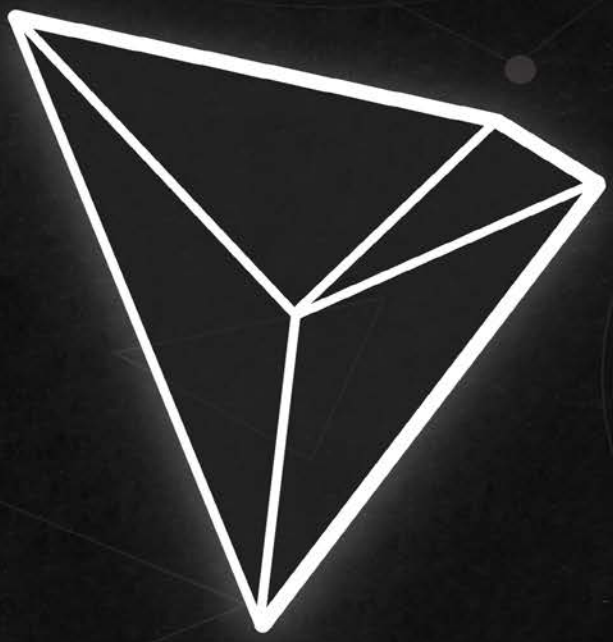


TRON

Whitepaper

前言 拯救互联网

WWW 的发明者 ,2016 年图灵奖得主 ,Tim Berners-Lee 在 2017 年发表声明，他的发明，互联网，正在偏离其最初的航向。

是的，这些年，互联网开始变得有些不对劲。

最初 ,当 Tim Berners-Lee 创造互联网时 ,互联网是一个完全去中心化的平台，任何一个人都可以创造内容，网页，网站，并与其他人自由互联。而如今的互联网，已经从当年那个学术研究的简单分享网络，茁壮成长为统治商业，传播，娱乐与资讯的庞然大物。

而关于互联网的权力结构也正在发生着转移。

毫无疑问 ,现在互联网不再属于每个人 ,而属于定义互联网规则的超过一千亿美金的大公司，Amazon，Facebook，Google，Apple，在中国，有 Alibaba，Tencent。

原先互联网的流量，数据，内容是分散的，现在流量，数据，内容都变得空前集中，集中于 Facebook，Messager，Instagram，Snapchat 等巨头，中国则集中于微信，头条，淘宝，QQ 等头部应用。

这些行业巨头享受着全球数十亿用户创造的天量数据而为己所用 ,创造巨额利润，并拥有着塑造用户所见，所得，所想的权力。

巨头公司 ,而非用户本身 ,拥有着控制数据的能力 ,那些原本属于用户创造的数

据，不再属于它的主人。那些试图夺回数据主动权的尝试变得不合时宜，搭建网站，自建 APP 变得难上加难，我们不得不试图去迎合微信，Facebook 的规则，试图揣测微博 ,Twitter 的分发机制 ,丧失了自己的本体。而即便自己搭建了 APP，被苹果下架也是轻而易举的事情。

摧毁一个人，抹掉一件事，灭绝一份事业，从来没有如此轻而易举。

本质上来说，互联网已经不是当初那个去中心化的互联网了，他甚至比报纸，杂志，唱片这些被它颠覆掉的旧势力还要中心化，毕竟我可以收藏我的报纸，但却无法备份我的微博。

是的，波场（TRON），是一场关于拯救互联网的尝试。

我们不管这个尝试在巨头看来是否不合时宜 ,也不管在普通人看来是否螳臂当车，也不论这件事情是否成功。

我们坚信，用户必须拥有最终对于其创造数据的所有权与处置权，这种权力将不再让渡给平台，用户自由的拥有所有数字信息。

我们坚信，用户必须拥有对内容所见所得的最终决定权，信息的分发必须自由，自愿，建立在用户自我选择的基础上。

我们坚信，用户必须拥有自由使用数据内容获得数字资产激励的权利，他们的数字资产将不再受任何平台的约束，得到去中心化互联网的保护，安全无忧，生来自由。

这一切，都会建立在一个去中心化，名为波场（TRON）的协议之上。

这是一场对于中心化互联网的反动，我们也许会失败，但我们相信，有人会成功。

因为，去中心化，是互联网本来的样子。

1. 什么是波场（TRON）？

波场 TRON 是基于区块链的去中心化内容协议，其目标在于通过区块链与分布式存储技术，构建一个全球范围内的自由内容娱乐体系，这个协议可以让每个用户自由发布，存储，拥有数据，并通过去中心化的自治形式，以数字资产发行，流通，交易方式决定内容的分发、订阅、推送，赋能内容创造者，形成去中心化的内容娱乐生态。

TRON 结合了社交网络与价值网络的双重优点，将协议生态繁荣置于首位。在任何一个社区，经济体，自由市场经济中，一个公平并合理反映参与者贡献的激励系统是社区立足之本。TRON 将首次利用数字资产去尝试准确透明的衡量与激励生态的参与者与贡献者，赋能内容生态。

2. 波场（TRON）的价值观

在设计波场（TRON）之初，如下核心价值观被贯彻始终：

1. 数据产生者（用户）将会拥有对于数据的根本所有权，互联网应当以去中心化的形态存在。这一逻辑在互联网诞生之初，由 Tim Berners-Lee 博士提出，是互联网最初诞生的初心。

2. 每个为波场生态做出贡献的人，都将按照规则获得按比例的收益。价值网络的最大优势，在于能够将社交与媒体网络中的一点一滴数字资产化。

3. 所有形式的贡献都应具有同等的量化价值。例如，参与者投入的时间，制作优秀内容，注意力本质来说与提供资本具有同等衡量价值。

4. 波场生态的根本目的是服务于大众。波场是由非盈利基金会所运行的生态，其目标是创造于服务全球享受内容娱乐的大众，而并非创造利润。波场的所有参与者将会受益于波场生态本身的繁荣。

5. 内容应当产生于人，而非资本，资本应用于奖励人，而非控制人。例如文创产业的核心推动力应当是对于艺术，内容本身质量的追求，需求应来自于内容创作者，艺术家，编剧，而非本身并不消费内容的资本家。

3. 波场（TRON）所提供的基础设施

波场生态将为生态参与者提供如下基础设施：

1. 高质量内容的内容平台
2. 连接所有人的社交网络
3. 桥梁数字货币
4. 支付网络
5. 生态自治系统

4. 波场（TRON）的特点

TRON（波场）作为去中心化的内容协议，与中心化的互联网结构相比，具有以下四个基本特征：

1. 数据自由：自由而不受控制的上传、存储并传播包括文字、图片、音频和视频在内的内容
2. 内容赋能：通过内容的贡献和传播获得应有的数字资产收益，经济激励赋能内容生态
3. 个人数字资产发行：个人可以自由的通过发行数字资产， 他人则可以通过购买数字资产享受数据贡献者不断发展所带来的利益与服务。
4. 基础设施：分布式的数字资产则会匹配一整套完整的去中心化基础设施，包括分布式交易所，自治性博弈，预测，游戏系统。

5. 波场（TRON）如何实现激励？

波场根本上设计要解决内容经济的货币化。波场机制是一套以经济激励内容产生的机制，但将其加密货币化。通过密码学实现的经济激励可以显着促进内容平台个体的成长，我们相信加密货币能够前所未有激励内容生态。

TRON 将提出一套不断完善的机制来对个人生态贡献进行评估。现有的绝大多数平台采用单用户一票制，这样的机制很容易被刷票与垃圾请求控制和攻击。现在的内容平台已经被盈利诉求与中心化的机制所控制，我们看到的内容都是内容中心化平台希望我们看到的内容，而并非我们希望看到的内容。微博，今日头条，微信公众平台，Facebook 信息流的算法并不是公正的，而逐渐沦为可被操纵的工具。平台也将广告平台当作第一获利模式，百度的蜂巢，今日头条的广告推荐

算法， 维系公众号的广点通，微博的推广计划，淘宝的广告频道都是典型的变现模式，而并无法将吸引流量本身的内容给予赋能。

而波场则希望通过去中心化的方式，将经济激励系统本身变为能够在系统内进行循环的体系，用户能真正拥有一个享受自己喜欢内容的平台，同时也不会与平台的盈利诉求冲突。波场所形成的自治体系，也将前所未有的赋能于生态成员，使得其形成生态自治，而非现在早已沙化的扁平用户机制。

生态管理与决策中，波场只允许参与多年阶段性解冻 TRX 的用户参与投票。在这样的模型下，社区成员将被鼓励长期持有 TRX，这样将会使 TRON 的长期价值最大化。

6. 波场（TRON）的实现路径

对于波场（TRON）来说，其整个体系的实现预计将会是一个为期 8-10 年的工程，涉及 6 个步骤的庞大工程，具体来说，实现路径如下：

1. Exudos，出埃及记，数据自由-基于点对点的分布式的内容上传、存储和分发机制

出埃及记阶段，波场（TRON）将建立在以 IPFS 为代表的分布式存储技术之上，为用户提供一个可以完全自由可依赖的数据发布，存储，传播平台。

2. Odyssey，奥德赛，内容赋能-经济激励赋能内容生态

区块链技术，将为内容产生，分发，传播建立一整套充分竞争、回报公平

的经济机制，激励个体，赋能内容，从而不断拓展系统的边界。

现有中心化的互联网体系之下，内容生产者绝大多数情况下通过广告模式进行变现，但是现有的广告模式推送带有极强的骚扰性质，严重干扰用户体验，变现效率因此也十分低下；其余内容创造者通过打赏与礼物变现，又因平台无法自带支付系统，而面临着高达 30%-90%的渠道抽成， 打赏变现模式也带有极大的随意性，绝大多数内容提供者无法实现盈亏平衡。

