个，即可完成合约添加。

5.3 其他可能收入

其他收入，如交易手续费等。

6. 发展路线图

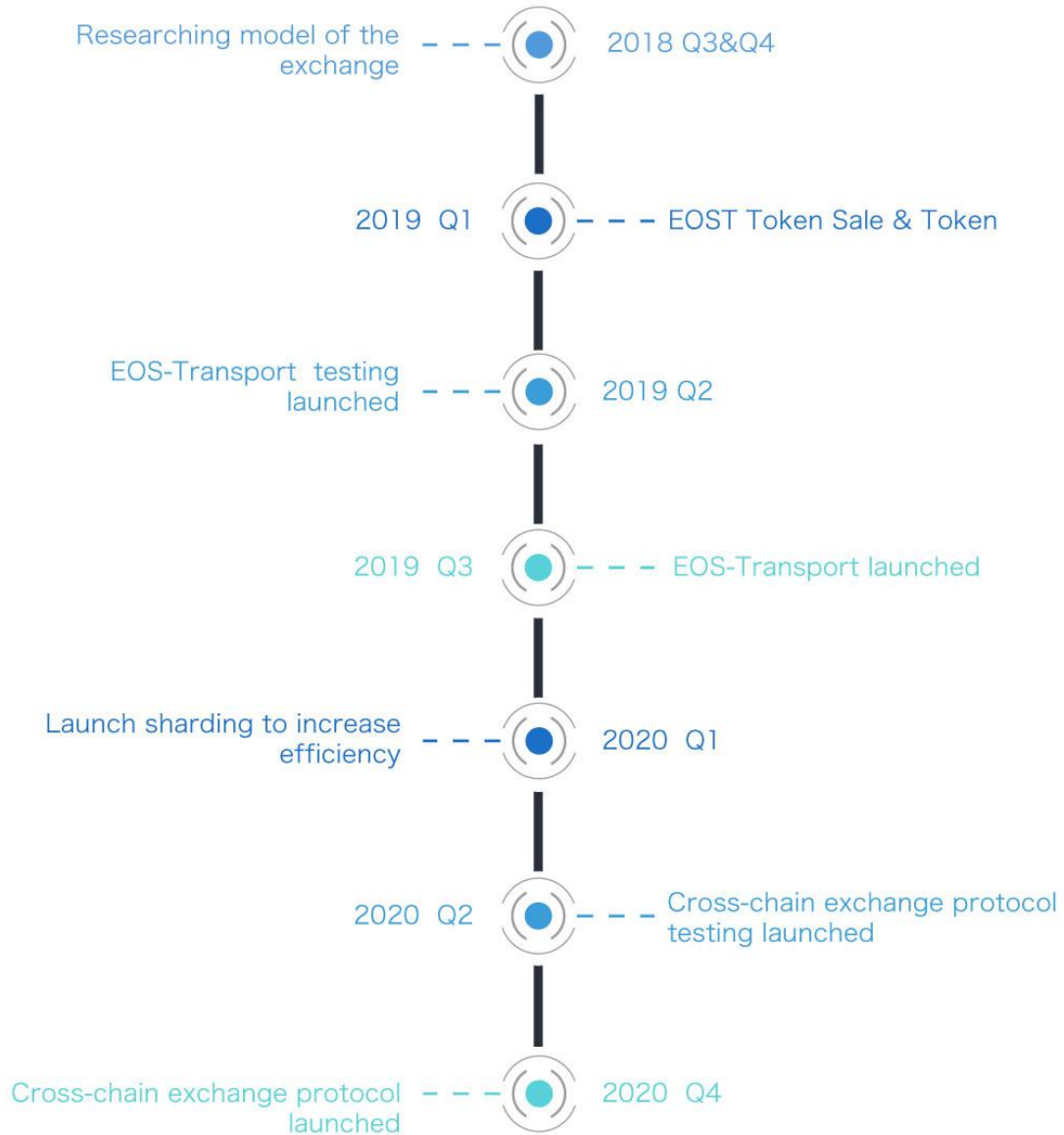


图 8 发展路线图

7. Token 发行计划

EOST 是 EOS-TRANSPORT 网络合约平台上流动的唯一 Token，Token 生成总量为 21 亿个，对外释放 30%，Token 数量 6.3 亿枚。

