

WHITE PAPER V1.0



基于SDAG的去中心化分层区块链网络技术白皮书

TOS ThingsOperatingSystem

Decentralized layered block network Technology based on SDAG

ABSTRACT

摘要

在白皮书中我们分析，TOS 链是一种用于物联网 IOT 行业基于 SDAG 的去中心化分层区块链网络技术。该技术自动分发海量交易数据到分层区块链网络，以减少全网区块链数据容量，将是区块链技术的下一步发展。

首先概述了 TOS 的远景，该项目计划分三阶段推进：

- 1) TOS 物联网底层公有链完成；
- 2) 供可定制物联网区块链解决方案的开源平台；
- 3) 对大型智能硬件厂商提供统一协议标准；

TOS 的核心技术 SDAG 协议，在保证安全的同时提高了交易速度，后文重点对这种快速又安全的物联网公有链进行了详细分析。本白皮书列举了一些现有物联网技术所面临的难题及其自身局限性，并给出了 TOS 对于目前物联网区块链的解决方案。还介绍了 TOS 的技术规范，并简要讨论了 TOS 及其在项目中的实施情况。

KEY WORDS

关键词

SDAG、物联网、分层区块链网络、TPoS、免费交易、付费交易，密码经济学平衡、TVM 虚拟机、智能合约



- (一) INTRODUCTION 引言
- (二) PROFESSIONAL GLOSSARY 专业名词解释
- (三) DISCUSSION OF EXISTING BLOCKCHAIN TECHNOLOGIES 现有的区块链技术讨论
 - Throughput 交易吞吐量
 - Latency 延迟
 - Size and Bandwidth大小和带宽
 - Security 安全性
 - Usability 可用性
 - Wasted Resources 浪费资源
 - Versioning, Hard Forks, and Multiple Chains 版本控制、硬分叉和多链
- (四) INTRODUCTION OF TOS TOS 基于 SDAG 的去中心化分层区块链网络技术介绍
 - 区块信息摘要
 - 权重及相关概念
 - TPoS-Transaction 交易证明
 - TPoS-PoS 权益证明
- (五) CORE GOALS TOS 核心技术 SDAG 的工作模式
 - SDAG网络特点
- (六) TECHNOLOGICAL INNOVATION TOS 技术架构图&技术创新
 - TOS 技术创新
- (七) TOS TECHNOLOGY ADVANTAGES IN IOT APPLICATIONS TOS 在物联网应用中的技术优势
 - 分层区块链网络
 - TPoS 共识
 - TVM 虚拟机
 - 减少冗余交易
- (八) APPLICATION SCENE TOS 的应用场景
 - 企业级智能硬件平台
 - 物联网大数据交易平台
 - 智能金融服务平台
 - 智能物流平台
- (九) TOS COMMUNITY FOUNDATION TOS 社区基金会
 - TOS 社区基金会的设立
 - TOS 基金会的治理架构
 - TOS 基金会的交易安全
 - 审计
- (十) TOS CORE TEAM TOS 核心团队和专家顾问
- (十一) BUDGET ALLOCATION TOS 数字通证分布与预算分配
- (十二) ROAD MAP 开发工作路线图
- (十三) DISCLAIMER 免责声明
- (十四) REFERENCES 参考文献

(一) INTRODUCTION

引言

“cash, after millennia as one of mankind’s most versatile and enduring technologies, looks set over the next 15 years or so finally to melt away into an electronic stream of ones and zeros.”

“现金，作为几千年来人类最通用、最长久的发明之一，在未来 15 年左右的时间里，将最终融化为一串 0 和 1 组成的电子流。”

——The Economist (2007)《经济学人》(2007)

在当今手机电子银行的世界里，钱正从一种攥在手里、看得见摸得着的东西，变化成互联网上一串串跳动的数字。在这样的背景下，一种存在于加密字符串代码中、被称为“加密货币”的新的货币形式应运而生。这场数字货币的革命始于 2008 年，当时还不知名的中本聪（Satoshi Nakamoto）发布了比特币白皮书。

现在，几乎每天都有新的加密货币诞生，而它们都有一个共同点：底层技术架构都是——区块链。

区块链本身就是一个共享公共账簿，记录并维护着系统上的所有交易记录——从第一个区块问世一直到此时此刻。这个被称为区块链的账簿由一个个链接在一起的块构成，其中每个区块都包含了一定数量在特定时间被网络验证的交易。

物联网是新一代信息技术的重要组成部分，其英文名称是：“Internet of things”。顾名思义，物联网就是物物相连的互联网。这有两层意思：

其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；

其二，其用户端从电脑手机延伸和扩展到了任何物品与物品之间，进行信息交换和通信。物联网就是“物物相连的互联网”。

物联网正在改变我们的生活，也可以看出来它的真正潜力仍然未被大范围开发，但还有很多安全技术效率等方面问题限制着行业的发展。

而区块链作为目前全世界认为最有潜力、最具想象力的一种技术革新。拥有去中心化、不可抵赖、不可篡改、安全及不可逆等基本属性。我们将如何使区块链技术融入到物联网中呢？

本项目将推出一种新的物联网区块链技术，叫做 TOS，旨在解决现有区块链技术所面临的一些难题。本白皮书重点介绍了 TOS 需要解决的问题、项目本身的目标、TOS 如何克服现有区块链的局限以及 TOS 的技术规范。

TOS 是一种用于物联网 IoT 行业基于 SDAG 的去中心化分层区块链网络技术。该技术结合了区块链账本和有向无环图两种技术，具有良好的拓展性。实现自动分发海量交易数据到分层区块链网络，以减少全网区块数据冗余，解决物联网行业海量数据存储问题；用户可以根据数据的价值高低决定使用免费或付费交易，达到密码经济学的平衡；开源和去中心化的网络协议降低了加入智能物联网协议（区块链+物联网）的经济门槛，创建一个跨越品类、跨越地域的智能物联网协议生态圈。

(二) PROFESSIONAL GLOSSARY

专业名词解释

区块：TOS 中区块是只包含一笔交易数据的"特殊区块"；

区块网络：基于 DAG（有向无环图）技术，把一个个区块构建成一个纠缠的网状结构；

创始区块：TOS 网络中第一笔交易生成的区块；

创始区块网络：包含创始区块的区块网络；

高层：根据离创始区块网络远近关系，相对近的区块网络层，创始区块网络层是最高层区块网络；

低层：根据离创始区块网络远近关系，相对远的区块网络层；

父区块网络：当前区块网络的上一层区块网络；

父层：同父区块网络；

子区块网络：当前区块网络的下一层区块网络；

子层：同子区块网络；

末区块网络：没有子区块网络的区块网络；

末层：同末区块网络；

分层：在当前的区块网络分离出一个新的子区块网络，子区块网络与当前区块网络形成一个依附关系；

TPoS：把 Transaction 与 PoS 这两种共识结合，在不同的阶段分别为 TOS 网络工作的技术方案；

未验证区块：从未被其他区块验证的区块；

高度：创世区块至当前区块的所有路径中最长路径的长度；

深度：当前区块到未验证区块的所有路径中最长路径的长度；

权重：区块的权重，与发送这笔交易的节点所投入的工作量成正比；

总权重：当前区块的高度里面包含的所有区块权重的总和；

交易自身验证：交易者自身发起一笔交易，通过 Transaction 共识验证；

免费交易：用户交易不需要支付矿工费；

付费交易：用户交易需要支付矿工费；

(三) DISCUSSION OF EXISTING BLOCKCHAIN TECHNOLOGIES

现有的区块链技术讨论

为方便讨论，我们将重点说一说迄今为止最为广泛使用和研究的区块链技术应用的代表——比特币和以太坊。

Yli-Huoma 等人的研究成果可以用作检验区块链技术的重要参考。其中总结了近期区块链技术的进展，并指出了区块链系统固有的局限性。虽然他们的研究完全集中在讨论比特币的文献上，但这一发现在我们的讨论中也同样适用，其中一些关键指标来自于 Swan。

研究指出了现今区块链系统的七大局限性：

- Throughput 交易吞吐量
- Latency 延迟
- Size and Bandwidth 大小和带宽
- Security 安全性
- Usability 可用性
- Wasted Resources 浪费资源
- Versioning, Hard Forks, and Multiple Chains 版本控制、硬分叉和多链