对于内容生产者来说，迫切需要内容协议中自带支付系统，获取内容行为本身就可以被支付行为所衡量，而且支付与购买行为是建立在透明的区块链记录之上。

波场（TRON）协议，作为基于区块链的自由内容娱乐体系，体系内以 TRX 进行流通，原生的经济体系使得现阶段的数字娱乐内容提供商，前所未有与普通用户实现一对一交互，无需再向 Google Play, APP Store 或者其他中心化平台缴纳高昂的通道费用，而文字，图片，视频，直播等内容的提供者，也将摆脱人气，点击量无法变现的魔咒，有人气便有的打赏，打赏越多越有人气，分布式的清算与存储模式，也将使得开发者，内容提供者能够完全自由的从事创作，不受中心化管理者的制约。

内容生产者可以在波场（TRON）系统内直接获得粉丝用户的为优质内容而付出的 TRX，也可以通过产出优质内容获得影响力和传播力从而直接获得体系给予的 TRX 奖励。

以内容分发主要权重的用户操作价值评分举例：

用户操作价值评分V_C^t的计算公式为：

其中：

$$V_C^t = \sum_{i=1}^{5} \sum_{j=1}^{c_i^t} w_i p_j x_j^t$$

$$p_j = trx_j / \left(d_1 + \frac{ca_j}{1 + e^{d_2 - ca_j}} \right)$$

C = 内容

w_i = 对应点击(1)、点赞(2)、评论(3)、打赏(4)、转发(5)等操作的权重

p_j = 第 j 次操作时用户的能量值。当用户在某段时间内，频繁操作某个交互时，用户的能量值会不断减小；当用户停止交互操作后，能量值会慢慢恢复，以此来限制某些刷量操作。

x_j^t = 第 j 次操作时用户的信用评分。该信用评分是根据用户在整个社区的信用情况，动态计算的。如果某个用户被多次举报投诉，他的信用评分会相应下调。

trx_j = 第 j 次操作时用户的可用 TRX 余额。用户当前 TRX 的余额，扣除系统锁定的数量，剩下的为当前可用 TRX 余额。可用 TRX 余额越大，用户的交互操作的价值评分越高，避免恶意用户注册多个空账户来刷量。

d_1 d_2 = 操作的阈值

ca_j = 第 j 次操作时用户各种操作的总数

c_i^t = 时刻 t，第 i 种操作的次数

对于直播类的即时内容生产者，区块链技术也可以透明、公正地展示主播人气，通过智能合约实时快速获得收入，避免中心化平台黑箱操作、拖延账期和无故封杀等有损主播和观众利益的问题。

直播平台主播分成智能合约举例：

```
pragma solidity ^0.4.11;

contract 波场（TRON）AnchorPay {
address platform;    // 平台地址

function 波场（TRON）AnchorPay() {
    platform = msg.sender;
}

function deposit(address anchor) public payable{
    uint for_anchor = msg.value * 9 / 10;            // 主播拿 90%
    uint for_platform = msg.value - for_anchor;
```

```
        anchor.transfer(for_anchor);
        platform.transfer(for_platform);
    }

    function withdraw() public{
        assert(msg.sender == platform);
        msg.sender.transfer(this.balance);
    }

function() payable{}
    }
```

通过波场（TRON）的底层区块链架构，使其可以自由地发行自有的代币，因而具备原生的经济体系，通过波场（TRON）的 Token – TRX，用户可以轻松实现内容价值的分发、支付和结算，体系也可以激励用户产出更多版权明晰且高质量具有高传播性的内容，从而使得整个内容产出体系达成良好的自运转。

3. Great Voyage，伟大航程，个人数字资产发行

波场（TRON）基于区块链的优势，解决了收益衡量、红利发放和支持者管理三大难题，实现了从“粉丝经济”向“粉丝金融”的重大转变，波场（TRON）基于区块链以 TRX 为官方代币的自治经济体系使得个人内容生产者在体系

内的每一笔收入和支出都公开、透明且不可篡改，通过智能合约，支持者们可以自动参与内容生产者的数字资产购买并按照约定自动共享红利成长，不需要任何第三方进行监督即可公正地完成全部流程。

内容生产者个人证券化融资举例：

波场（TRON）体系内短视频红人 Tom，基于对自身价值的判断，发行个人官方代币 Tom Token ,短时间内筹集较多 TRX ,而支持者将获得对于 Tom 产出内容的一系列特权，例如付费内容免费观看，TOM Token 持有前十名参与视频制作等，另外，也将获得 Tom 之后收益的使用权，如果未来 Tom 名气大增，收入大量增加，则 Tom Token 的智能合约使用将同样增加，价值将指数级上涨，支持者也将获得 Tom 成长的收益。

Tom Token 可以限定收益时效，比如一周，一个月，一年，三年，或无限期的级别，可以发行不同时限的 Tom Token，等级越高的，时限越长，比例越高。

例如 Tom 现有 1 万粉丝，日均打赏为 100 万 TRX，Tom 出让三年内收益 20%的使用权限 ,支持者 Kevin 花 3 亿 TRX 购买了全部发行的 Tom Token，静态溢价约 36.9%。购买之后，Tom 与 Kevin 签定一个智能合约，Tom 的粉丝 A 给 Tom 的打赏，自动按比例折算给 Kevin。

为防止 Tom 在融资之后创作质量下降，系统将规定 Tom Token 的变现条件，可以规定条件，例如以周为单位进行解禁，并且设立一定的指标衡量

创作的质量，达标才允许解禁，否则投资者 Kevin 可以取消合约。

显然，对 Tom 越不利的条件，越有利于 Tom 获得高估值，而 Tom 为了获得更高的收益，也有提高创作数量和质量，增加影响力的动力。

4. Apollo，阿波罗，价值自由流动-去中心化的个体专属代币交易

当每一个波场（TRON）体系内的内容生产者都可以发行自己的专属代币，则系统必须拥有一整套完整的去中心化交易所解决方案，方能实现价值的自由流动。

该平台将面临如下挑战：

1. 随着时间推移，平台上发行的代币种类数量惊人，交易者难以进行筛选，容易迷惑甚至被骗

2. 单个支持者的金额很小，但总人数众多，支持者对于平台资金的安全性要求很高，特别是要防止黑客攻击、交易平台携款潜逃等现象

3. 不同代币背后所代表的利益分配逻辑不尽相同，需要实时完成提示并快速交割

4. 交易历史需要公开透明，从而让参与各方了解历史全程，保证信息充分，降低交易风险

现有的中心化交易所无法应对以上挑战，特别是针对海量种类的代币的快

速筛选交易以及平台资金安全风险管控，因而需要去中心化的交易平台完成撮合交易，所有资金并不经手中心化的交易平台，而是始终存储在交易上方自己的账户当中，不存在资金被盗取或交易平台卷款潜逃的问题；另一方面，通过点对点的去中心化分布式内容寻址协议，交易者可以轻易而准确地在海量专属代币中找到自己希望投资的标的，而不会产生困惑。

通过去中心化交易平台的搭建，体系内的价值、财产权和风险可以实现自由流动交换，从而使得整个体系的经济活力呈几何倍数增加。

5. Star Trek，星际旅行，流量变现-去中心化的博弈与预测市场

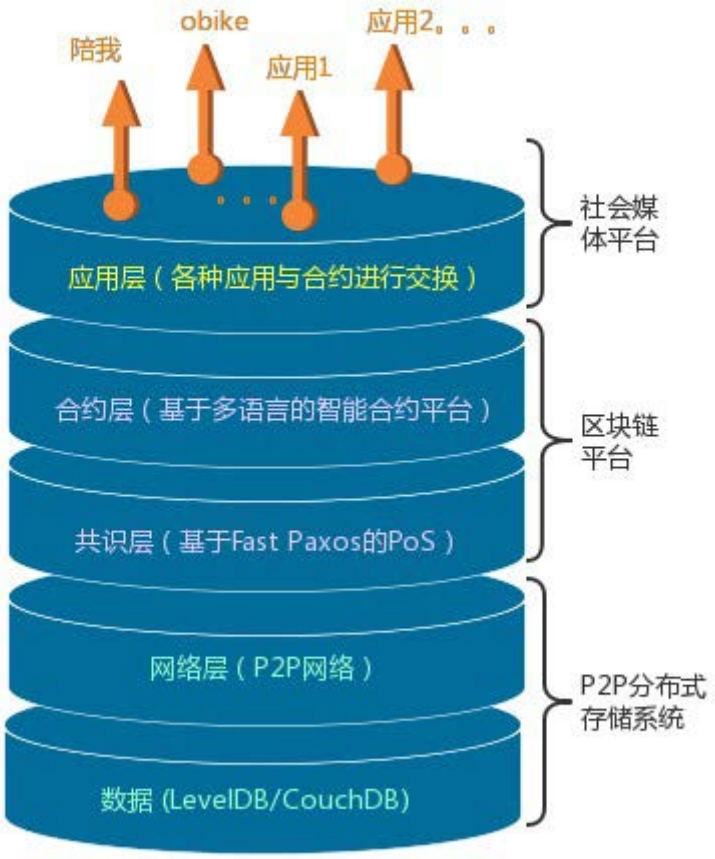
全球博弈市场规模 2014 年超过 4500 亿美元。波场（TRON）内容平台所带来的流量，为构建去中心化的线上博弈平台提供了可能。开发者可以通过波场(TRON)自由搭建线上博弈平台 ,提供全自治的博弈预测市场功能。