7.1 EOS-TRANSPORT 网络 Token 功能:

1. 交换 EOST 流通的经济模型标的;
2. 添加 Token 智能合约 GAS (燃料);
3. 添加 Token 成为超级节点, 参与投票;
4. EOST 是整个生态的流通支撑。

7.2 私募细则

EOST 项目 Token 分配: 创始团队 10%, 项目市场推广运营 10%, EOST 项目自生态建立 40%, 对外合作预留 10%, 对外私募 30%。

锁定周期:

1. 私募部分不锁仓;
2. 创始团队锁定 3 年;

分配方式

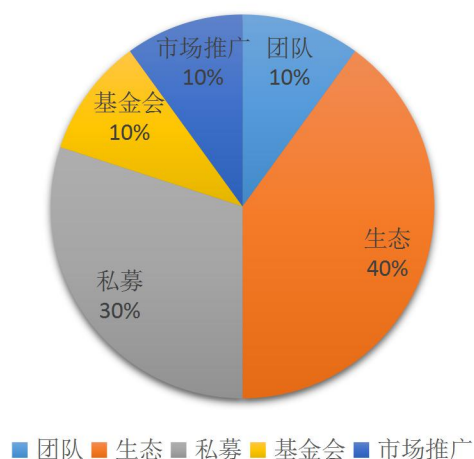


图 9 代币分配图

7.3 募集资金用途

EOST 募集的资金将用于支持推动基金会社区的发展和扩张,改善区块链社区行业生态。发现更多的生态参与者,奖励重大价值发现和贡献。

研发费用: 50%

建立一个安全、透明并且具有持续自我迭代能力的 EOS-TRANSPORT 网络。

市场推广: 20%

EOS-Transport Network 网络的市场推广、知名度提升以及用户增加。

对外合作及社区生态: 20%

用于支持推动 EOST 项目的对外合作及社区的发展和扩张,改善区块链行业生态。发现更多的生态参与者,奖励重大价值发现和贡献。

早期支持者及团队: 10%

用于社区早期支持者及后期团队人员增加。

8. 风险提示与免责声明

本声明不涉及与证券招标以及承担 EOST 经营性的相关风险

不涉及任何在司法管制内的受管制产品: 本文件是项目阐述的概念性文件【白皮书】,并非出售或者征集招标与 EOST 产品及其相关公司的股份、证券或其他受管制产品。根据本文件不能作为招股说明书或其他任何形式的标准化合约文件,也并不是构成任何司法管辖区内的证券或其他任何受管制产品的劝告或征集的投资建议。本文件不能成为任何销售、订阅或邀请其他人去购买和订阅任何证

券，以及基于此基础上形式的联系、合约或承诺。本白皮书并没有经过任何国家或地区的司法监管机构审查。

不作为参与投资的建议：在本文件中所呈现的任何信息或者分析，都不构成任何参与 Token 投资决定的建议，并且不会做出任何具有倾向性的具体推荐。您必须听取一切有必要的专业建议，比如税务和会计梳理相关事务。同时不能构成任何声明和保证：本文件用于说明我们所提出的 EOST 平台与 EOST Token，但是 EOST 基金会明确表示：

1) 对于本文件中描述的任何内容的准确性或完整性，或者以其他方式发布的与项目相关的内容，不给予任何声明和保证；

2) 在没有前提条件的情况下，不能对任何具有前瞻性、概念性陈述的成就或合理性内容给予任何声明和保证；

3) 本文件中的任何内容，不作为任何对未来的承诺或陈述的依据；

4) 不承担任何因白皮书的相关人员或其他方面造成的任何损失；

5) 在无法免除的法律责任范围内，仅限于所适用法律所允许的最大限度。

不是任何人都可以参与项目：EOST 的网络系统和 EOST 并不是任何人都可以参与，参与者可能需要完成一系列的步骤，其中包括提供表明身份的信息和文件。

非授权公司与该项目无关：除了 EOST 基金会和 EOST 之外，使用其他任何公司或者机构的名称商标，并不说明任何一方与之有关联或认可，仅供说明相关内容之用。与 EOSTToken 相关的注意事项：“EOST Token”或“EOST”，是 EOST 区块链网络的虚拟密码学 (Cryptographic) Token。