Throughput 交易吞吐量

典型的区块链（如比特币）需要 10 分钟或更长的时间来确认交易，平均交易速率约为每秒 4 个交易，最高可达每秒 7 个交易。以太坊每秒可以处理 10 个或更多交易，确认时间也比在比特币网络上快 10 倍。然而对比 VISA 交易网络，就能清楚看出当前区块链交易吞吐量的局限性：VISA 可在几秒钟内确认交易，平均每秒处理 2000 个交易，每秒交易量最高可达 65000 个。从这些指标可以看出，与传统的中心化支付网络（如 VISA）相比当今使用最多的区块链网络的交易吞吐量也还存在着很大的差距。限制区块链网络交易吞吐量的主要因素是节点间的延迟。人们虽然已经做出一些积极的尝试，并试图解决这个问题，比如比特币所采用的闪电网络，以及已经作为一个微版本在以太坊区块链上运行的雷电网络等，但就一个可行的长期解决方案各方还没有达成共识。

Latency 延迟

如上所述，因为网络的最大交易吞吐量受到节点间延迟的限制，延迟也就成为了区块链的限制因素。如果节点之间存在较高的延迟，矿工则更有可能是旧块上进行采矿。在比特币网络上，一个块同步到 50% 的节点的平均时间不到 2 秒，同步到 90% 的节点大约需要 13 秒（截至 2017 年 4 月）。而在以太坊上，同步到 50% 的节点的平均时间小于 1 秒，同步到 90% 的节点大约在 10 秒内。对于比特币来说，出块时间与网络同步时间的比值很大，说明节点间的延迟尚不构成一个大的限制因素，而以太坊的出块间隔时间较短，在同步上耗费过多时间就会更有问题。不过以太坊采用了基于 GHOST 协议的算法来激励矿工在最长的链上进行采矿，而不是试图使用由于高延迟和低间隔时间产生分链。

Size and Bandwidth大小和带宽

在讨论大小和带宽时，必须考虑到两个问题：整个区块链的物理数据的大小，以及通过网络发送的单个块的大小。根据要求，作为一个能挖出新块并与区块链网络交互的完全节点，必须保留一份完整区块链的本地副本。很显然，对保留这份副本的存储空间大小的要求是与链上的区块数量成正比的，这就有可能导致中心化，因为如果区块链变得足够大时，将只有少数几个节点有能力进行块的操作。此外，当交易量开始突破可用带宽的限制，再加上块容量大小的限制，矿工费会显著增加，为了达到更大的吞吐量，这可能需要修改核心协议，获得更大的块容量或更短的块确认时间。面对这种情况，必须进行核心协议的修改，但是导致的硬分叉通常又是很难接受的。

Security 安全性

工作量证明（PoW）区块链的最大卖点就是技术上很难被破解。攻击者若想要修改已经出现在区块链上的块，他们需要重做该块以及后续所有块的工作量证明。为了实现这样的攻击至少需要全网51%的哈希算力，因此也称为“51%攻击”。而这显然不太可能发生，因为拥有 51%的算力所产生的采矿收益远比用来攻击获得的收益大。

Usability 可用性

在比特币区块链上，大约每十分钟就会打包交易生成区块，但是之后通常需要等待 50 分钟甚至更久来进行后续对交易的确认。这就类似于在现实世界中，从商店买了东西，却要等待一个小时排队付款。对于一个希望在真实世界中实时应用的程序，这显然是不可接受的。

Wasted Resources 浪费资源

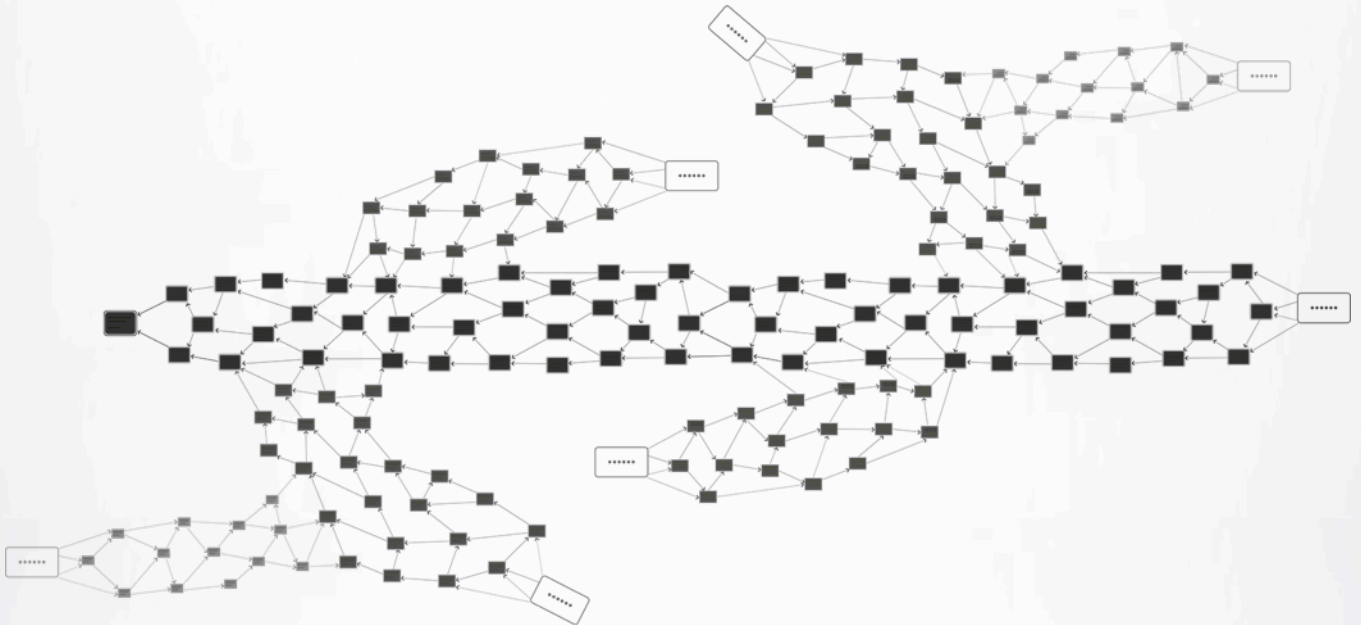
比特币对电力乃至环境的影响相当大。按照现在的估计，验证一笔交易需要 249 千瓦时的电力，比特币区块链上的矿工每年要消耗 32 太瓦时的电力来持续不断地开采出新的块。虽然相对来说以太坊消耗电力较低，但其能量消耗对环境的影响仍然很大。实际上，如果将维持比特币和以太坊正常运作的电力加起来，足以为新西兰供一年的电力。目前已经有有人试图改变工作量证明（PoW）的区块链，取而代之的是权益证明（PoS），以太坊就是其最突出的支持者。

Versioning, Hard Forks, and Multiple Chains 版本控制、硬分叉和多链

区块链分叉带来的主要问题是共识机制和安全性的缺失。举两个极端的例子，一边是一个严重膨胀、占用了地球 100%的可用算力的区块链，另一边是 100 个互相竞争的链，各自拥有 1%的可用算力。硬分叉通常是由于共识机制被破坏导致的另一种不太受欢迎的结果。区块链会因其生态系统中不同干系人的不同意识形态产生分裂，或分叉链。比较著名的例子有因为比特币的扩展问题致使其不能成为一种便捷廉价的电子现金，从而分裂出比特现金（BCH），以及以太坊经典（ETC），也是从以太坊区块链中各种意识形态不一致，无法达成共识的基础上分裂而来。不过硬分叉并不总是因为意识形态的分裂，很多时候也来自区块链系统核心协议的变更，比如以太坊 2017 年的大都会升级。硬分叉形成后，原链上的哈希算力仍然存在。但是在无法达成共识分裂产生的硬分叉中，哈希算力被分给两条互相竞争的链，使得链安全级别都降低了且易受到攻击。

(四) INTRODUCTION OF TOS

TOS 基于 SDAG 的去中心化分层区块链技术介绍



SDAG 超级有向无环图 (Super directed acyclic graph), SDAG 是基于现有的 DAG 技术, 在 Transaction 共识的基础上增加 PoS 权益证明结合为 TPoS 共识, 再通过 S-mechanisms(Smart miner fees regulatory mechanisms)机制与 B-algorithm(Block chain network economic algorithm)算法, 构建分层区块纠缠网络。每个层级的区块链网络存储对应的数据, 类似国家->省->市->县->区, 每个行政中心各自管理数据。把全网的区块数据作分离, 这样不同的省之间, 不需要关心别的省的数据。同理, 不同国家之间也不需要关心对方的数据。可以减少大量的数据冗余。每个地区只关心各自需要的区块数据。并且增加 TVM 虚拟机及 Transaction 和 PoS 管理合约, 构建 SDAG 的智能合约。最终 SDAG 可以做到, 用户能根据数据的价值高低决定使用免费或付费交易。是一个特殊的去中心化系统, 他结合了两种技术, 区块链账本与有向无环图。因此包含了两种不同的共识, 它们分工有序且数据保持同步, 缺一不可。