6. Eternity，永恒之地，流量转化-去中心化的游戏

2016 年，全球电子游戏市场规模达 996 亿美元，其中手机游戏市场规模 461 亿美元，占比 42%。波场（波场（TRON））为构建去中心化的线上游戏平台提供了可能。开发者可以通过波场（TRON）自由搭建游戏平台，实现游戏开发众筹，并为普通投资者提供参与投资游戏的可能。

7. 波场（TRON）技术体系

7.1 整体技术框架图



我们整体的架构由三个平台组成：

1.社交媒体平台：应用层，负责各种不同应用转化成智能合约语言；

2.区块链平台：提供了最核心的区块链的功能模块；

(1)合约层：基于多语言的智能合约平台；

(2)共识层：基于 PoS 的拜占庭容错共识算法；

3.P2P 分布式存储系统：底层的存储系统；

(1)网络层：基于内容寻址的定制化的 P2P 存储网络；

(2)数据层：实现了 LevelDB/CouchDB 的数据存储。

（一）社交媒体平台

通过利用许多现有的成熟技术，波场（TRON）作为一种新的内容平台提供安全、扩展性和私密性，同时也通过采取激励的机制让参与者积极贡献自己机器的处理能力构建用户注册网络，赋予积极贡献者发送广告给整个网络的特权达到激励的目的，当然这种消息群发会有数量上的限制。

1.用户注册 P2P 网

无中心但安全的用户注册通过区块链机制实现，同样的机制已经在比特币中得到应用，无需中心授权，能避免双重支付难题。通过区块链保证不会出现重复的注册用户，新注册用户在生效前必须得到多个区块的确认，即公证。每个块定义为：

$$Block_i = [i, H(Block_{i-1}), Nonce_i, SpamMsg_i, [UserReg_j, UserReg_{j+1}, ...]]$$

H（$Block_i$）提供 proof-of-Work 工作量证明，证明用户确实在 $Nonce_i$ 空间通过暴力求解的方法找到了满足条件的 Nonce 值，同时通过验证也避免偶然的哈希冲突。求解的困难度由 Difficulty 值决定，同比特币网络一样，每小时平均产生的块数由系统自动设置。

$$UserReg_j = [Username_j, PUBK_j, Nonce_j]$$

新用户 j 向网络注册的时候必须广播 $UserReg_j$，其它节点收到广播消息后，必须进行 H（$UserReg_j$）的工作量证明，这防止通过虚假注册进行拒绝服务攻击。这种工作量比区块链的工作量要小得多，典型地几分钟的计算量即可求得问题的解。

区块链提供了从用户名 $Username_j$ 到用户公钥 $PUBK_j$ 的映射，一种可公开查询的词典。

2.可路由的 DHT 覆盖网

第二个网络是类似于 Kademlia[3]的 P2P 覆盖网，主要用于资源存储和内容查找，也用于用户之间直接递送通知。

使用用户的 ID 作为网络节点标识似乎是一种好的选择，但这导致用户身份和位置的暴露，破坏了系统的私密性。因此，采用对节点的 IP 地址和端口号进行哈希来对节点标识，作为 DHT 网络中节点的名字，这种方式也能避免女巫攻击：

$$ID_{node\_j} = H([IP_j, port])$$

DHT 网络中从 ID_{src} 发往 ID_{dst} 的包定义如下：

$$Packet = [ID_{dst}, ID_{src}, SIG_j(payload), ID_j)]$$

负载 payload 通过用户 ID_j 签名，在包重传/刷新时 ID_j 可能是不同于 ID_{src} 的其它用户。

这些功能构成了 DHT 覆盖网概念模型第三层功能，再往上是“应用层”，提供数据存储原语 PUT 和 GET，PUT 定义如下：

$$payload_{PUT} = [target, value, time, seq] \text{ where}$$
$$target = [owner, resource, restype] \text{ and } ID_{dst} = H(target)$$

接受存储请求前，目的节点需要做如下规则的检查：

ID_{dst}= H（target）：确信目的地址正确计算；

ID_{dst} 是实际收到请求节点 ID_{node} 的邻居；

ID_j = H（owner）：在 restype 为“single”时校验；

seq 大于存储的旧值 seqold，同样也是在 restype 为“single”时校验；

time 是有效时间（即不应该是一个未来的时间值）。

restype 定义资源类型，存在两种可能的值“single”和“multi”，single

表示仅可由键的属主更新的资源；multi 表示来自于不同用户的响应（比如对某个帖子的所有回复）。对 single 类型，节点仅存储单个值，而 multi 类型，新 PUT 请求会将值附加到 list 上。这两种类型的存储都可设置过期时间，超过设定时间后相应的存储会从系统删除，从而自动清除过期的数据。

数据检索原语 GET 也能对两种类型的存储资源进行操作，别的与动态内容相关的非存储资源也可以实现类似的访问操作，从而共用同样的 API 接口。

3.用户内容

用户 j 的第 k 个消息定义为：

$$UserPost_{jk} = SIG_j([Username_j, k, type, MSG_k, REPLY_k])$$

MSG_k 是内容，k 是一个单调递增的数，type 可能的取值包括：新的帖子、回复、重传（RT）、直接递送的消息（DM）,$REPLY_k$ 是一个可选域，在回复/重传时提供对原始消息的引用，定义为：

$$REPLY_k = [Username_{j'}, k']$$

表示原始消息是用户 j’ 个的第 k'个消息。

内容在两个覆盖网同时被共享：

1.作为短期存储值存储于 DHT 中；

2.在 BitTorrent 网络中类似文件一样进行归档。

当新的内容创建时，客户端必须向下面的两个地址都发送 PUT 请求：

$$ID_{UserPost\_jk} = H([Username_j, \text{“post”} + k, \text{“single”}]) \text{ and}$$
$$ID_{swarm\_j} = H([Username_j, \text{“swarm”}, \text{“single”}]).$$

$ID_{UserPost\_jk}$ 是第二个 DHT 网络中目标存储节点的地址，提供任意内容的检索能力。

ID_{swarm_j} 是第三个网络中与用户 $Username_j$ 的内容相关的 torrent swarm

群的网关地址，这个 torrent 包含给定用户 j 全部的内容，独立于第二个 DHT 网络基于 BitTorrent 协议提供快速的内容分发和共享。ID_{swarm_j} 的邻居节点需要加入用户 j 的 swarm 集群，帮助内容的存储和分发，提供数据的可靠性、更好的数据分发性能；类似地，$ID_{UserPost\_jk}$ 的邻居节点也需要存储 $ID_{UserPost\_jk}$ 存储的同样的值。

Swarm 群机制解决了新内容快速高效通知和分发的问题，使用户的跟随者不用一直轮询 DHT 网络地址以判断是否有新的内容产生。

（1）直接递送的消息（DM）

用户发布内容这种操作也可以被用于直接的消息递送，当然前提是消息接收者是用户 k 的跟随者才行。

$$UserPost(j \to l)_k = SIG_j\left([\text{“”}, k, \text{“dm”}, [PUBK_l(DM_k), H(DM_k)]]\right)$$

DM 除了内容不同外（现在是$[PUB_Kl(DM_k)，H(DM_k)]$），跟普通的帖子并无差别。DM 只会被成功解密的用户 l 接收到，尽管别的跟随者也能接收到该消息，但它们无法对消息进行解密，也感知不到消息的最终接收者是谁。加密采用基于 ECIS 椭圆曲线加密的算法。

（2）用户内容 torrent/tracker 规则

1. 在哈希空间离 ID_{swarm_j} 一定距离内的在线邻居节点需要加入相应的 Swarm 群；

2. 当 ID_{swarm_j} 的邻居从 DHT 网络收到新的内容时，它必须工作为 BitTorrent 网络的一个网关，将内容合并到像文件的归档结构中；

3. BitTorrent tracker 是只读的多值 list 存储，其哈希地址计算如下：

$$ID_{tracker\_j} = H\left([Username_j, \text{“tracker”}, \text{“multi”}]\right)$$

4.用户 j 的跟随者应当加入对应的 swarm 群接收内容的实时更新，为此通过 GET 原语查询 $ID_{tracker\_j}$ 获取初始 Peer 的地址；

5.$ID_{tracker\_j}$ 不同于其它存储值 ,因为它是只读的 ,这可以防止 tracker 攻击，包含 swarm 群成员的隐私。IP 地址的列表通过 swarm 协议获取，这需要 $ID_{tracker\_j}$ 的在线邻居节点加入 swarm 群；

6.Swarm 成员仅能通过 IP 地址知道对方，BitTorrent 不提供关于用户名的任何信息；

7.用户所有内容的哈希不需要，因为内容（包括 DM）都已经签过名能用于验证内容的完整性；

8.产生新内容时增加的 k 值直接通过泛洪的方式在 Swarm 群里广播；

9.Swarm 群的成员间互换拥有的内容列表，成员可以选择只保存或请求最近最新的内容；

10.种子节点是选出来对内容归档的节点；

11.内容发布者(用户 j)可以选择不成为对应 swarm 群的成员(保护隐私，隐藏 IP 地址)；

12 如果发布者选择成为 swarm 群成员，它可以不遵循 ID_{swarm_j} 网关机制，当然这会将自己的 IP 地址暴露；

13.即使发布者成为 swarm 成员，它也可以不担当种子节点；

14.新块产生速率会影响用户发文速度，如果每 10 分钟产生一个新块，平均下来，每天最大可发布 288 篇内容。

4.用户提及机制

如果新内容提及用户 j，客户端也必须向 IDj 发送通知，包含全部的消息内

容，通知通过 DHT 网络进行路由。

提及机制是系统中唯一需要用用户 IDj 而不是用 IDnodej 寻址的功能 ,这有可能暴露用户的隐私信息。一种替代实现机制如下：

$$ID_{mention\_j} = H\left([Username_j, \text{“mention”}]\right)$$

通过哈希的方式隐藏用户名，同时计算出一个新地址用于接收和累计所有 mention， $ID_{mention\_j}$ 的邻居节点也会参与 mention 的存储，提供最大的可靠性和存储性能。这种方法的一个不好地方是用户需要周期地轮询这个地址，判断是否有新的 mention 收到。

