WHITE PAPER V1.0

TOS

基于SDAG的去中心化分层区块网络技术白皮书

TOS ThingsOpreatingSystem

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网络技术。该技术自动分发海量交易数据到分层区块网络，以减少全网区块数据容量，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（超级有向无环图），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

“cash, after millennia as one of mankind’s most versatile and enduring technologies, looks setover thenext15 years or sofinally 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，全称名为 ThingsOpreatingSystem，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络协议（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络协议生态圈。

(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；

创世区块：TOS 网络中第一笔交易生成的**区块**；

创世区块网络：包含**创世区块**的**区块网络**；

高层：根据离创世**区块网络**远近关系，相对近的**区块网络**层，**创世区块网络**层是最高层**区块网络**；

低层：根据离**创世区块网络**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**；

父区块：当前**区块网络**与**父区块网络**共用的**区块**；

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**；

子区块：当前**区块网络**与**子区块网络**共用的**区块**；

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；

累积总权重：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；

TOS TOKEN：TOS 在以太坊上的智能合约 ERC20 Token (Token 符号为 TOS)；

TOS COIN：TOS 公有链用来流通与交易的数字资产；

DAPP TOKEN：TOS 公有链上开发的 DApp 应用中使用的 Token，其 Token 的兑换及流通只能使用 **TOS COIN**；

(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-Huomo 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，矿工则更有可能是在旧块上进行采矿。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，而不是试图使用高延迟和低间隔时间去产生分链。

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，但其能量消耗和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。区块链会因为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) TOS DESIGN BACKGROUND
TOS 设计背景

上面我们讨论了现有的区块链技术的一些局限性，针对这些情况 TOS 的设计初衷是要做一个高可用的区块链技术，用区块链技术去解决物联网行业中海量数据存储、并发量高、交易成本大、数据的价值很难挖掘等痛点。

首先，TOS 的技术设计中，针对现有区块链技术成果进行分析，如 PoW 共识是一种非常大的浪费资源，通过消耗大量的电力来维持比特币网络的稳定，其交易的并发量比较低，并不是我们的理想模型；物联网中并发量高，交易成本大等问题也不是比特币技术所能解决的。但是，通过已有的 DAG 技术纠缠成区块网状结构给了我们很多启发。使用 DAG 技术构建的共识，可达到并发量高及交易免费。再加上现有成熟的 PoS 权益证明共识形成免费及付费相结合，在免费、付费类型和交易的矿工费基础上，把数据根据价值标签做分离能更好的去挖掘数据的价值。