区块信息摘要

我们定义，网络系统中的所有区块都包含一个区块头，里面包括一个有效 JSON 数据格式

```
{  
  "parentblockhash": "00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09",  
  "previousblockhash": "0000000008e647742775a230787d66fdf92c46a48c896bfbcb85cdc8acc67e87d",  
  "hash": "00000000a2887344f8db859e372e7e4bc26b23b9de340f725afbf2edb265b4c6",  
  "hashMerkleRoot": "00000a83b83by22aa86832dwu4a4uh42ewa456b5e3282aue5so23dt356aa6f3f",  
  "transactioncost": "0",  
  "totalweight": "12",  
  "weight": "1"  
}
```

其中，parentblockhash 是区块的父区块网络 hash 值，previousblockhash 是区块的上一个区块 hash 值，hash 是当前区块的 hash 值，hashMerkleRoot 是交易默克树根节点 hash 值，transactioncost 是交易费用，totalweight 是区块总权重值，weight 为区块中交易数量权重和值。

权重及相关概念

我们定义，每个区块有自身权重、区块总权重及其相关概念。区块的权重与发送这笔交易的节点所投入的工作量成正比。每发送一笔交易会生成一个新区块，在网络系统中自动标记为未验证区块，并带上一个初始的权重值。当交易者自身参与网络中使用 Transaction 工作证明时，如果证明验证完毕，则新区块的总权重值为被验证的直接间接节点的总权重值加上最新的区块权重值。区块链节点的设计保证了去中心化全球数据库中数据的安全、可信与不可篡改。区块链新节点添加，需要网络中的区块链节点审核。收拢 DAG 数据结构，使之不会一直发散下去。TOS 节点通过 TPoS 共识验证算法，达成共识实现快速交易。解决了传统区块链结构中产生分片的无序区块之间的双重支付、与数据篡改的问题，解决了因发现分片不及时可能导致的大量交易最终无效的问题。

TPoS-Transaction 交易证明

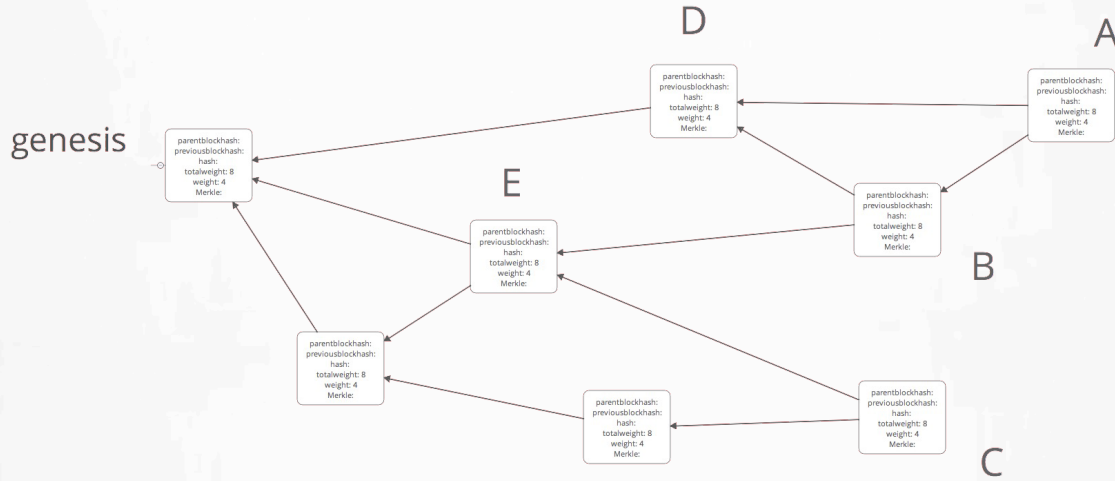
我们定义，每笔交易者自身可以通过验证区块链网络中两个末端未被验证的区块，以生成的新区块并串联起之前的两个末端区块证明交易的有效。基于诚实节点不会直接或者间接地验证具有冲突的区块，那么随着交易的数量增加，当前区块会被越来越多的新区块直接或间接的交易自身验证，系统就会就趋向于安全稳定，换句话说就是一个交易被双花是极为困难的。Transaction 交易证明是由交易者自身验证，此过程中并不需要支付费用，所以 Transaction 验证生成的新区块 transactioncost 为 0。通过 TOS 的节点来接收交易，并将交易数据记录到区块链上，使区块链产生新的区块。TOS 节点在进行交易验证时，先通过 B-algorithm 算法监测区块链网络经济价值，再根据 S-mechanisms 机制选择 Transaction 或 PoS 进行初步验证，迅速完成交易，经全网达成共识后延伸在 TOS 区块链网络中。

TPoS-PoS 权益证明

我们定义，节点可以用数字货币为担保，通过共识算法参与虚拟挖矿用来验证交易数据产生新的区块。此过程中交易需要支付费用，所以 Transaction 验证生成的新区块 transactioncost 为大于 0。因为矿工付出了劳动成本，收益被矿工按付出成本的比例分配。这里我们有一个算法机制来监控整个网络的节点数及其数据量用来估算区块链网络的经济价值（此价值包括当前区块链网络及全部子区块链网络经济价值的总和）。当前网络的经济价值达到一个阈值时，自动触发下一个新区块验证需要费用，当然在没有达到全网阈值时，用户也可以设置交易费用。这时交易成功后，新区块会写入交易费用，我们会有检验算法验证这种个人行为的数据，少量行为不影响无费用 Transaction 验证机制。当经济价值达到系统约定值时，利益驱动一些人使用网络中 PoS 验证，矿工验证交易完成获得矿工费并把矿工费写入区块的 transactioncost 值，则相当于区块链网络提前进入交易费用阶段。此时，用户面临两种选择，一，继续在此区块链网络上生成交易数据但需要支付一定量的交易费用；二，不想支付交易费用选择无费用交易，则网络系统会自发从当前区块链网络分层一个新的子区块链网络并把新的交易写入子区块链网络。达到了区块链网络自动分层功能。这些行为都由网络中的参与者共同作用得出来的结果。当节点数足够多时，随着时间的推移 TOS 区块链网络自动形成不同层级的区块链网络。每个区块链网络只有当前区块链网络及所有子层区块链网络数据访问权限。同级别的区块链网络数据不能直接交互，但可以通过对应的父区块链网络通信数据。这样物联网的海量数据就会自发的根据不同区域形成不同子区块链网络。海量数据被切割成无数个小块，把原来区块链全网数据共享一个账本变成父区块链网络有无数个小账本，子区块链网络只负责管理自身的小账本。这就是 TOS 区块链的数据存储瘦身,也能更好的做到大数据管理。

(五) CORE GOALS TOS

TOS 核心技术 SDAG 的工作模式



网络工作的情况下，TOS 按以上方式运行。是由多个不同层级的 DAG（有向无环图）组成一个树状结构，也称之为 SDAG（超级有向无环图）。通过节点发出的所有区块构成了这个超级有向无环图 DAG 的集合，并且 SDAG 不存在全局的区块链。每笔新的交易出现时，生成一个新区块，且新区块必须验证之前的两个区块。我们定义，新节点验证旧节点称为新节点为输出旧节点为输入。这些验证关系通过有方向的边来表示，如图所示（在图中，时间走向总是从左到右）。如果从交易 A 的区块到交易 B 的区块之间至少有两个有向边的路径存在，我们就说交易 A 的区块直接地验证了交易 B 的区块又间接的验证了交易 E 的区块。我们认为诚实节点会检查验证交易是否存在冲突，同时不会直接或间接地验证具有冲突交易的区块。这种机制随着交易产生的新区块都会直接或间接的验证区块网络中的区块，区块被验证的数量增加，整个区块就会被区块网络所接受。换句话说，要伪造一个双花交易是极为困难的（或者至少在实践上是几乎不可能的）。

SDAG网络特点

1) 良好的扩展性

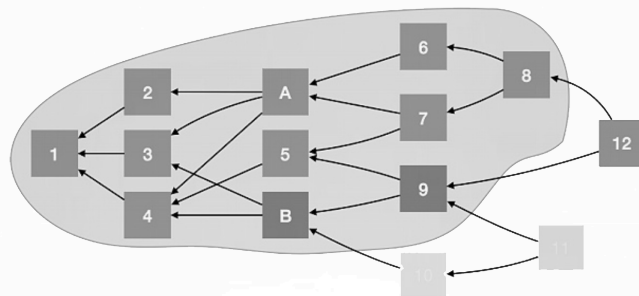
众所周知，由于 SDAG 网络的分层区块机制，可以做到网络具有无限分层子区块功能，就像树根一样无限扩展延伸。在 TPoS 共识的区块网络中，PoS 负责验证带交易费用的数据，它的特点是安全性更高，越是重要的信息付出高交易费用就能写入越高层的区块网络；Transaction 交易自身验证，交易数据写入末区块网络，安全性相对比 PoS 低，但是可以做到交易并发量高、吞吐量大。综上所述，SDAG 具有良好的可扩展性。