提及机制需要客户端的共同协作，如果它不往网络发送通知消息，用户根本不会感知到自己曾被提及。

5.显式消息请求

用户 l 可以不加入 Swarm 群而显式的从用户 j 请求特定的消息，这通过从第二个 DHT 网的地址 $ID_{UserPost\_jk}$ 直接检索相应的内容得以实现，支持“消息向上追溯”功能。

6.向下的消息追溯

向下的消息追溯（比如查询特定内容的回复/RT）相对比较难以解决，一种可能的方案是给多值 list 的某个存储地址发送通知

$$ID_{replies\_jk} = H\left([Username_j, \text{“replies”} + k, \text{“multi”}]\right)$$

存储的值是所有回复的拷贝，这种机制也需要客户端的协同才能工作。

7.哈希标签

如同提及机制，哈希标签在新消息的上下文中进行检测，消息的拷贝被发送到一个特定的多值 list 存储地址：

$$ID_{hashtag_t} = H\left([hashtag_t, \text{“hashtag”}, \text{“multi”}]\right)$$

这与向下消息追溯机制类似，不同之处在于：哈希标签会创建一个新的 Swarm 群，IDhashtagt 的邻居也必须加入这个虚拟的 Swarm，称之为虚拟是因为 Swarm 群不共享任何文件内容，仅用于为想监控该哈希标签的用户实现广播功能。

8.内容搜索

对任意出现内容的搜索可以通过扩展哈希标签的实现，针对出现的内容构建类似机制。为了减小开销和网络传输，必须附加相应的限制，比如对内容大小进行限制、排除介词等。另外，对包含相同内容的内容统一存储到一个临时的多值 list 地址可以显著减少存储开销和降低系统实现复杂度，地址计算如下：

$$ID_{word_w} = H\left([word_w, \text{“word”}, \text{“multi”}]\right)$$

波场（TRON）内容提供安全性、扩展性和隐私特征如下：

1.架构本身提供弹性扩展，没有单个公司、政府或组织能关闭它；

2.分布式用户注册机制类似比特币事务一样安全，提供非中心化的内容认证；

3.为了选择自己喜欢的用户名，用户更踊跃于提早注册；

4.采用通常的用户命名方式，摒弃长的加密哈希，使用户具有更好的使用体验；

5.公钥替代机制允许用户在安全受到威胁时更改自己的键对；

6.具备其它博客系统的主要功能，包括用户名查找、消息追溯、提及、加密消息、哈希标签和内容搜索；

7.通过 DHT 路由实现对特定用户发送通知、请求资源的功能，不管他在线与否；

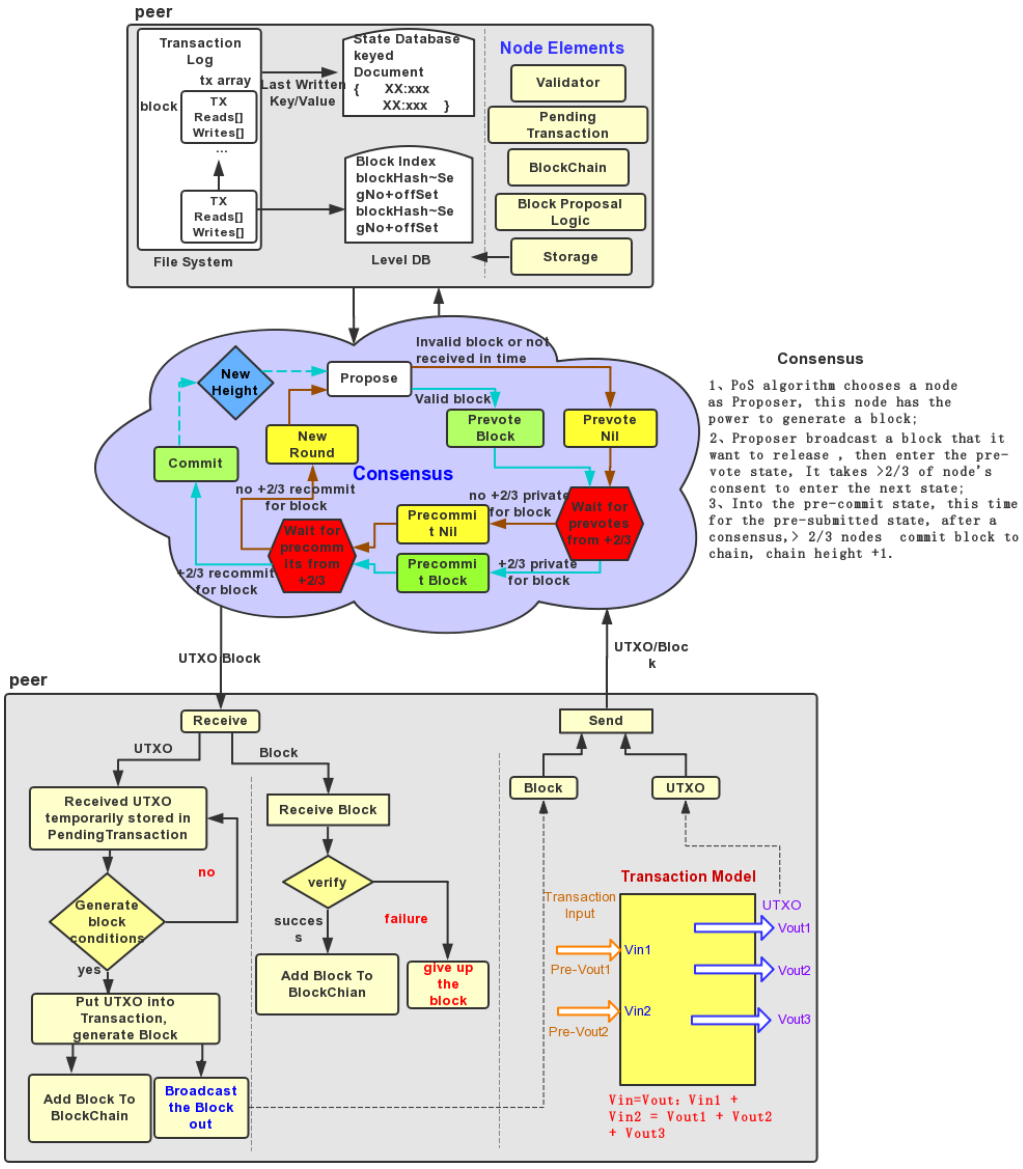
8.架构提供激励机制使参与运行的节点有机会获取发送广播消息的特权；

9.可以通过只读的 web 接口访问用户公开的内容和哈希标签，这并不破坏系统的安全性；

10.对于资源受限的客户端可以进行优化，比如，不存储全部的区块链，仅仅存储块的哈希值。为了搜索特定用户，它们可以询问网络哪个区块包含用户的注册，客户端仅需下载想要的区块而不降低安全性，通过 Merkle 树的部分分支即可验证数据的完整性。

（二）区块链平台

区块链平台的架构图如下：



1.简介

TRON 包含共识引擎、ABCI(Application BlockChain Interface)[2]、UTXO、智能合约等模块。共识引擎是其核心，应用通过 ABCI 与之对接，实现为拜占庭容错的状态机，可以由任意一种编程语言实现。

TRON 区块链平台具有以下特点：

1.可扩展性：TRON 区块链可通过侧链扩容，意味着不仅货币交易，具有法律约束能力的合同及证书、音频视频文件都可储存在区块链的数据库上；

2.去中心化：没有中介机构，所有节点的权利和义务都相等，任一节点停止工作都不会影响系统整体的运作；

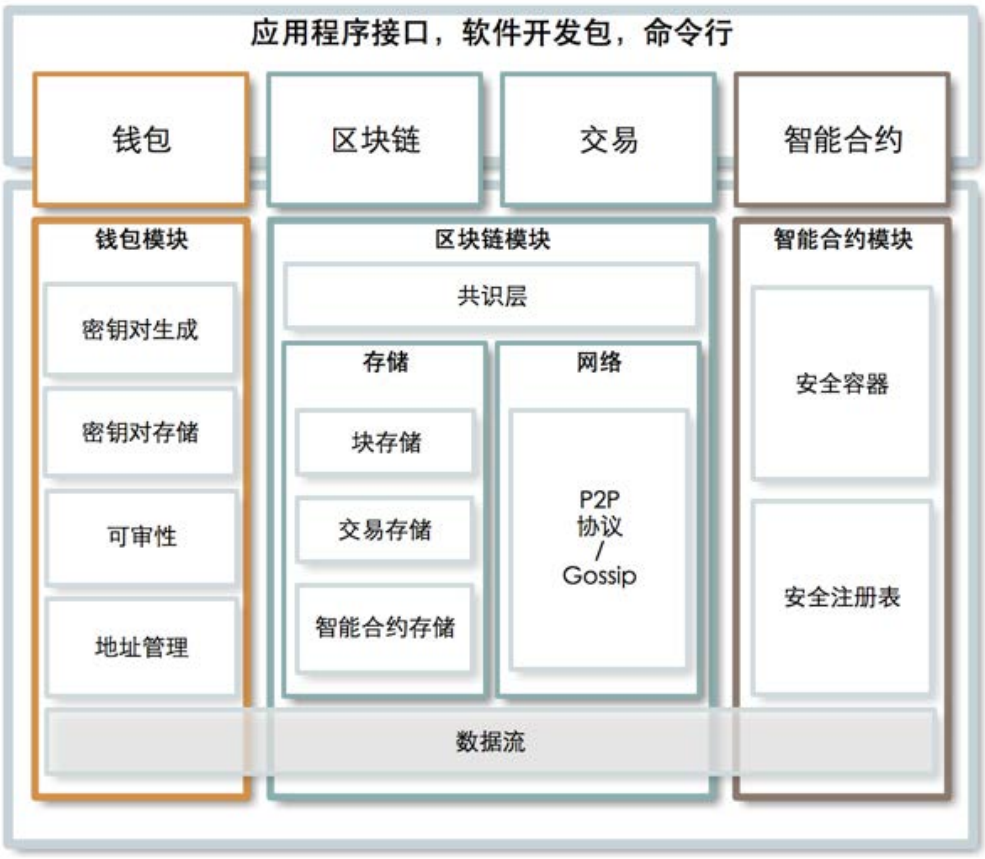
3.非可信环境：系统中所有节点之间无需信任也可以进行交易因为数据库和整个系统的运作是公开透明的，节点之间无法欺骗彼此；