EOST 不是虚拟货币：在本文件未完成期间，EOST 不能在交易所兑换物品、服务和交易，也不能在 EOST Token 网络以外使用。

EOST 不是投资品：没有任何人能够保证，也没有任何理由相信，你所持有的 EOST Token 将会一定升值，甚至有可能存在贬值的风险。EOST 不是所有权证明或具有控制权：持有 EOSTToken 并不是授予持有者所有权以及 EOST 和 EOST 网络系统的股权；也并不是授予其直接控制或者替 EOST 和 EOST 网络系统做任何决策的权利。

EOST Token 相关的风险提示

由于用户个人错误行为造成的风险

1) 由于私钥遗失带来的风险:

在 EOST Token 分配给参与者前, 参与者会获得和 EOST Token 相关联的公钥账户, EOST Token 公钥账户可以通过参与者随机分配的私钥进入, 私钥遗忘将可能失去在相关联公钥账户的 EOSTToken。建议多练习如何操作以便于参与者能够安全的将私钥在多个本地设备中备份, 最好在非网络环境进行操作。

2) 由于私钥泄漏给第三方的风险:

任何第三方的个人或机构在获得了参与者的公钥账户的私钥后, 有可能就会处理其相应账户的 EOST Token。建议参与者保护好相关的设备, 防止未经授权登陆, 降低风险几率。

3) 由于参与投票可能会出现的风险:

EOSTToken 持有者在参与投票中, 由于恶意或者不负责任的投票行为, 极有可能导致 EOST 丢失。

由于在使用 EOST Token 期间网络安全相关的风险

1) 基于 EOS 网络 EOS-TRANSPORT 网络带来的相关风险:

EOST 在初期会发行基于 EOSEOS-TRANSPORT 网络开发的 ERC20Token, EOSEOS-TRANSPORT 网络上的任何故障和未知的功能, 都有可能导致 EOST 出现未知的不希望发生的情况。EOS 和基于 EOSEOS-TRANSPORT 网络的本地单元账户, 有可能会像 EOST 一样失去任何价值, 更多关于 EOSEOS-TRANSPORT 网络的信息参看: www.ethereum.org

2) 非官方的 EOST 网络替代的风险:

在 EOST 网络系统开发出来后, 由于是开源的代码和 EOS-TRANSPORT 网络极有可能存在被其他人抄袭并建立类似的网络系统。官方的 EOST 网络系统有可能需要同这些抄袭的网络系统竞争, 由此带来对 EOST 网络系统的负面影响需要所有用户承受。

3) 来自恶意第三方的不法入侵的风险:

黑客、其他团队或机构等恶意第三方，可能会试图干预 EOST 网络系统的发展，可能会采用但是不限于以下的方式：DDOS、Sybil、spoofing、smurfing 或者基于共识机制的攻击等。

4) 由于 EOST 网络系统存在基础设施软件安全漏洞的风险：

本网络系统是一个开源的系统，存在 EOST 的员工或者其他第三方机构有意或无意引入 bug 到网络核心系统中去，如此会导致 EOST 的使用风险和损失。

5) 密码学领域的重大技术突破会造成隐藏的弱点被挖掘和利用的风险：

密码学技术是区块链技术的重要部分，密码学的进步或其他高科技技术的发展，可能会对 EOST 网络系统和 EOSTToken 带来被盗或者丢失的风险。

6) EOST 网络系统故障的风险：

EOST 网络作为比较高新的系统，可能会产生让人不能够接受或意想不到的网络故障，同时也有可能导致 EOSTToken 消失的风险或其他对市场造成波动的风险。

7) EOST 可能会因为其高价值出现被挖矿攻击的风险：

对于很多去中心化的密码学 Token 和虚拟货币，EOST 网络系统的区块链技术生成的 EOST 有被挖矿攻击的可能，其中包括并不局限于双重攻击、大矿池攻击、“自私挖矿”攻击和竞争条件攻击等，也可能出现未知的更新颖的挖矿攻击，对 EOST 网络系统的运行带来巨大的风险。

由于市场的不确定性造成的风险

1) EOST 系统用户量少的风险：

EOST 系统会随着时间产生相应的价值，如果 EOST 网络系统不被更多的商业、个人或者其他机构使用，不能够产生更多的公众关注度对其发展造成使用人数少的影响，可能会限制或降低 EOST 的使用和价值。