2) 支持无费用交易

Transaction 交易自身验证可以做到交易无费用，这给很多用户带来非常便捷。比如，在物联网的某大型工厂中设备数据诉求是：要能够做到与其他设备通信交互，又能访问整个物联网中第三方授权的设备数据。假如设备属于高频数据发生端，每笔交易数据写入区块都需要费用，这对于工厂的成本管理而言是不可接受的。这时 Transaction 共识机制的优势就体现出来，工厂可以自己分层一个末区块网络。使用 Transaction 共识验证，用来交易记录数据。当然有人会挑战安全性，因为末区块网络的节点数少时，发起恶意攻击，付出足够大的代价是可以做到篡改数据，对比现实互联网中这种安全现象也不可避免，任何作恶者发起攻击的动机都是为了利益。如果是一些普通无价值或少量价值的数据，作恶者不会有足够的动力来做这种亏本的事情，但如果是很值钱的数据，也没必要记录在末区块网络中，也就是说，用户可以根据自身数据的价值来决定把数据记录在什么样层次的区块网络。风险是用户考虑的，当然想要数据的安全性越高，对应付出的成本费用也越高，这也是符合经济现象，安全是需要成本的。

3) 区块数据分层隔离

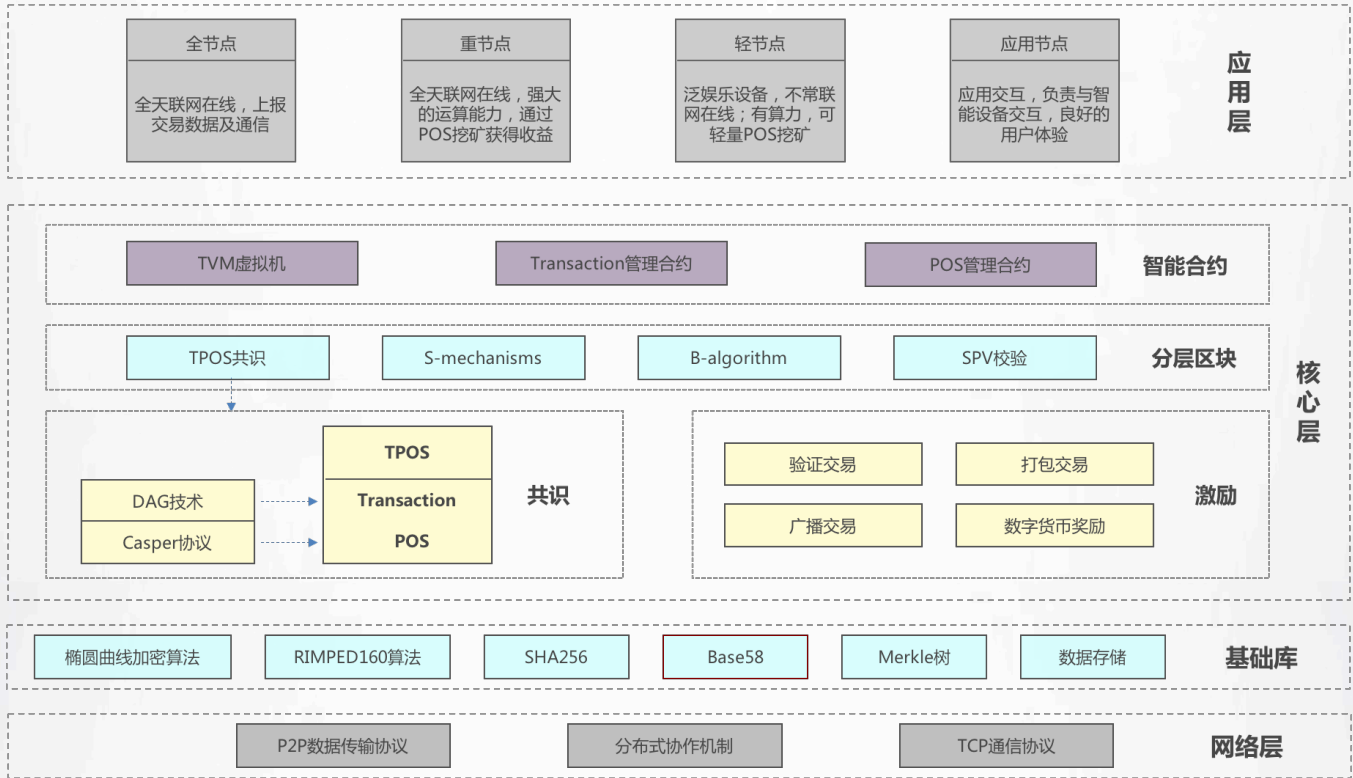
前面说到，区块网络具有无限分层子区块网络功能。每个层级的区块网络各自存储对应的数据，把全网的区块数据分离。这样全网区块，被分割成一条条的分层区块网络，且同级分层区块网络之间是不能通信的。可以将这个模型理解为长江及其支流，



长江源头就是区块网络开始区，主区块网络如同长江主干道，区块网络上的无数分层区块网络如同长江主干道上的无数个支流，主区块网络分层的各子区块网络写入的新交易数据就如河水流入各支流。小河流之间不能直接流通，同理子区块网络也不能直接交互数据。但是可以使用反射功能，通过对应的父区块网络反查对应的子区块网络数据。这样数据是分层隔离的，因此每条子区块网络的数据总量是包含这条分层上所有父区块网络(如同:小沟->小溪->小河->长江)。在网络系统中区块数据隔离机制，可以大大的减少全网区块数据冗余，从而减少了单节点的数据容量，系统的负载也会变轻。可以预测经系统运行一定时间后，交易数据经过系统机制越是重要数据越会存储在上层区块网络，因此SDAG也能更好的支持大数据管理与高价值数据挖掘。

(六) TECHNOLOGICAL INNOVATION

TOS 技术架构图&技术创新



TOS 技术创新

1) SDAG支持免费交易与收费交易

通过 TPoS 结合共识机制，免费交易让用户记录普通数据，不需要交易成本，与物联网设备产生的海量数据场景相契合。收费交易，适用于物联网中高价值数据交易转让。记录在高层级区块链网络，流通性更好，安全保障更高。

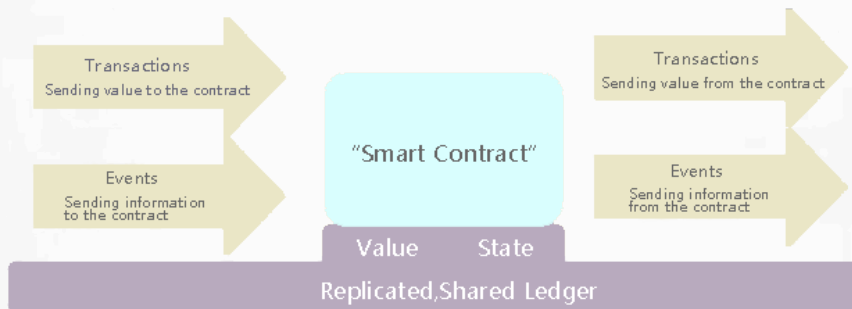
2) SDAG 拥有无限分层区块链网络能力

SDAG 通过 S-mechanisms 机制与 B-algorithm 算法实现区块链网络分层。B-algorithm 算法监控区块链网络的经济价值，当网络的经济价值达到阈值，S-mechanisms 机制会自动触发下一个新区块验证需要费用。此时，用户面临两种选择，在此区块链网络交易数据需要费用。如果想继续使用免费交易，网络系统会从当前区块链网络分层一个新的子区块链网络，并把新的交易生成的区块写入子区块链网络，达到无限分层区块链网络能力。

3) SDAG 密码经济学平衡机制

免费交易与收费交易结合，可形成相互制衡关系。通过收费与免费形成一个数据分配的等级制度。免费交易数据只存储在末区块网络，收费交易存储在高层级区块网络，交易费用越高存储的网络层级越高。这样避免垃圾数据阻塞高层级区块网络，也可以减少高层级区块网络的数据量。将数据分离在不同层级区块网络，根据数据价值进行分层存储，更合适于数据挖掘及未来与人工智能的结合。