4.一致性：节点之间的数据信息是一致的；

5.容错型：系统能包容 1/3 节点的拜占庭故障；

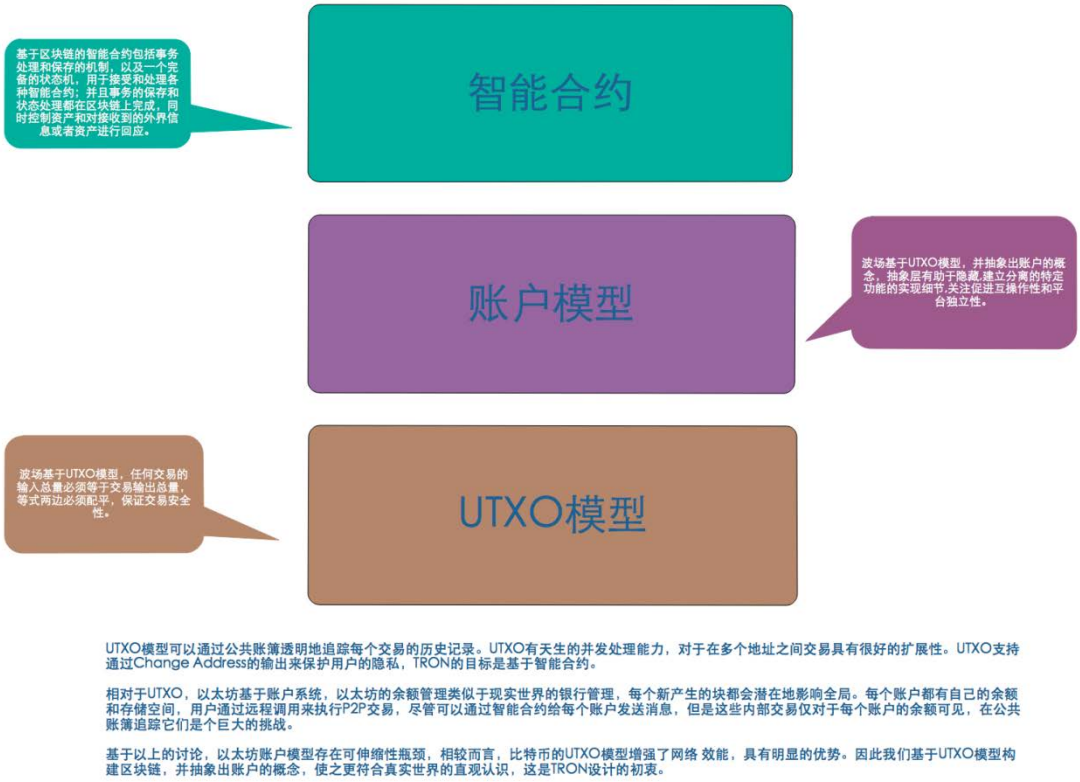
6.扩展性账户模型：UTXO 模型 + Account 抽象。TRON 在采用了 UTXO 易于并行运算的模型前提下，还做了针对性的改进；为了数据易于管理，易于编程，TRON 引入世界状态—轻量级状态树的概念，每一种资产都维持一个全局世界状态，该全局状态具有快速可查找，不可更改，简单易提供证明的特性。

2.软件层次图



软件层次分为两大部分。第一部分为应用程序接口，软件开发包和命令行，主要为外部提供程序调用接口，方便开发；第二部分为模块，包括钱包模块，区块链模块和智能合约模块，同时提供了存储接口，方便各个模块的数据持久化。

3.UTXO

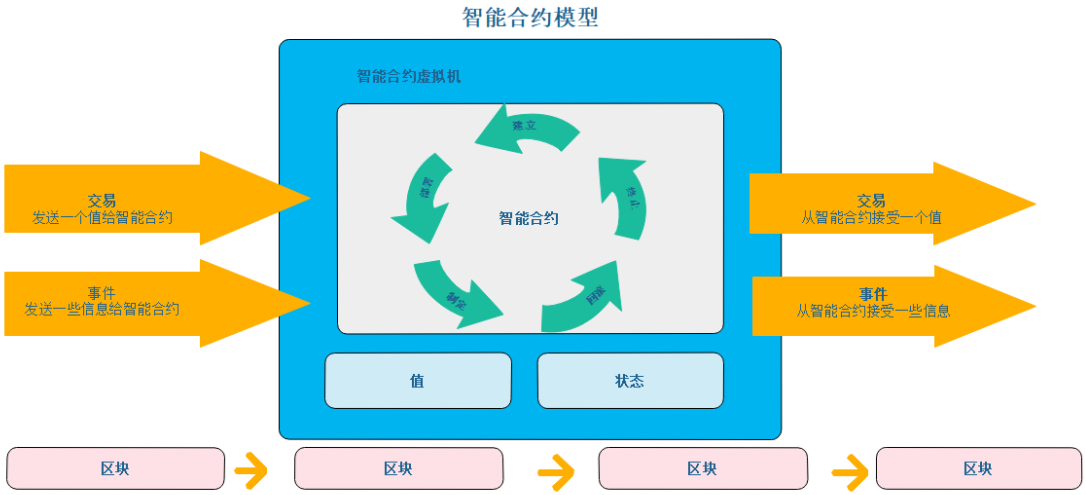


UTXO 模型可以通过公共账簿透明地追踪每个交易的历史记录。UTXO 有天生的并发处理能力，对于在多个地址之间交易具有很好的扩展性。UTXO 支持通过 Change Address 的输出来保护用户的隐私，TRON 的目标是基于智能合约。

相对于 UTXO，以太坊基于账户系统，以太坊的余额管理类似于现实世界的银行管理，每个新产生的块都会潜在地影响全局。每个账户都有自己的余额和存储空间，用户通过远程调用来执行 P2P 交易，尽管可以通过智能合约给每个账户发送消息，但是这些内部交易仅对于每个账户的余额可见，在公共账簿追踪它们是个巨大的挑战。

基于以上的讨论，以太坊账户模型存在可伸缩性瓶颈，相较而言，比特币的 UTXO 模型增强了网络效能，具有明显的优势。因此我们基于 UTXO 模型构建区块链，并抽象出账户的概念，使之更符合真实世界的直观认识，这是 TRON 设计的初衷。

4.智能合约



确定性和可终止性是智能合约的两种性质，在设计智能合约系统的时候，需要想办法把非确定性因素排除在外。

比特币内置了一套脚本引擎，其指令集非常简单且非图灵完备，具有可终止性，因此比特币的智能合约是确定性的。以太坊虚拟机（EVM）是以太坊中智能合约的运行环境，以太坊智能合约的系统函数不是非确定性的，但是合约的调用路径会是非确定性的，会导致一个可扩展性上的重要性能损失，它采用计价器实现可终止性。Hyperledger Fabric[4]智能合约采用了 Docker 作为执行环境。Docker 是轻量级的虚拟化技术，在区块链下 Docker 是一个比较“重”的执行环境，这也是 Fabric 的性能瓶颈所在，目前只能达到每秒几百 TPS，它采用计

时器实现可终止性。

为了兼顾确定性,可终止性以及虚拟机的轻量级和容器方案的编写语言灵活性这些优点，TRON 准备在未来开发轻量级的 TVM（Tron Virtual Machine）作为其智能合约的执行环境，它的启动速度非常快，占用资源也很小。TRON 虚拟机的数据操作指令直接对数组及复杂数据结构提供支持。这些都会提升 TRON 智能合约的运行性能。TRON 网络计划对代币转账和智能合约的运行和存储进行收费，从而实现对记账人的经济激励和防止资源滥用。

未来 TRON 智能合约开发者可以直接使用几乎任何他们擅长的高级语言来进行 TRON 智能合约的开发工作。首批计划支持的语言是 java，Go 等。TRON 计划提供这些语言的编译器和插件，用于将高级语言编译成 TRON 虚拟机所支持的指令集。