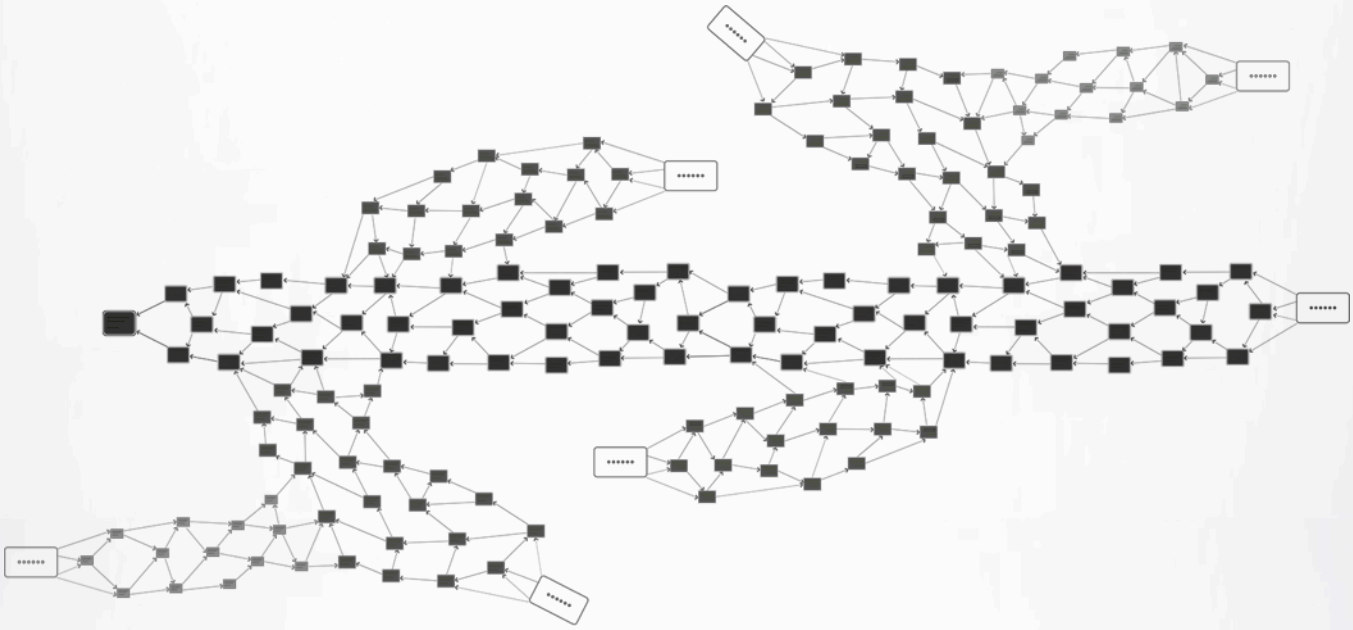
其次，使用现有 DAG 技术虽然可以做到高并发量及免费交易，但对于物联网中海量的数据存储、交易数据无法确定时长、数据的价值归类等问题是无法解决的，而在物联网中这些问题又是至关重要且不可忽视的。

最后，现有的公有链技术只是应用于数字货币的交易流通作用，还没有真正达到可企业级商业应用。从技术上讲，高可用的商业级公有链技术需要具备安全、可扩展、去中心等特性。由于在区块链技术世界里面有一个相互制衡的铁三角关系（安全、可扩展、去中心），三者很难兼顾。基于这种矛盾点，对现有的区块链技术进行了大量的分析，我们设计一些新的技术指标模型，例如区块网络经济价值，智能矿工费调节等等。在现有区块链技术上进行重新架构，于是就有了 TOS 的核心 SDAG 分层区块网络技术。

TOS 的分层区块设计，先把区块链里面所有区块由链拓扑成 DAG 区块网络结构，再由 DAG 区块网络分层为无数层的 DAG 区块网络，每一层的 DAG 区块网络都由区块里面的"父区块网络 hash"值链接关联，首先，区块纠缠成 DAG 区块网络，不同层级的 DAG 区块网络又形成一个的链条关系，链条中每个单元可以理解是一个 DAG 区块网络；然后，增加免费交易与收费交易相结合的机制，把交易数据根据价值标签做分离，越是重要的数据越会存储在更高层的区块网络；最终，这种密码经济学平衡机制保障商业活动的高可用，加上 TVM 虚拟机实现智能合约创造了基于 SDAG 的去中心化分层区块网络技术。

TOS 的设计解决区块数据冗余、交易性能及交易成本、数据的价值归类等问题，这只是一个可商用的公有链技术方案的开端，在这个生态系统中，未来我们的战略规划还包括全数据类型上链，区块数据存储激励，数据银行等，构建成一个完整的高可用的商业级公有链生态体系。

(五) INTRODUCTION OF TOS
TOS 基于 SDAG 的去中心化分层区块网络技术介绍



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": "0000000008e647742775a230787d66fdf92c46a48c896bfbc85cdc8acc67e87d",
"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 是区块累积总权重值，weight 为区块中交易的权重值。

权重及相关概念

我们定义，每个区块有自身权重、区块累积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，则新区块的累积总权重值为被验证的直接间接节点的累积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