4) SDAG 扩展智能合约



SDAG 中的区块包含了签名、区块信息与父区块网络的信息。区块之间以哈希相关联，是区块链账本与有向无环图结合技术。不过 SDAG 是基于 DAG 技术的扩展，就原 DAG 技术架构本身而言，存在一个很大的隐患，不能完全保证交易状态的原子统一性。从时间上来讲，可能存在特定节点（比如远程节点）确认某笔交易的时间无法估计；从节点上来讲，全网络节点中的某个节点可能无法更新某一时刻的交易信息，即该节点没有被广播到某一时刻的交易信息。这些情况对于很多商业形态来说是一个极大隐患。为了解决这一问题，对原有 DAG 技术架构进行了改进，在 SDAG 中增加虚拟机(TVM)实现智能合约。

5) 物联网分层架构

物联网分层安全体系结构分别针对感知层、传输层和应用层提出相应的安全措施，确保在物联网的每一环节和层次都得到安全防护与管理与控制，从而保证数据安全。

5.1) 感知层

感知层通过电子标签或 RFID 进行识别，再通过传感器网络进行全方面的感知。因此，在安全防护方面，要对 RFID 相关物理设备进行保护，对传感器节点进行保护，定期进行安全验证与鉴权；还应在传感器节点之间建立信息安全传输机制，保证传送数据不会被未授权节点获取或即使被获取后也无法被破译。

5.2) 传输层

传感器感知到的信息通过初步处理和过滤后通过传输层传到应用层进行处理，再由应用层接入到 TOS 网络节点。因此，在传输层要保证端到端的数据加密、节点安全性验证，以及网络接入安全性。通过验证、鉴权、密钥等技术确保端到端的传输安全性；此外，通过相关的数据加密算法，确保数据的完整性和安全性。

5.3) 应用层

通过传输层传送到应用层的数据量大，数据存在异构性，因此需在应用层上处理海量异构数据，转换为 TOS 标准协议格式接入到网络节点中上链数据。还需建立起一个统一的标准体系和安全机制，进行数据访问权限、授权管理等安全防护手段，以加强对个人隐私和各类应用数据的保护。首先，各家智能设备经感知层、传输层到应用层，应用层运行着各厂商的兼容包；然后，经过兼容包转换过的数据接入到 TOS 网络节点，再由 TOS 去中心化区块链技术把所有智能设备万物互联起来。对于各厂商来说，不需要改变现有的设备协议标准，而且把设备数据上 TOS 链之后，厂商没有了中心化的数据营运成本，只需开发一个协议兼容包就能达到双赢。随着物联网不断渗透到各行各业和人们的日常生活中，不论是在感知、传输，还是应用处理阶段都会存在一定的安全隐患。而物联网数据呈现数据量大、异构性大、突发性等特点，因此在对物联网采取相关安全措施时，更需要分层次、分阶段进行不同的管理和控制。TOS 采用物联网分层安全体系结构，该结构分别针对感知层、传输层和应用层的数据感知采集、数据传输、数据处理进行全方面的保护，从而全面提升物联网安全性。

6) 去中心化的物联网操作系统

物联网操作系统是一个公共的业务开发平台，具备丰富完善的物联网基础功能组件和应用开发环境。它可大大降低物联网应用的开发时间和开发成本；提升数据共享能力，统一的物联网操作系统具备一致的数据存储和数据访问方式，为不同行业之间的数据共享提供了可能。物联网操作系统可打破行业壁垒，增强不同行业之间的数据共享能力，甚至可以提供“行业服务之上”的服务，比如数据挖掘等；物联网的范围很大，一般来说，所有的操作系统都可应用在物联网领域中，操作系统是物联网时代的战略制高点，今天 PC 和手机时代的操作系统霸主未必能在物联网时代延续霸业。操作系统产业的规律是：当垄断已经形成，后来者就很难颠覆，只有等待下一次产业浪潮。如今，TOS 正在开启一个全新的、充满想象空间的去中心化的操作系统。

(七) TOS TECHNOLOGY ADVANTAGES IN IOT APPLICATIONS

TOS 在物联网应用中的技术优势

TOS 的核心技术 SDAG 解决物联网存在的三个痛点，海量数据存储、并发量高、交易成本大。

对于现有的区块链技术，DAG 技术可以解决并发量高和交易成本大的问题。但是海量的数据冗余、巨大的网络数据传输量和无法确定交易时长的问题并没有被解决，在物联网中这是必须要解决的问题。

从 TOS 的核心技术 SDAG 来讲，SDAG 的四大特性可解决上述问题：

分层区块网络

它减少物联网中大量的数据冗余，单个节点数据容量更小，降低设备存储成本。每节点只需验证当前区块网络交易数据，每层区块可独立验证，提高交易效率。不妨做一个大胆设想，假如 TOS 有 1 万个分层区块网络，每个分层区块网络的 TPS 都和比特币一样 7 笔每秒，那么 TOS 的总 TPS 就是 7 万；如果 TOS 的单层区块网络 TPS 性能是 1 千，那么 TOS 的总 TPS 就是千万级。实际上 SDAG 完全具备 DAG 技术上的高 TPS，初步可达到比特币千倍的性能，也就是说随着区块网络分层越多，TOS 总 TPS 就越高，甚至可以达到千万级乃至亿级以上。

TPoS 共识

通过 TPoS (Transaction+PoS) 结合共识，实现用户根据数据的重要性选择使用免费或付费交易。免费与付费的模式并存，根据交易费用的多少，将数据存在不同层级区块网络。

TVM 虚拟机

TVM 虚拟机可实现智能合约，在物联网商业应用中，这些具有事件驱动的状态，并且存储及运行在区块链上的智能合约双方履约带来安全保障，使得在没有第三方的情况下可以进行可信交易，减少不必要的损失。

减少冗余交易

在 SDAG 分层区块网络的 TPoS (Transaction+PoS) 共识机制中，PoS 矿工验证的一个区块内可以收集大量的交易，如果出现双花的问题，可以将冗余交易剔除，既不会出现冗余交易且不会影响交易的验证效率。SDAG 的当前层区块网络分层出子层区块网络之前，使用 Transaction 共识机制，当分层区块网络的经济价值达到阈值时，自动启动 POS 收费验证机制，此时之后，当前层级区块网络就不会出现冗余交易。总之，Transaction 共识会产生冗余交易，POS 共识不会产生冗余交易。在 SDAG 中所有的冗余交易只会出现在经济价值低的末区块网络中，并且仅在这层区块网络经济价值未达到阈值的阶段。由此可见，分层区块网络发展的越庞大，冗余交易占比就会越低，从而减少了大量的冗余交易。

根据 SDAG 的四大特性，在 TOS 链中，首先，节点的数据冗余非常少，对设备的存储空间要求非常低；其次，减少了网络传输数据，降低了对网络带宽的要求；第三，用户可选择交易付费类型，减少交易成本；第四，SDAG 的分层区块网络能实现快速交易及高 TPS，数据经过 S-mechanisms 机制过滤后分拨到不同层级的区块网络可数据挖掘；第五，减少了大量的冗余交易；最后，智能合约在 DApp 商业应用时可以强制履行双方的合同及经济保障。综上所述，TOS 的技术方案很适用于物联网行业。

(八) APPLICATION SCENE

TOS 的应用场景

企业级智能硬件平台

企业级智能硬件平台是 TOS 公链的基础也是最核心的应用平台。基于智能合约，设备、对象、数据、逻辑方法、凭证等可以完美的在 TOS 公链上进行组织和执行，并为 TOS 其他应用提供运行环境和执行系统。TOS 的智能硬件平台包括有丰富的应用类型，并为满足不同的物联网及不同公司环境场景下应用进行优化，目前设定的智能合约类型有：

1) 主控类合约

A.基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约；并且事务的状态处理和保存都在区块链上完成。事务主要包含需要发送的数据；而事件则是对这些数据的描述信息。事务及事件信息传入智能合约后，合约资源集中的资源状态将会更新，进而触发智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状态机根据预设信息选择合约动作自动执行。

B.特色：全球首家区块链平台将物联网设备智能合约投入实用场景中

C.举例：去中心化智能租房案例

-某高端公寓，采用TOS 去中心化的租房方案，将门锁替换成支持 TOS 智能合约的门锁，并在区块链模式的租房网站发起租房信息，拟定租房合约，例如，租房免押金，租金每月定时扣 XX 币，逾期门锁自动换密码；看房时在网上进行预约，预约成功暂扣 1 个月房租担保金，并将则 1 小时有效门锁密码发送到租客手机，租客凭借密码在一个小时内看房，如果不满意，则直接走人，1 个小时后密码重置并退还房租担保金；如果看房成功，则租房智能合约生效，扣除租房房租，并将门锁密码设置成租客专用。在整个租房过程中，不需要销售陪同，无需信用认可，节省了大量的人力物力。