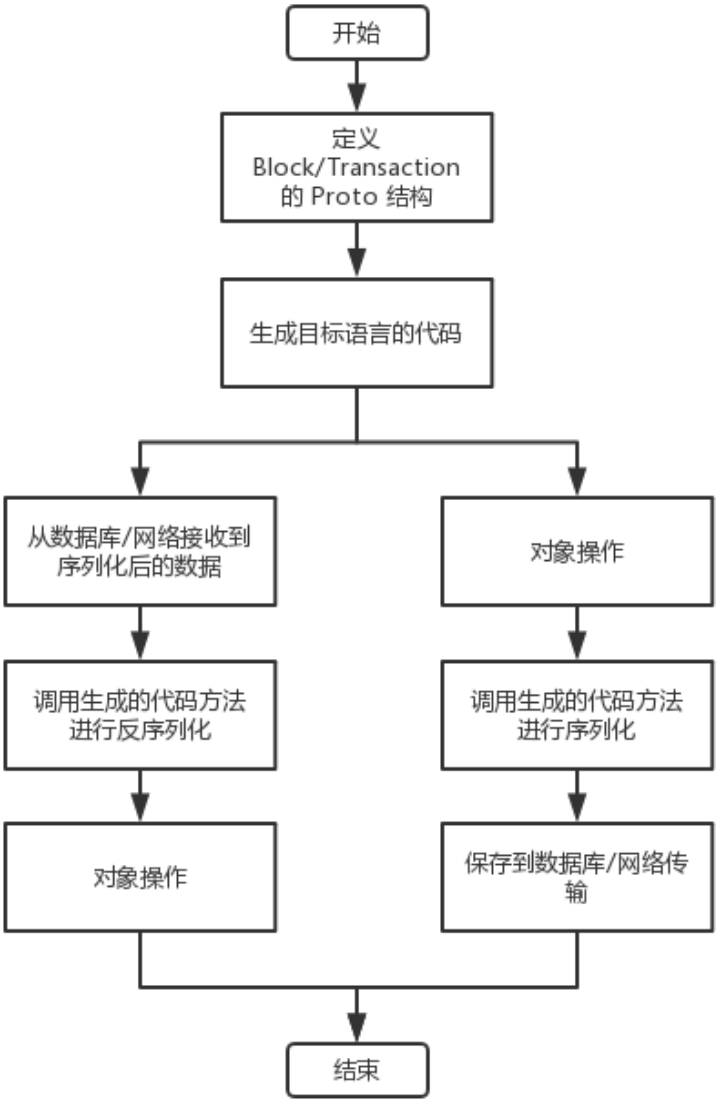
如上图所示是 TRON 的智能合约模型：一段代码（智能合约），运行在智能合约虚拟机上，被部署在分享的、复制的账本（区块链）上，TRON 对智能合约进行了生命周期的管理，分别是：建立，部署，制定，回滚，终止。它可以维持自己的状态，控制自己的资产值和接收到外界信息、交易或者对外界信息、交易进行回应。

5.共识

TRON 的共识采取分三步走的策略，第一步采用基于 Kafka 的技术体制，实现中心化共识算法，目的在于实现系统的联调联试，功能集成；第二步采用基于 Raft 的分布式共识机制，实现了从中心化到分布式的跨越，这一步逐渐完善网络、分发等功能，为最终实现无逻辑中心的广域全分布打下基础；第三步实现 PoS 的共识机制，实现基于 “保证金机制 + epoch 确认”的拜占庭容错共识，

同时兼容 PoS 和 PoW 的集成共识。目前 TRON 的开源代码实现了第一阶段的中心共识算法。第二阶段的分布式共识算法正在开发测试中。

6.基于 Protocol Buffer 的对象编码和序列化



（1）实例

Proto 代码

```
message Block {
      repeated Transaction transactions = 1;
BlockHeaderblockHeader = 2;
}
```

序列化

```
Block.Builder block = Block.newBuilder()
      .setTransactions(transactions)
      .setBlockHeader(blochHeader)
      .build();

byte[] blockData = block.toByteArray();
byte[] keyData = block.getHash();
DB.saveBlock(keyData, blockData);
```

反序列化

```
byte[] keyData = block.getHash();
byte[] blockData = DB.getBlock(keyData);
Block block = Block.parseFrom(blockData).toBuilder().build();
```

（三）P2P 分布式存储系统：TRFS

因特网正处于一个技术推陈出新、快速变革的时期，比特币、以太坊和其它区块链网络已经证明了无中心事务账簿的可用性，这些公共的账簿处理复杂的智能合约应用，交易价值百亿美元的数字资产。这些系统提供因特网级的开放式服

务，参与者形成一个无中心的网络，提供无中心管理的支付服务。波场（TRON）TRFS 是一个基于 P2P 的分布式存储系统，旨在构建一个无中心的存储网，支持上百亿文件跨对等网的共享和传输，彻底改变数据的存储模式，最大化数字信息存储访问的性能。

TRFS 将存储从云模式转变为一个基于算法和规则运作的市场模型。市场以区块链为基础，基于虚拟货币 TRX 进行交易，即通过提供存储从客户端赚取 TRX；相反，客户端花费 TRX 存储和分发数据。类似于比特币，矿工之间竞争挖块获得回报，但 TRFS 其挖矿能力正比于矿工提供的存储空间，提供的是一种对客户端有用的服务（不像比特币，矿工的工作仅对区块链共识有用），这形成一种极强的驱动激励矿工尽可能贡献多的存储空间，租赁给客户端使用。协议将这些资源构建为一个自愈合的存储网络供给外界使用，网络通过复制和分散存储内容实现健壮性，并能自动检测和修复复制错误。客户端可以针对不同威胁程度和级别选择不同的复制参数对数据进行保护，存储网络也提供其它方面的安全保证，比如内容在客户端进行端到端的加密，而存储提供者无法获取相应的解密密钥。

TRFS 由一个多层的协议栈，以模块的方式组合成为一个整体。层间定义了相应的接口标准，包含以下五个层次：

1.名字层 :使用基于 PKI 公钥基础设施进行节点标识，它是公钥的密文哈希。节点存储它的公私钥（私钥通过密码保护）。

2.数据表示层；采用 Merkle[1]有向无环图构建任意复杂的数据结构，无需中心化的写者。其特点是基于内容寻址、对象持久化存储、支持任意数据结构建模、容忍网络分区和合并，它是可信、去中心化、持久的 Web。

3.互换层：负责协调数据的传输，一旦节点之间建立连接，就可以通过互换协议进行内容寻址块的传输和复制。

4.路由层：定位对等节点和对象。服务于两个目的：节点路由（查找别的节点）和内容路由（查找发布到 TRFS 的数据）。路由层定义了一个通用接口，任何满足和实现了该接口的实现都可以接入 TRFS 使用。

5.网络层：在两个波场（TRON）节点间提供点对点可靠或非可靠传输，处理 NAT 穿透（打洞、端口映射和中继），支持加密、签名和多种传输协议（TCP、SCTP、UDP 等），支持连接、流的多路复用。

7.2 技术特点及对比

（一）Bitcoin vs Ethereum vs Tron 整体技术对比

	Bitcoin	**Ethereum**	**Tron**
共识算法	PoW	PoW	PoS 拜占庭共识
交易吞吐量	7 笔/每秒	25 笔/每秒	1500 笔/每秒
块的生产时间	10 分钟	15 秒	15 秒
确认时间	6 块	12 块	1 块
智能合约	简单脚本语言	基于 solidity 语言	多种程序语言
钱包签名算法	ECDSA 椭圆曲线算法	ECDSA 椭圆曲线算法	Lamport 算法
交易模式	基于 UTXO 交易模型	基于账户模型	基于 UTXO 交易模型，加本地缓存账户信息

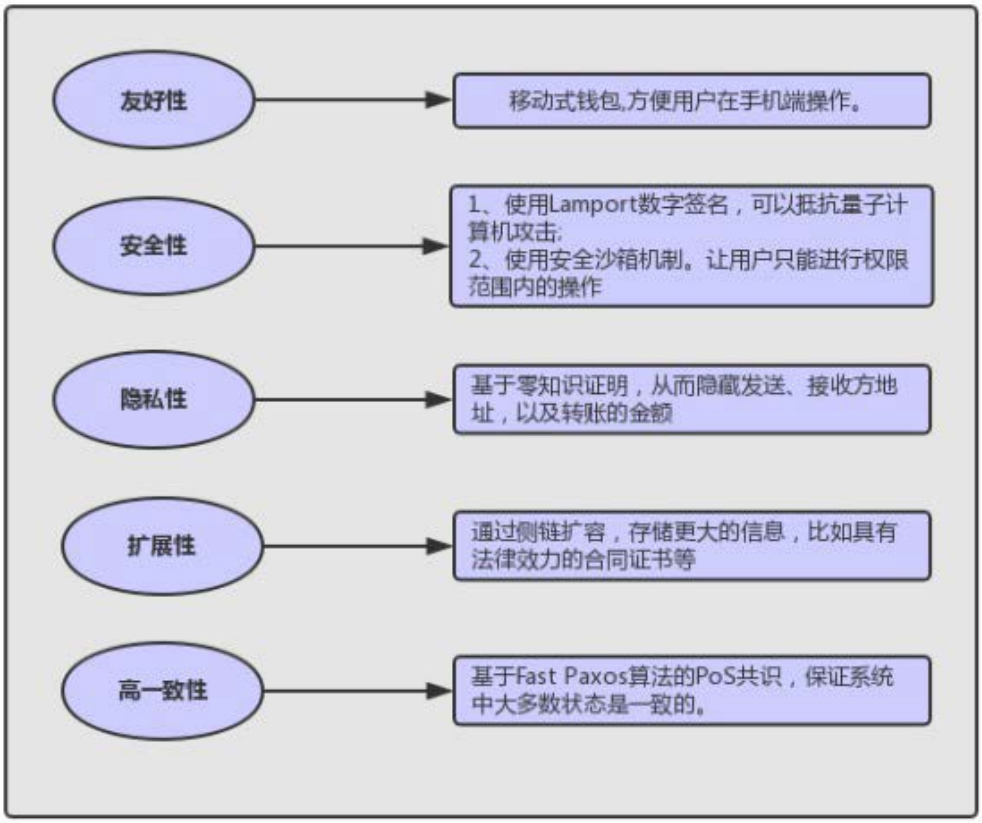
钱包交易平台	PC 端	PC 端	移动端

（二）Bitcoin vs Ethereum vs Tron 安全性技术对比

Bitcoin	**Ethereum**	**Tron**
没有智能合约	EVM 虚拟机没有特权操作检查机制	提供安全沙箱 ,根据用户授权策略对特权操作进行权限检查
ECDSA 椭圆曲线数字签名算法 ,以目前“天河二号”的算力来说 ,产生比特币 SHA256 哈希算法的一个哈希碰撞大约需要 248 年，但随着量子计算机等新计算技术的发展 ,未来非对称加密算法具有一定的破解可能性	ECDSA 椭圆曲线数字签名算法，同 Bitcoin 存在一样的问题	Lamport 数字签名算法 ,能抵抗量子计算机的攻击
PoW 工作量证明，并没有对块达成全局共识 ,只是随着后续块的链接加入 ,降低了链分叉的概率	当前为基于 Ethash 的工作量证明算法，存在类似比特币一样的分叉问题	基于 Fast Paxos 的共识算法变种 ,根据 State 决定 Peer 的投票权重，只要 2/3 节点确认就可对块达成全局共识 ,不存在分叉问题。并且实现上，