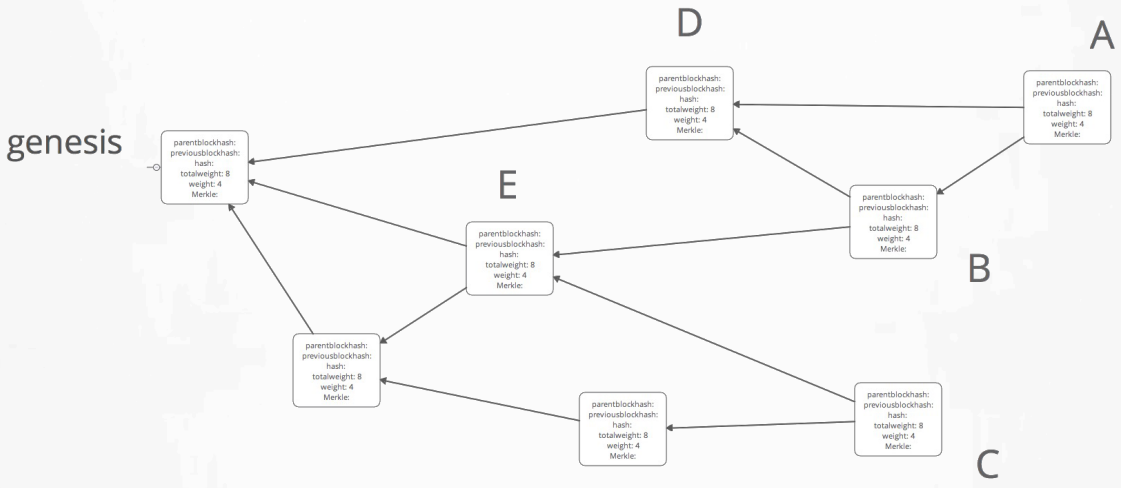
我们定义，每笔交易者自身可以通过验证区块网络中两个末端未被验证的区块，以生成的新区块并串联起之前的两个末端区块证明交易的有效。基于诚实节点不会直接或者间接地验证具有冲突的区块，那么随着交易的数量增加，当前区块会被越来越多的新区块直接或间接的交易自身验证，系统就会就趋向于安全稳定，换句话说就是一个交易被双花是极为困难的。Transaction 交易证明是由交易者自身验证，此过程中并不需要支付费用，所以 Transaction 验证生成的新区块 transactioncost 为 0。通过 TOS 的节点来接收交易，并将交易数据记录到区块链上，使区块链产生新的区块。TOS 节点在进行交易验证时，先通过 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网络的经济价值（此价值包括当前区块网络及全部子区块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量，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网络分层一个新的子区块网络并把新的交易写入子区块网络。达到了区块网络自动分层功能。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 区块网络自动形成不同层级的区块网络。每个区块网络只有当前区块网络及所有子层区块网络数据访问权限。同层级的区块网络数据不能直接交互，但可以通过对应的父区块网络通信数据。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网络有无数个小账本，子区块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。

(六) 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）。

基于 SADG 分层区块网络工作模式如下：

1）设置区块用于记录区块创建过程中的交易记录，采用 DAG 技术连接区块，多个区块相互连接构成区块网络，区块网络的经济价值包括区块网络中的节点数、记录的交易数量、交易金额和交易的矿工费等参数模型。通过 B-algorithm 算法(Block chain network economic algorithm)计算对应层级区块网络的经济价值，B-algorithm 算法数学公式是一个复杂的曲线函数，随着时间推移函数值必可达到一个阈值(evolveValue)，往后的时间内函数值 E(t)一定是大于阈值(evolveValue)的波动曲线。

2）设置区块网络的经济价值函数为 E，定义 α、β、γ、δ 为常量系数，当前网络的节点数为 N；其中，区块网络中的交易总数为 T，区块网络中的交易总金额为 M，区块网络中的交易总矿工费为 F，区块网络经济价值 E(t)数学模型公式如下：

$$E(t) = exp(\alpha N_t) + \left(\sum_{t:t \to t\prime} exp(\beta T_{t\prime} + \gamma M_{t\prime} + \delta F_{t\prime}) \right)$$