2) 数据结算合约

A.数据结算合约用于物联网设备或其他可以提供数据的产品上，由设备拥有方拟定可以开放分享的数据内容，并提供数据接口，数据需求方可以按照约定的价格和方式，按照数据接口定时获取数据，并自动完成结算。结算的代币，将直接转入拥有方的账户，并且可以支持超小额支付。

B.特色：

- 支持多种不同的数据类型，以及多样化物联网设备的数据采集
- 支持超小额支付，满足数据碎片化的交易需求
- 支持超低手续费交易，方便小额支付

C.举例：用户利用行车数据进行交易

-用户小A 刚刚购买了一辆带有数据交易、智能合约的新小轿车，并且每天使用。根据智能合约内容，只要小A 同意将行车数据，包括驾驶习惯，地理轨迹，车辆信息等以匿名的方式进行分享，这些数据将被用来分析车辆驾驶者的驾驶习惯，完成司机用户的画像分析，帮助厂商的无人驾驶 AI 完善驾驶模型，并且广告厂商也可根据数据有所侧重地分析定位用户的喜好，并在车载设备里进行了精准广告投放，作为回报，小A 获得了代币，可以用代币在 4S 店冲抵保养费用，或者在支持的加油站自动加油结算。

3) TPoS 共识合约

– TPoS 共识协议是 TOS 的核心运行机制,通过基于原 DAG 技术实现的 Transaction 共识与基于 Casper 协议的 PoS 共识,让每一个连入网络的物联网设备都可成为 TOS 的矿工。智能设备可通过 PoS 的保证金经济激励管理合约“虚拟挖矿”获得手续费,并通过验证之前的两个区块,及区块直接或间接验证的机制保证网络安全。由于采用 Transaction + PoS 的 TPoS 共识,在 TOS 系统中,只需少量算力用于交易自身验证 Transactoin 共识与基于保证金经济激励协议的 PoS 共识运算,避免了浪费算力。

– 特色

- 采用基于 DAG 技术的 Transaction 共识,少量算力基础的交易自身验证及间接验证
- 支持 PoS 共识验证收取手续费,为矿机提供持续运转费用
- 基础算力可支持物联网设备及嵌入式在 TOS 环境运行

– 举例: 小米扫地机器人成为中心节点

小米扫地机器人在家庭使用的时候,每一个都成为了 TOS 网络节点,数据上报实现了交易自身验证及数据存储功能。通过连接更多的物联网设备节点,更多的交易数据量,让每个智能设备成为 TPoS 共识的一部分。由此,扫地机器人能为其主人提供 PoS 共识“虚拟挖矿”获得代币,持续创造财富。

4) 账本类型合约

– TOS 的区块链技术也可以用去中心化账本功能来创建、确认、转移各种不同类型的资产及合约。包括数字股票、私募股权、众筹、债券和其他类型的金融衍生品。这些形式,可以被用来做 TOS 的智能硬件孵化器平台,供智能硬件基于 TOS 来发行众筹项目或融资手段,并利用TOS 的完整区块链技术和数据体系,实现更丰富类型的智能账本合约。

– 特色:

- 专为智能硬件公司设计,帮助其产品上链
- 提供从数字股权、数字项目分成到数字债券等多种丰富的合约内容
- 提供用户、数据、API 等多种上下游资源给参与孵化的智能硬件企业

– 案例–某智能硬件公司产品及业务和区块链关系不大,不方便直接用以太坊的模式发行代币融资。利用TOS 的智能硬件合约,可以直接基于硬件产品进行项目众筹,所有的参与用户可以利用智能合约,享受到未来硬件产品成功销售后的分成。因为每一个智能硬件都在 TOS 的链上,因此厂商无法造假,必须按照智能合约给参与众筹的用户进行代币结算,保障参与者获得收益内容。



物联网大数据交易平台

TOS 数据交易平台是 TOS 代币系统流通的重要基础平台。在此平台上，设备厂商可以建立采集数据、销售数据的渠道，并增加设备的获益功能，以吸引更多的用户购买；设备用户，可以通过此渠道提供个人数据以获取收益；数据购买方，如广告主，也可以利用此平台精准定位用户，取用户画像数据，并以更低的价格高效的达到传播目的。

TOS 的数据交易平台目前包括以下 2 个核心模块

智能广告传播平台/物联网数据交易中心

对于广告主而言，目标用户的一个核心概念是“用户画像”(personal profile)：指的是个人的年龄、性别、行为、性格、趋势等，简而言之就是用户是个什么样的人，这对于广告的“差异化受众”来说是一个很关键的区分标准。在互联网出现以前，个人用户画像产生非常缓慢，而随着互联网尤其是移动互联网的兴起，个人数据突然间以一种可轻易分享和复制的方式进入了全球互联网。个人画像变成日益壮大的数据海洋，为许多人所用。广告技术的前景本应当是创造一个更高效、更透明的市场，将广告与目标消费者匹配。数字技术也应当使广告主及目标市场之间的交易流变得更容易追踪，并确保信息到达目标消费群体。然而，经过二十年的发展而形成的广告技术生态系统却充斥着各式中介和复杂交易，令人迷惑。广告主则因为虚假数据、不精准数据，损失了数以十亿计的收入，欺诈甚嚣尘上。广告主还深受反馈不到位和投放精准度不足之苦。毫无疑问，这一切都需要一个良好的解决方案。

1) 智能广告投放平台，则是基于物联网与 AI 时代的一个突破性服务模式，重点解决了中心化广告传播与投放的种种问题。首先可以让广告主以去中间商的模式，直接将广告投放到用户面前。物联网电视、冰箱、汽车等等，都可以成为传播媒介，精准而高效。其次，广告主对目标用户的筛选也变的非常高效。由于 TOS 平台可以将参与数据交易的个人生活有关的各种数据进行采集和分析，远远不止手机和浏览器搜索关键词这样的单一维度。对用户画像的精准性大增，甚至可以做到在用户喝啤酒的时候由 AI 机器人推荐炸鸡翅。一方面满足了用户精准需求，另一方面也让广告主投放传播效率更高。



2) 物联网数据交易中心作为数据分享和交易平台，数据的安全性和消费者隐私尤为重要。TOS 的去中心化技术本身具备不可篡改性。公开交易信息和 SDAG（超级有向无环图）交易自身 Transaction 验证及 PoS 验证确保了用户的交易可确定性安全。在 TOS 网络中，其交易的唯一性和确定性都将会被保障，并且不可篡改。此外，用户如希望在链上应用存储数据，将可以自由选择加密方式，加密安全性取决于选择加密的算法和强度。同样，其唯一性和确定性也会被保障，并且一旦应用交易成功写入，也将不可篡改。消费者的隐私也是 TOS 去中心化平台考虑的重中之重，除了采用分布式存储，降低单个设备被入侵的风险，并采用苛刻的数据加密手段以外。所有的对外分享的数据，都可以消费者自己设定分享权限，也可以完全封闭。此外分享的数据也将消费者个人隐私信息，包括 ID、姓名、详细住址等等进行严密保护，并未对外分享，也不能和已有数据进行关联。确保进行交易的数据，只是基于大众行为的画像，而不是某一个消费者的具体信息。

智能金融服务平台

TOS 的金融服务平台、智能合约系统、数据交易平台三大板块，加上智能硬件入口，3+1 模式融合在一起，从生态价值链的角度为 AI 及智能硬件企业提供了融资、产品研发、产品上网、产品分发、产品获益等一条龙解决方案，帮助传统硬件和家电企业快速上链，通过去中心化物联网模式快速获得用户并提升用户体验。这三大系统和一个核心产品，也是 TOS 区别于其他公链平台的关键，TOS 更注重落地，更注重应用，更注重用户实际应用区块链技术的反馈。我们有理由相信，TOS 将引领区块链技术走向更加实用的未来。

智能物流平台

TOS 未来将会利用条形码、射频识别技术、传感器、全球定位系统等先进的物联网技术通过信息处理和网络通信技术平台广泛应用于物流业运输、仓储、配送、包装、装卸等基本活动环节，它将实现货物运输过程的自动化运作和高效率优化管理，提高物流行业的服务水平，降低成本，减少自然资源和社会资源消耗。物联网为物流业将传统物流技术与智能化系统运作管理相结合提供了一个很好的平台，进而能够更好更快地实现智能物流的信息化、智能化、自动化、透明化。利用集成智能化技术，使物流系统能模仿人的智能，具有思维、感知、学习、推理判断和自行解决物流中某些问题的能力。即在流通过程中获取信息从而分析信息做出决策，使商品从源头开始被实施跟踪与管理。即可通过 RFID、传感器、移动通讯技术等让配送货物自动化、信息化和网络化，在技术上将实现：物品识别、地点跟踪、物品溯源、物品监控、实时响应。