		可以根据的业务需求调整 ,同时灵活应用多种共识机制！比如 Pos 和 PoW 的结合
采用 Merkle 树进行数据完整性校验	采用 Merkle Patricia Tree 树进行数据完整性校验	采用 Merkle Patricia Tree 树进行数据完整性校验
基于 Gossip 协议的广播机制	采用基于 Kademlia 的 P2P 网络 ,但数据非存储加密 ,可以追溯数据源头	采用定制化的 P2P 网络，具有数据存储加密、位置透明、源不可追溯性

7.3 技术解决方案



8. 波场（TRON）官方 Token - TRX

波场 TRON 的官方 Token 是 TRONIX，以 TRX 为延伸的，波场中将拥有如下资产类别：

（1）TRONIX

TRONIX 是 TRON 区块链上帐户的基本单位。所有其他代币的价值均从 TRON 价值衍生出来。希望进入或退出 TRON 平台的人必须购买或出售 TRONIX。TRONIX 总量发行为 1000 亿。

（2）TRON Power (TP)

TP 是锁定的 TRON，用户可以将自身的 TRONIX 锁定来获得 TP。TP 本质是具有投票权的 TRONIX，意味着拥有 TRON POWER 的持有者有更高生态权限。

在加密货币的世界里。我们看到短期投机者不断的寻找升值更快的币种进行投资。 波场想要建设一个有长期看好波场的持有者完全控制的生态，我们希望波场能够长期被符合波场价值观的人所控制。

我们将向长期持有 TP 的人奖励更多的 TP，配送比例将是动态分配。这也意味着长期持有并锁定的人会获得奖励。

TRON POWER 余额不可转账，不可出售，意味着 TRON POWER 不可被交易。

对相信的方向长期投入是十分重要的，生态因此可以做更长远的规划，而不因短期利益放弃对理想的追去。同时利益相关者也因为长期发展的增速而享受活力。利益相关者的长期持有会成为生态的标杆，可以更好的引导生态的发展。

（3）TRON 20 TOKEN

内容主体数字资产发行: 内容主体(IP， 个人，团体)可以自由的通过 TRON20 标准发行数字资产，他人则可以通过购买数字资产享受数据贡献者不断发展所带来的利益与服务。

代币(Token)是区块链中定义价值的方式，用于标定金融或数字资产。在 TRON 上，我们建议所有代币使用相同的标准 TRON 20，这样代币之

间的兑换和 DAPP 支持就会变得容易。

在 TRON 区块链上，可以通过社区提供的代码，发型衍生的内容主体数字资产发行。

在 TRON 区块链上的基础，社区也会一定程度支持 DAPP 的发展， 比如去中心化的交易所，预测市场和随机数源等生态项目。

9. 投票与社区治理

区块链投票机制对与系统自我升级至关重要，当协议层改变，生态将决定跟随最长链发展。现有投票机制低效甚至有时达不到大多数投票情况，导致社区决策停滞不前。

TRON 第一个提出混合投票机制，设立两层投票体系，

1. 选举投票

2. 跟随投票

波场（TRON） 节点互相交流，但是可能在不同时间确认交易。区块链需要数列性的统一性，意味着每笔交易的时间顺序必须统一。为了保证每一轮广播的统一性，波场（TRON）的投票系统需要三个步骤：

1. 初准备

当一个用户发出交易申请 ,主节点将会产生发送一个消息给所有的验证节点，并等待回复。

2. 准备

一个验证节点 将审核这条信息。如果 2/3 多数的共识被达成，主节点将会广播交易到下一阶段。

验证节点会有三个反应选项

1) 节点批准交易

2) 节点拒绝交易

3) 节点在没有在规定时间内回复

4) 多次不回复的节点将被驱除

3. 确认

一个验证节点正式向所有验证承诺信息正确。 再次， 如果 2/3 多数的共识被达成，交易将正式完成，区块将会链接上链，并广播到网络内所有节点 。

10. 波场（TRON）预计简要时间表

1. Exudos，出埃及记，数据自由-基于点对点的分布式的内容上传、存储和分发机制，2017 年 8 月-2018 年 12 月

2. Odyssey ,奥德赛 ,内容赋能-经济激励赋能内容生态 ,2019 年 1 月-2020 年 6 月

3. Great Voyage，伟大航程，个人数字资产发行，2020 年 7 月-2021 年 7 月

4. Apollo，阿波罗，价值自由流动-去中心化的个体专属代币交易，2021

年 8 月-2023 年 3 月

5. Star Trek，星际旅行，流量变现-去中心化的博弈与预测市场，2023 年 4 月-2025 年 9 月

6. Eternity，永恒之地，流量转化-去中心化的游戏，2025 年 4 月-2027 年 9 月

11. 合规性

1. 运营主体

波场[TRON]的团队作为蒂姆·伯纳·李爵士(Sir Tim Berners Lee)的信徒,我们确信从协议诞生的第一天开始，它便属于全人类，而并不是一小部分人用来盈利的工具。因此，TRON（波场）在新加坡成立 Tron Foundation，该基金会的主要任务是公开、公正和透明的并且不以盈利为目的运营 TRON 网络，并对 TRON 的开发团队进行支持。

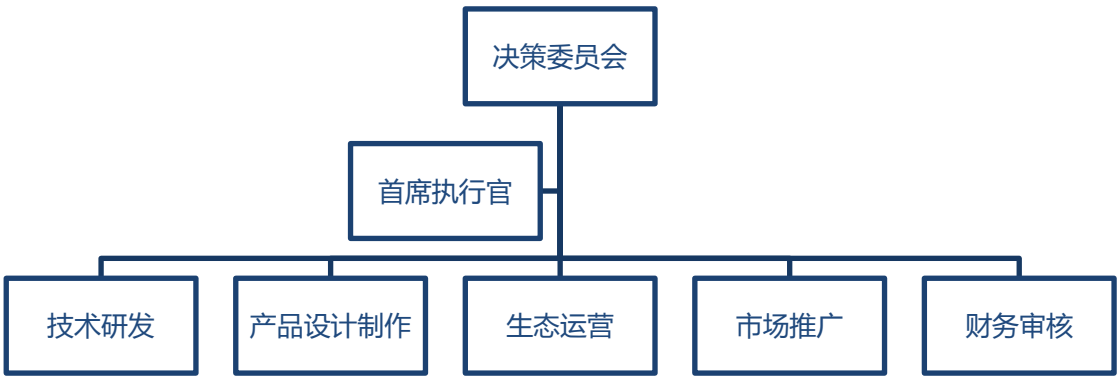
Tron Foundation 由新加坡会计与企业管理局（ACRA）批准成立，受新加坡公司法监管，该基金会由具备受托资格人组成的受托董事会或管理委员会独立管理运营并独立于政府之外。

新加坡以稳定而健全的法律、金融环境著称，Tron Foundation 是在新加坡成立的非盈利组织（Non-Profit Entity），依照新加坡法律，该基金会是为支持或参与公共利益或私人利益的活动，而不具任何商业利益的合法成立的组织。基金会所获得的“利润”被称为盈余，将被继续保留作为其他活动的经

费，而不在其成员中分配利润。

2. 治理结构与投票

为使Tron Foundation在公开、公正、透明的前提下合理利用基金会的资金、资源，不断推进波场 TRON 协议的快速发展，扩展 TRON 协议的应用场景，吸收更多机构、公司、组织进入开源的波场 TRON 生态，基金会设立了三层的组织架构如下：



· 决策委员会

决策委员会是 TRON Foundation 的最高决策机构，承担最终决策职能，决策委员会委员无职位高低之分，负责对基金会战略规划、年度计划、预算等重大事项进行审议和审批，并代表基金会对波场协议的生态重大议题做出表决。

· 首席执行官

首席执行官由决策委员会票选产生，对决策委员会负责。首席执行官将全面组织实施决策委员会的有关决议和规定，负责 TRON 的日常运营，全面完成其下达的各项指标，并定期将实施情况向其汇报。首席执行官有权组建必要的职能部门，组聘管理人员，负责统筹技术研发、产品设计制作、生态运营、市场推广、财务审核等五个部门的业务，形成一个以其为中心的组织、管理体系。

· 技术研发部门

技术研发部门负责底层技术的开发和审核工作，是基金会的基础部门。为确保团队内部保持信息互通，步调一致，技术研发部门应与其他部门（特别是产品设计制作部门）互通信息，及时调整沟通项目细节，确定下一阶段的研发方向。