3）设置一个阈值(evolveValue)作为区块网络经济价值的临界值，并设置 S-mechanisms 机制(Smart miner fees regulatory mechanisms)智能矿工费调节机制，实现区块网络生成分层制度。在 S-mechanisms 机制的工作原理中，当某一区块网络经济价值小于临界值时，新区块通过 Transaction 共识交易验证写入该区块网络末端；当某一区块网络经济价值大于临界值时，新区块通过 PoS 共识矿工验证写入该区块网络末端；或者，新区块通过 Transaction 共识交易验证生成该区块网络的下一层区块网络，从而实现区块网络的分层。

4）不同层级的区块网络对应不同的交易规则，根据用户的选择对新的交易执行对应的交易规则，且不同层级的区块网络满足越早生成的区块网络层级越高，交易规则具体包括如下步骤：

- 若新区块写入最低层级的区块网络中，执行 Transaction 交易验证；
- 若新区块写入其他层级的区块网络中，执行 PoS 矿工验证；

Transaction 交易验证方法中，验证任意两个区块，并将验证结果与交易一起记录到新的区块中。PoS 矿工验证方法中，矿工缴纳保证金并下注到他认为下一个可以被写入区块网络中的区块，被写入区块网络中的区块由挖矿合约决定部分参与下注的矿工获胜并负责打包交易。若赌赢，则所有猜测正确的矿工拿回保证金并收取交易费用，同时验证任意两个区块；若网络中的矿工没有打包交易就等下一轮矿工生成的区块达成共识，则矿工将被扣除部分保证金，当矿工的行为违反系统中的相关规定时，保证金将被没收，同时也将被取消参与创建区块的资格。

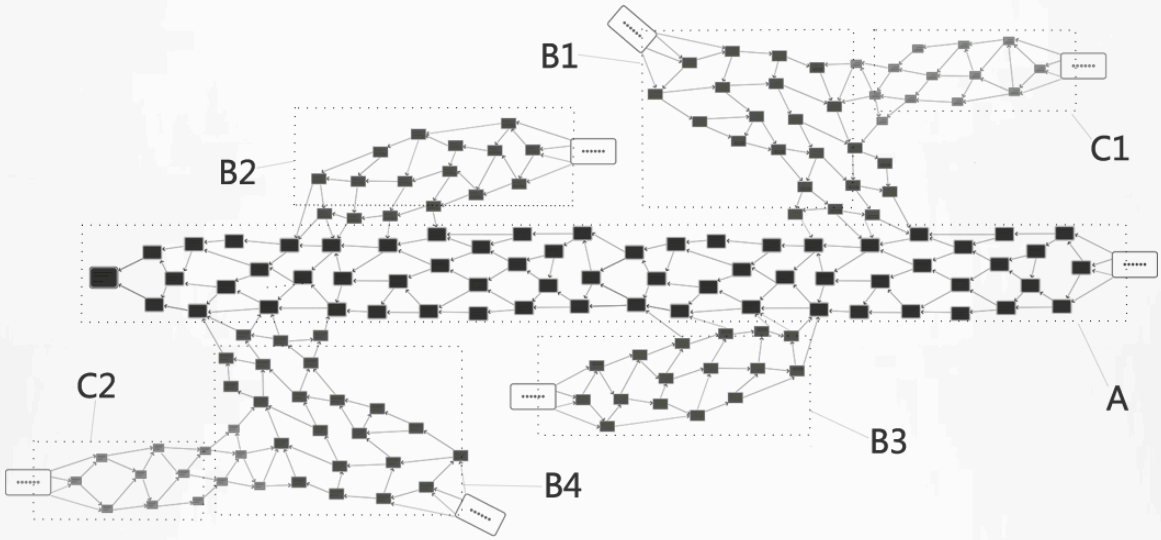
Transaction 交易验证和 PoS 矿工交易验证时，还会计算此区块的累计总权重值，累计总权重值为从创世区块到当前区块最长路径中所有区块的区块交易权重值的总和，创世区块为第一个生成的区块。

区块网络中区块的累计总权重值与该区块网络末端区块累计总权重值的差值的绝对值越大，表示区块被验证的次数越多，区块的安全性越高。累计总权重值为从创世区块到当前区块最长路径中所有区块的区块交易权重值的总和，路径指从当前区块沿区块验证的方向（即箭头的方向）到创世区块所经过的区块。