(九) TOS COMMUNITY FOUNDATION

TOS 社区基金会

TOS 项目是由基金会驱动的全球性智能物联网开放协议项目。

TOS 社区基金会的设立

基于 TOS 社区的国际化定位和影响力，TOS FOUNDATION PTE LED（以下简称 TOS 基金会）是一家总部设立在新加坡的非营利组织。基金会致力于 TOS 开源社区的维护运营，以及 TOS 公链平台的开发、发展和建设，倡导透明治理和 DAO 模式的管理，让 TOS 社区真正归属所有参与 TOS 物联网价值链的建设者与爱好者，并促进 TOS 开源生态社区的成熟和持续发展。

TOS 基金会的治理架构

TOS 社区基金会治理架构包含了针对日常工作和特殊情况的操作流程和执行规则。TOS 推崇去中心化的 DAO 治理模式，认为所有 TOS 项目参与者，都是 TOS 基金会的组织成员，共同享有 TOS 的发展价值和决策权。TOS 的重大事项，均有全体成员共同投票决定。若有促进 TOS 发展议题，任何 TOS 的参与者都可以组织追随的社区成员共同发起。首届 TOS 基金会决策委员会由核心创始成员组成，一共 5 人，任期为 4 年，核心创始成员在区块链领域中具有丰富的行业经验。任期满后由社区根据持有 TOS 数字资产的持有份额和资产龄计算权重，选举 50 名社区代表，再最终选举产生 5 位决策委员会成员。

TOS 基金会的交易安全

TOS 公有链通过区块链共识、智能合约等技术以及数字签名、终端用户加密钱包等安全手段确保用户账户及资金安全。TOS 公有链提供金融级别的安全数据存储、网络等资源，将数据、应用和交易集成到分层区块链网络中，构建安全的交易网络环境。

审计

TOS 基金会将保持高度的诚信和商业行为道德，遵守相关法律法规及行业自律原则，TOS 基金会每年会邀请国际知名第三方审计机构对 TOS 公有链运营管理上的资金使用、成本支出、利润分配等方面定期进行审计和评估，TOS 基金会将毫无保留的将数字资产信息公开发布给第三方机构进行评估和审核。

(十) TOSCORE TEAM

TOS 核心团队和专家顾问



基金会主席
Jeffers Kieron Matthew

证券投资学院(SII)顾问。
特许证券研究所所长。
英国金融行为管理局: CF1主任; CF10 合规监督;
CF11 洗钱报告; CF30 客户区域链金融监管。
Manari 有限公司: 英国伦敦董事长: 管理各种资产类别(包括外汇,证券和期货) FCA 监管,为批发,机构,专业和零售客户安排交易。
全球市场指数(GMI): 伦敦, 英国/上海, 中国/香港, 特定定制 OTC 交易的原始 ISDA 协议。



CEO
吴相庆 Stephen Wu

领冠资本创始人
数字货币资深投资人
曾任职: 香港新鸿基集团独立投资部 基金经理
Infinity Service USA Inc. 大中华区 COO
2006 年, 为香港新鸿基集团独立投资部创下净利润一亿港币, 被评为年度十大杰出基金经理; 2008 年, 任职 Infinity Service USA Inc. COO 期间, 将公司规模发展到 64 家分公司, 并进行系统标准化管理。
拥有区块链技术交易所整体解决方案的运营经验, 熟悉数字货币市场, 并对未来发展趋势和走向有深入的研究。



CTO
陶海军 Navy Tao

曾任腾讯公司高级工程师。
曾任华为心声社区项目移动端总架构师。
数字货币社区爱好者, 致力于引导推动区块链行业发展。
近十年的技术研发经验及多年深入区块链技术研究。对区块链金融创新、区块链与传统应用场景结合有独到见解。目前带领团队专注于物联网区块链技术技术创新研发, 并认定区块链发展将会开启互联网第二纪元。



CFO
Daniel Hornstein

区块链专家/密码货币顾问/财务顾问。
区块链开发和技术加密货币实现绩效管理、谈判项目管理。
Traxco 瑞士 Blockchain 的技术和后端 IT 顾问。
Bayz Sdn 停车有限公司首席执行官和财务顾问。
Taniwha Sdn 有限公司总监/财务顾问。
荷兰皇家大使馆(吉隆坡) 顾问。



首席产品官
石梦星 Timothy Shi

曾任农泰金融项目研发经理。
曾任华安保险客户端项目总架构师。
曾任华为重点项目高级开发工程师。
数字资产爱好者, 拥有多年的项目架构经验。曾参与研究应用区块链技术解决保险行业和 P2P 投资交易信任和安全问题, 现致力于实现去中心化技术的落地研发工作, 专注于应用区块链技术解决传统领域的各种痛点。



首席架构师
李球 Tony Lee

曾任平安金融科技高级工程师。
曾任华为心声社区移动端项目经理。
区块链技术狂热分子, 致力于区块链技术的研发。拥有多年项目研发架构经验, 现专注于研究解决区块链海量数据、交易效率等问题, 致力于打造安全可靠、低成本高效率的区块链系统生态圈。



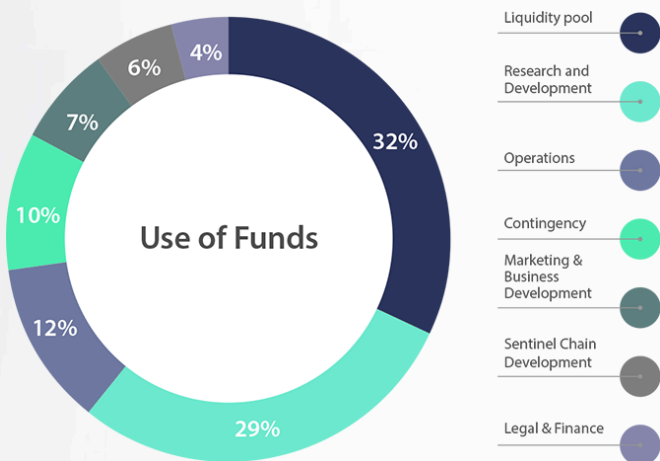
技术顾问
Diego Cresta

巴黎高等管理学院金融管理硕士。
菲律宾国立雷省科技大学工商管理学博士。
曾经在马来西亚、英国、澳洲、香港等地担任投资顾问投资培训师, 企管顾问。
英国伦敦工商会计专业证书。
马来西亚注册财务理财师(RFP)。
美国财务管理学院专业顾问。
香港证券专业学会颁发证监会资产管理专业证书。
美国寿险训练学院院长(LUTCF)。
美国金融工程师研究所会员(IAFE)。
澳大利亚税务和管理会计师协会会员(ATMA)。
美国宾夕法尼亚州美国金融学院和马来西亚保险学院颁发的特许财务顾问证(ChFC)。

(十一) BUDGET ALLOCATION

TOS 数字通证分布与预算分配

TOS 公有链的数字通证简称 TOS，是 TOS 基金会官方发行的原生加密数字令牌。第一阶段将在以太坊上依据智能合约生成，第二阶段将基于 TOS 公链自行生成，并作为 TOS 基金会的唯一基础积分通证，用来作为社区奖励、论坛积分、结算、交易、以及公链物联网智能合约履约使用。第一阶段通证将以 1:1 的比例与第二阶段通证进行置换。数字通证 TOS 共发行 10 亿枚，由 TOS 基金会一次性创设出来，其总量上限已设定，不可更改，不可增发。数字通证 TOS 按照一定的规则和比例分配给不同的持有人。其中 50%通过私募获得的数字资产用于区块链底层建设、产品模块研发、应用生态布局、TOS 公有链整体运维等。5%的代币将预留给早期基石投资者，15%将预留给创始团队成员(锁定期为三年。第四年开始每半年释放一次，每次释放量不超过持币量的 30%，且总释放量不超过持币量的 50%)，20%将预留给基金会用于后期开发应用，市场推广和运营以及区块链研究，10%将用于 TOS 社区建设投入。