· 产品设计制作部门

产品设计制作部门负责为技术部门提供的产品框架进行充实完善，建立可持续的具体发展策略，包括进行市场调研、对产品功能进行统筹，并承担 TRON 的 UI 设计、图像设计等工作。成员需要时刻了解社区的动态、热点和反馈，与代币持有者积极进行沟通，并不定期地举办技术交流会等活动。

· 生态运营部门

在技术和产品部门提供的基础上，生态运营部门负责“一外一内”——首先，将工作向深处延伸，积极开拓合作伙伴，将 TRON、终端用户、合作伙伴紧密地联系在一起，从而打造开放式、分布式、保护隐私的全球娱乐生态链；

其次，构筑社区内部生态圈，形成一个良性互动、信息自由流动且充分对称的用户社区。

· 市场推广部门

市场推广部门负责推广 TRON 的核心或衍生产品和服务，职责包括但不限于联系媒体合作、进行广告宣传、设计用户互动等工作。该部门将与生态运营部门展开紧密合作，根据合作伙伴、终端用户的要求制定最恰当的宣传方案。

· 财务部门

财务部门负责管理全公司的财务事宜，具体包括资金管理、会计核算、成本控制等方面的工作内容。同时，由于数字资产项目有较高的风险，本部门还负责风险管控业务，将配合其他部门对项目的经营与财务风险进行分析评估。在审计方面，鉴于数字资产与代币本身的特殊性，现有制度难以对其进行有效的监管。决策委员会将会聘请具有相关经验的专业审计从业者，确保 TRX 使用的公开透明。

12. 团队简介

创始人兼首席执行官 | 孙宇晨（Justin Sun）

先后毕业于北京大学本科和美国常春藤盟校宾夕法尼亚大学，硕士学位。中国最大的声控声优社区陪我 APP 创始人，早期加入 Ripple，曾任 Ripple 大中华区首席代表。2015《福布斯》中国 30 位 30 岁以下创业者、2017《福布斯》亚洲 30 位 30 岁以下创业者，2014 达沃斯论坛（世界经济论坛）全

球杰出青年。马云湖畔大学首期唯一 90 后学员。Ripple 币值超百亿美金，陪我 APP 注册用户超过 1000 万，月活用户突破 100 万。

技术负责人 | 陈志强（Lucien Chen）

曾任职网易有道，腾讯，奇虎 360 ，神马搜索（阿里 P8+）等一线互联网企业。在大数据，广告算法，DMP 系统、BT 系统和 CTR 平台等有丰富的经验，具有亿级系统架构的开发能力，对高并发系统框架设计有丰富经验，在团队管理、战略规划和业务统筹方面都有丰富的实战经验，同时，在密码学方面也有着极深的造诣，也是比特币 Bitcoin 的早期支持者和投资者。

技术总监 | 杨凯山

毕业于清华大学计算机系，学士学位。拥有 15 年以上的前后端工作经验，先后就职于亚太地区领先的企业管理软件、企业互联网服务和企业金融服务提供商用友以及中国领先的高速公路监控系统解决方案中交远洲信息技术（北京）有限公司。杨凯山在系统前端和后端均有极深的造诣，自 2013 年起便密切关注区块链领域的技术发展。

资深后端工程师 | 霍冬冬

计算机专业，学士学位。资深后端工程师，曾任拉美地区最大的新闻资讯应用之一 InstNews 和东南亚地区领先的新闻资讯应用 VnNews 后端技术负责人，在平台安全、高并发处理方面经验丰富，2015 年开始深度关注区块链领域技术发展。

产品总监 | Deuce Yu

先后就职于中国 SNS 社交的两大领先平台，开心网与人人网，在开心网时任社交游戏部产品经理，负责当时最风靡的网页端“偷菜类”社交游戏以及开心手机端自有游戏研发推进；之后供职于人人网，任游戏开放平台运营主管，负责开放游戏平台游戏接入、联运以及定制手机端游戏开发推进。自 2015 年起关注区块链领域，全面统筹波场（TRON）协议娱乐平台与协议的对接流程和表现形态。

运营总监 | 张晨

社群实操专家。曾任优雅 Space 联合创始人兼 COO、优雅 Space 芝加哥分院秘书长、在行行家、《社群商业》一书编委。10 万高端女性社群构建及运营者，领域覆盖了女性、培训、留学、基金、投资、互联网等 10 多个方面，变现千万余元。曾被北京大学、随行付、中建华通、互联网运营机构等邀请讲课百余次，2016 年起关注区块链领域。

13. 风险提示

- 系统性风险：是指由于全局性的共同因素引起的收益的可能变动，这种因素以同样的方式对所有证券的收益产生影响。例如政策风险——目前国家对于区块链项目以及 ICO 方式融资的监管政策尚不明确，存在一定的因政策原因而造成参与者损失的可能性；市场风险中，若数字资产市场整体价值被高估，那么投资风险将加大，参与者可能会期望 ICO 项目

的增长过高，但这些高期望可能无法实现。同时，系统性风险还包括一系列不可抗力因素，包括但不限于自然灾害、计算机网络在全球范围内的大规模故障、政治动荡等。

- 监管缺场风险：包括 TRX 在内的数字资产交易具有极高不确定性，由于数字资产交易领域目前尚缺乏强有力的监管，故而电子代币存在暴涨暴跌、受到庄家操控等情况的风险，个人参与者入市后若缺乏经验，可能难以抵御市场不稳定所带来的资产冲击与心理压力。虽然学界专家、官方媒体等均时而给出谨慎参与的建议，但尚无成文的监管方法与条文出台，故而目前此种风险难以有效规避。

- 监管出台风险：不可否认，可预见的未来，会有监管条例出台以约束规范区块链与电子代币领域。如果监管主体对该领域进行规范管理，ICO 时期所购买的代币可能会受到影响，包括但不限于价格与易售性方面的波动或受限。

- 团队间风险：当前区块链技术领域团队、项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。TRON 项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、愿景规划等方面挂钩，也受到市场上诸多竞争者乃至寡头的影响，其间存在面临恶性竞争的可能。

- 团队内风险：TRON 汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链领域的资深从业者、具有丰富经验的技术开发人员等。作为中国地区区块链技术领域的领头羊角色，团队内部的稳定性、凝聚力对于 TRON 的整体发展至关重要。在今后的发展中，不排除有核心人员离开、

团队内部发生冲突而导致 TRON 整体受到负面影响的可能性。

- 项目统筹、营销风险：TRON 创始团队将不遗余力实现白皮书中所提出的发展目标，延展项目的可成长空间。目前 TRON 已有较为成熟的商业模型分析，然而鉴于行业整体发展趋势存在不可预见因素，现有的商业模型与统筹思路存在与市场需求不能良好吻合、从而导致盈利难以可观的后果。同时，由于本白皮书可能随着项目细节的更新进行调整，如果项目更新后的细节未被 ICO 参与者及时获取，或是公众对项目的最新进展不了解，参与者或公众因信息不对称而对项目认知不足，从而影响到项目的后续发展。

- 项目技术风险：首先，本项目基于密码学算法所构建，密码学的迅速发展也势必带来潜在的被破解风险；其次，区块链、分布式账本、去中心化、不同意篡改等技术支撑着核心业务发展，TRON 团队不能完全保证技术的落地；再次，项目更新调整过程中，可能会发现有漏洞存在，可通过发布补丁的方式进行弥补，但不能保证漏洞所致影响的程度。

- 黑客攻击与犯罪风险：在安全性方面，单个支持者的金额很小，但总人数众多，这也为项目的安全保障提出了高要求。电子代币具有匿名性、难以追溯性等特点，易被犯罪分子所利用，或受到黑客攻击，或可能涉及到非法资产转移等犯罪行为。

- 目前未可知的其他风险：随着去快链技术与行业整体态势的不断发展，TRON 可能会面临一些尚未预料到的风险。请参与者在做出参与决策之前，充分了解团队背景，知晓项目整体框架与思路，合理调整自己的愿

景，理性参与代币众筹。

14. 免责声明

- 本文档仅作为传达信息之用，文档内容仅供参考，不构成在 TRON 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。
- 本文档内容不得被解释为强迫参与 ICO。任何与本白皮书相关的行为均不得视为参与 ICO，包括要求获取本白皮书的副本或向他人分享本白皮书。
- 参与 ICO 则代表参与者已达到年龄标准，具备完整的民事行为能力，与 TRON 签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对 TRON 进行了清晰必要的了解。
- TRON 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。TRON 明确表示，概不承担参与者因(i)依赖本文档内容、(ii)本文信息不准确之处，以及(iii)本文导致的任何行为而造成的损失。
- 团队将不遗余力实现文档中所提及的目标，然而基于不可抗力的存在，团队不能完全做出完成承诺。
- TRX 作为 TRON（波场）的官方代币，是平台发生效能的重要工具，并不是

一种投资品。拥有 TRX 不代表授予其拥有者对波场(TRON)平台的所有权、控制权、决策权。TRX 作为在 TRON 中使用的加密代币，均不属于以下类别：(a)任何种类的货币；(b)证券；(c)法律实体的股权；(d)股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

- TRX 的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值，团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。
- 在适用法律允许的最大范围内，对因参与众筹所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，本团队不承担责任。
- TRON 平台遵守任何有利于 ICO 行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确。
- TRON 平台明确向参与者传达了可能的风险，参与者一旦参与 ICO 众筹，代表其已确认理解并认可细则中的各项条款说明，接受本平台的潜在风险，后果自担。

15. 联系方式：

官方网站：tron.network

电子邮箱：service@tronlab.com

16. 参考文献：

[1] Merkle tree: https://en.wikipedia.org/wiki/Merkle_tree

[2] ABCI: https://github.com/tendermint/abci

[3] Petar Maymounkov and David Mazières. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric.

[4] hyperledger : http://www.hyperledger.org/