2) EOST 来自交易所造成的流动性不足的风险：

目前 EOST Token 还未在交易所进行交易，如果在交易所开放交易后，很有可能因为交易所比较新对于各种法律法规了解的少，比起那些成立时间久声誉好有其他成熟虚拟 Token 正常交易的交易所来说，新交易所很容易出现欺诈和失

败的可能。交易所的问题可能会造成有很大一部分 EOST Token 交易陷入欺诈或其他运营风险问题，如此会导致 EOST 的价值和流动性降低。

3) EOST 网络系统的发展跟不上 EOST Token 持有者预期的风险：

EOST 网络系统当前还处于开发阶段，而且在对外正式发布前可能会有很大的变化，参与者对 EOST Token 或者网络系统的预期可能跟实际的发布时间会不同，同时也可能会在设计和执行上的实际情况的变化导致不能按计划发布。

4) 参与者在面对损失时无法得到保险的风险：

EOST Token 公钥账户和银行账户、其他金融机构账户或者其他社交服务账户不同，EOST 基金会通常不会对网络系统购买保险。当出现 EOST 丢失或者网络系统失去价值时，不会有任何保险机构可以对 EOST 的持有者提供索赔服务。

5) EOST 项目解散的风险：

EOST 项目会存在各种因素，比如比特币、EOS 的价值大跌、商业运作失败或者因为知识产权索赔等，EOST 项目或许会无法继续运营从而导致不能成功发布或者团队解散。

6) 相关地区和国家的司法或行政部门的监管政策的风险：

区块链技术目前在世界范围内都获得了支持或认可，但是同时也受到了各种监管部门的仔细审查。EOST 网络和 EOST 的功能可能会受到部分监管政策的影响，其中包括但是不限于限制使用或者拥有 EOST Token，由此可能会阻碍或者限制 EOST 网络系统的发展。

7) 其他未知的风险：

区块链技术和相应的数字货币技术 是相对比较新的并且未经完全验证的科技，可能会出现更多无法预测的风险，风险可能会以更多的方式出现。本文件可能随时会被修改或者置换，然而我们没有任何义务更新此版本白皮书，或者提供读者额外资讯的渠道。

9. References

- [1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/en/bitcoin-paper>, 2008.
- [2] EOSIO: EOS.IO Technical White Paper. <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md>, 2016
- [3] Jeff Coleman. State Channels. <http://www.jeffcoleman.ca/state-channels/>. Accessed: 2018-04-05.
- [4] Joseph Poon, Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. <https://lightning.network/lightning-network-paper.pdf>, 2016.
- [5] Jeff Coleman, Liam Horne, and Li Xuanji. Counterfactual: Generalized State Channels. 2018.
- [6] Will Warren, Amir Bandeali. 0x: An open protocol for decentralized exchange on the Ethereum blockchain. https://www.0xproject.com/pdfs/0x_white_paper.pdf, 2017.
- [7] Loi Luu , Yaron Velner. KyberNetwork: A trustless decentralized exchange and payment service. 2017.
- [8] Bitcoin Wiki: Contract. <https://en.bitcoin.it/wiki/Contract>, Accessed, 2017-11-23.
- [9] Bitcoin Wiki: Payment Channels. https://en.bitcoin.it/wiki/Payment_channels, Accessed, 2018-03-23.
- [10] Ledger Labs: State Channels Wiki. <https://github.com/ledgerlabs/state-channels/wiki>. Accessed: 2017-12-16.
- [11] Raiden specification. <http://raiden-network.readthedocs.io/en/stable/spec.html>, Accessed, 2018-01-23.
- [12] Stefan Dziembowski, Sebastian Faust, Kristina Hostakova. Foundations of state channel networks. <https://eprint.iacr.org/2018/320>, Accessed, 2018-02-21.
- [13] Gavin Wood. Ethereum: A secure decentralized generalised transaction ledger. <https://ethereum.github.io/yellowpaper/paper.pdf>, Accessed, 2017-10-14.
- [14] Sun changhao. Design of highly reliable financial transaction matching system with high performance. <http://www.docin.com/p-1885705562.html>, Accessed, 2018-06-23.