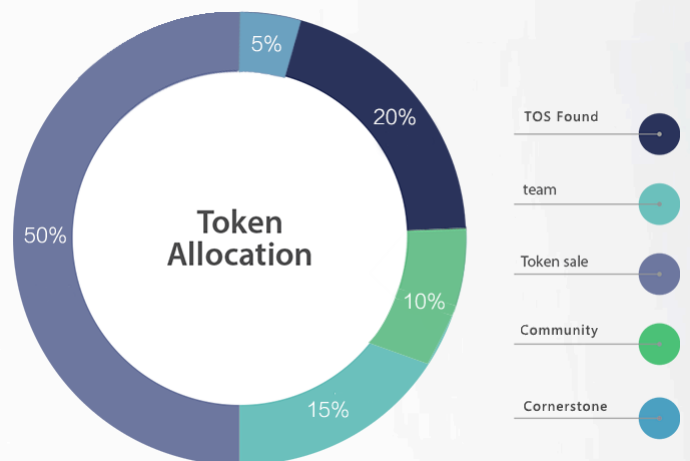
流动性池: 多达三分之一的资金用于维护TOS区块链的预先筹资流动性池。

研究与开发: 高达29%的资金用于持续参与区块链应用和研究，及在当地社区建立一个完整的生态系统。

运营: 最多12%的资金用于促进与战略合作伙伴的联盟与合作，并启动项目。

意外事故: 多达10%的资金将用于任何意外的项目超支。

市场营销和业务发展: 高达7%的资金将用于在不同司法管辖区营销TOS项目。这将包括线上和线下营销活动，与各种商业合作伙伴签署合作关系。



TOS发展: 持续开发TOS公有链的技术基础设施至关重要。高达10%的资金将用于扩大开发人员的人才库，以建设各种本地化的TOS侧链和子链。

法律和财务: Daniel Hornstein已被任命为监管和合规事宜提供建议，包括提供独立的法律建议。在项目开发和实施过程中，将建立一个强大的内部法律团队来驾驭法律环境。

Diego Cresta已被任命为税务和审计事宜提供咨询。将建立一个强大的内部财务团队来管理符合全球最佳实践的财务和会计职能。

根据令牌销售结果和项目进度，预计的细节可能会发生变化。

(十二) ROAD MAP

开发工作路线图



(十三) DISCLAIMER

免责声明

本项目将由 TOS 基金会管理，该基金会是一个注册在新加坡的非盈利性机构，受到新加坡法律和 ACRA 监管。该基金会的使命是促进和支持 TOS 去中心化项目发展，使其成为一个更为全球接受的、值得信赖的物联网公有链。在任何司法管辖区，TOS 代币都不能作为证券。本白皮书不构成招股说明书或任何类型的要约文件，无意构成证券要约或投资招揽，以任何方式涉及首次公开发行或股票发行 / 融资，亦不以任何方式涉及在任何司法管辖区的证券发售。TOS 代币无意在任何被适用法律禁止、或者需要在任何相关政府部门进行进一步登记的司法管辖区进行推销、提呈发售、购买、出售或交易。TOS 代币并非本基金会的贷款。TOS 代币既不是任何性质的债务工具或债券，也不是向本基金会预付的任何其他形式的贷款。不论是通过代币发售还是其他途径获得 TOS 代币，并不表明向代币持有人授予对本基金会的财务或任何其他资产的任何求偿权。

TOS 代币未授予参与本基金会或其资产的权利。TOS 代币未向代币持有人提供本基金会的任何所有权或其他利益。获得 TOS 代币不等于可以用加密货币换取本基金会任何形式的股份或本基金会资产（包括知识产权）。代币持有人无权享有任何有保证形式的利息、收入分配和投票权利。TOS 代币不可退款。本基金会不会出于任何原因为代币持有人提供与 TOS 代币相关的退款，代币持有人不会收到代替退款的金钱或其他补偿。关于 TOS 代币的未来表现或价值，现在没有且将来也不会有任何承诺，包括内在价值的承诺、继续支付的承诺和 TOS 代币拥有任何特定价值的保证。

(十四) REFERENCES

参考文献

- [1] Blake2.net. (2017). BLAKE2. [online] Available at: <https://blake2.net/> [Accessed 16 Oct. 2017].
- [2] CoinDesk. (2016). Understanding The DAO Attack – CoinDesk. [online] Available at: <https://www.coindesk.com/understanding-dao-hack-journalists/> [Accessed 20 Nov. 2017].
- [3] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106–125). Springer Berlin Heidelberg.
- [4] Decker, C. (2017). BitcoinStats. [online] Bitcoinstats.com. Available at: <http://bitcoinstats.com/network/propagation/> [Accessed 10 Nov. 2017].
- [5] Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on (pp. 1–10). IEEE.
- [6] digiconomist.net. (2017). Bitcoin Energy Consumption. [online] Available at: <https://digiconomist.net/bitcoin-energy-consumption> [Accessed 16 Nov. 2017].
- [7] Digiconomist. (2017). Ethereum Energy Consumption Index (beta) – Digiconomist. [online] Available at: <https://digiconomist.net/ethereum-energy-consumption> [Accessed 8 Dec. 2017].
- [8] The Economist. (2007). The end of the cash era. [online] Available at: <http://www.economist.com/node/8702890> [Accessed 27 Sep. 2017].
- [9] Ethereum Blog. (2014). Toward a 12-second Block Time – Ethereum Blog. [online] Available at: <https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/> [Accessed 27 Sep. 2017].
- [10] Etherscan.io. (2017). Ethereum Average BlockSize Chart . [online] Available at: <https://etherscan.io/chart/blocksize> [Accessed 16 Nov. 2017].
- [11] Ethstats.net. (2017). Ethereum Network Status. [online] Available at: <https://ethstats.net/> [Accessed 16 Nov. 2017].
- [12] Goland.org. (2017). How to make block chains strongly consistent – Stuff Yaron Finds Interesting. [online] Available at: http://www.goland.org/why_block_chains_are_strongly_consistent/ [Accessed 27 Sep. 2017].
- [13] Goland.org. (2017). The block chain and the CAP Theorem – Stuff Yaron Finds Interesting. [online] Available at: http://www.goland.org/blockchain_and_cap/ [Accessed 27 Sep. 2017].
- [14] Google Developers. (2017). Protocol Buffers | Google Developers. [online] Available at: <https://developers.google.com/protocol-buffers/> [Accessed 20 Oct. 2017].
- [15] James-Lubin, K. (2015). Blockchain scalability. [online] O'Reilly Media. Available at: <https://www.oreilly.com/ideas/blockchain-scalability> [Accessed 16 Nov. 2017].
- [16] Koteska, B., Karafilovski, E. and Mishev, A. (2017), Blockchain Implementation Quality Challenges: A Literature Review : Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia, 11–13.9.2017.
- [17] Malanov, A. (2017). Six main disadvantages of Bitcoin and the blockchain. [online] Kaspersky.com. Available at: <https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/> [Accessed 16 Nov. 2017].
- [18] Motherboard. (2017). One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week. [online] Available at: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change [Accessed 20 Nov. 2017].

- [19] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.
- [20] The NodeSource Blog – Node.js Tutorials, Guides, and Updates. (2014). Why Asynchronous?.
[online] Available at: <http://nodesource.com/blog/why-asynchronous/> [Accessed 16 Nov. 2017].
- [21] Park, J.H. and Park, J.H., (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, 9(8), p.164.
- [22] Poon, J. and Dryja, T.. (2016). The Bitcoin Lightning.network [online] Available at:
<https://lightning.network/lightning-network-paper.pdf>.
- [23] Raiden-network.readthedocs.io. (2017). Raiden Specification — Raiden Network 0.2.0 documentation. [online] Available at: <https://raiden-network.readthedocs.io/en/stable/spec.html>
[Accessed 7 Dec. 2017].
- [24] Reitwiessner, C. (2017). zkSnarks in a Nutshell [online] Available at:
<http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf> [Accessed 23 Nov. 2017].
- [25] Sirer, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106–125). Springer Berlin Heidelberg.
- [26] Sompolinsky, Y., Lewenberg, Y. and Zohar, A., 2016. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. IACR Cryptology ePrint Archive, 2016, p.1159.
- [27] Sompolinsky, Y. and Zohar, A., 2015, January. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 507–527). Springer, Berlin, Heidelberg.
- [28] Son, M. (2017). Bitcoin's Rise Happened in Shadows of Finance. Now Banks Want In. [online] Bloomberg.com. Available at: <https://www.bloomberg.com/news/articles/2017-10-05/bitcoin-s-risehappened-in-shadows-of-finance-now-banks-want-in>
[Accessed 7 Dec. 2017].
- [29] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
- [30] VISA (2017). Visa Inc. Facts & Figures . [online] Available at:
<https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf>
[Accessed 20 Nov. 2017].
- [31] Yli-Huomo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), p.e0163477.
- [32] Dziembowski, Stefan; Faust, Sebastian; Kolmogorov, Vladimir; Pietrzak, Krzysztof (2015). "Proofs of Space". 9216: 585–605.
Available at: <https://eprint.iacr.org/2013/796.pdf>
- [33] Secg.org. (2010). Standards For Efficient Cryptography 2, [online] Available at:
<http://www.secg.org/sec2-v2.pdf> [Accessed 20 Jan. 2018].
- [34] Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151.