将交易写入层级越高的区块网络中，所需支付的交易费用越高。并且区块只能与当前所在的区块网络的区块、区块网络的父区块网络和区块网络的子区块网络的区块验证交易，父区块网络为当前区块的上一层区块网络，子区块网络为当前区块的下一层区块网络。

每笔需要记录的交易在系统中发送时，系统会标注为未验证交易，并会带有一个初始的权重值。当交易者参与网络中交易证明时，如果证明验证完毕，则新区块的累计总权重值为被验证的两个区块的累计总权重的最大值与当前区块权重值的和值。

当网络中的节点的数量和交易者的数量足够多时，TOS 网络的区块就形成了多个不同层级的区块网络，如下图所示，区块网络形成的越早，区块网络的层级越高；A 区块网络中的区块为最早形成的区块网络是层级最高的区块网络， B1~B4 为 A 区块网络的子区块网络，A 区块网络为 B1~B4 区块网络的父区块网络，C1~C2 区块网络处于当前区块网络的末层，为当前层区块网络的最低层；层级较高的区块网络在交易中逐渐衍生出多个层级较低的区块网络分层，以此类推，最终形成了类似于海洋、江河、小溪的区块网络结构。



各区块网络只会存储本层级区块网络中的交易账本，节点在同步区块链网络中的数据时，只需要同步节点所在区块网络及更高层级的区块网络中的数据，无需同步所有区块，从而可大量节省单个节点账本的存储空间，也极大的减少了节点储存负荷。根据用户愿意支付的交易费用，系统自动判断将交易记录在哪一层级的区块网络中，用户支付的交易费用越多，交易可以写入的区块网络的层级越高，交易数据的安全性就越高。同时，层级越高的区块网络中区块的安全级别越高，数据的价值越大，更有利于后期的数据管理和数据挖掘。

当用户选择交易费用为 0 时，执行 Transaction 交易验证方法，如当前区块网络经济价值大于阈值，将从当前区块网络的末端生成一个新的子区块，将交易记录在新的区块中，否则，将交易记录在当前的区块网络。当用户选择交易费用大于 0 时，执行 POS 矿工交易验证方法，系统根据矿工费自动判断交易写入对应层级的区块网络，用户意愿支付的费用越高，写入的区块层级越高。

SDAG 是一种并发量高，交易速度快，支持不同层级区块网络使用不同的交易类型的一种分层区块网络技术。最低层级区块网络采用的 Transaction 交易证明方法区块生成机制简单，交易并发量高；高层级网络采用的 PoS 矿工交易验证方法速度慢但交易安全性高，通过高层级区块网络交易方法和低层级区块网络交易方法的有机结合，克服了传统区块链交易方法中并发量小，速度慢和所有交易的地位均等的缺点。

(七) SDAG NETWORK FEATURES
SDAG网络特点

良好的扩展性

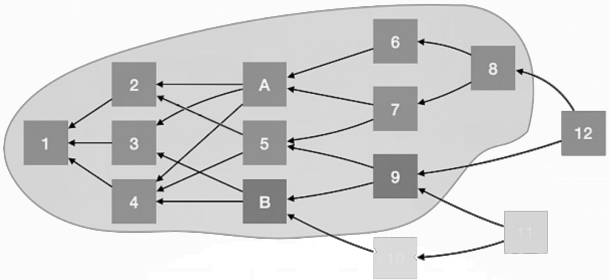
众所周知，由于 SDAG网络的分层区块机制，可以做到网络具有无限分层子区块功能，就像树根一样无限扩展延伸。在 TPoS 共识的区块网络中， PoS 负责验证带交易费用的数据，它的特点是安全性更高，越是重要的信息付出高交易费用就能写入越高层的区块网络；Transaction 交易自身验证，交易数据写入末区块网络，安全性相对比PoS 低，但是可以做到交易并发量高、吞吐量大。综上所述，SDAG 具有良好的可扩展性。

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，但如果是很有价值的数据，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。

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，

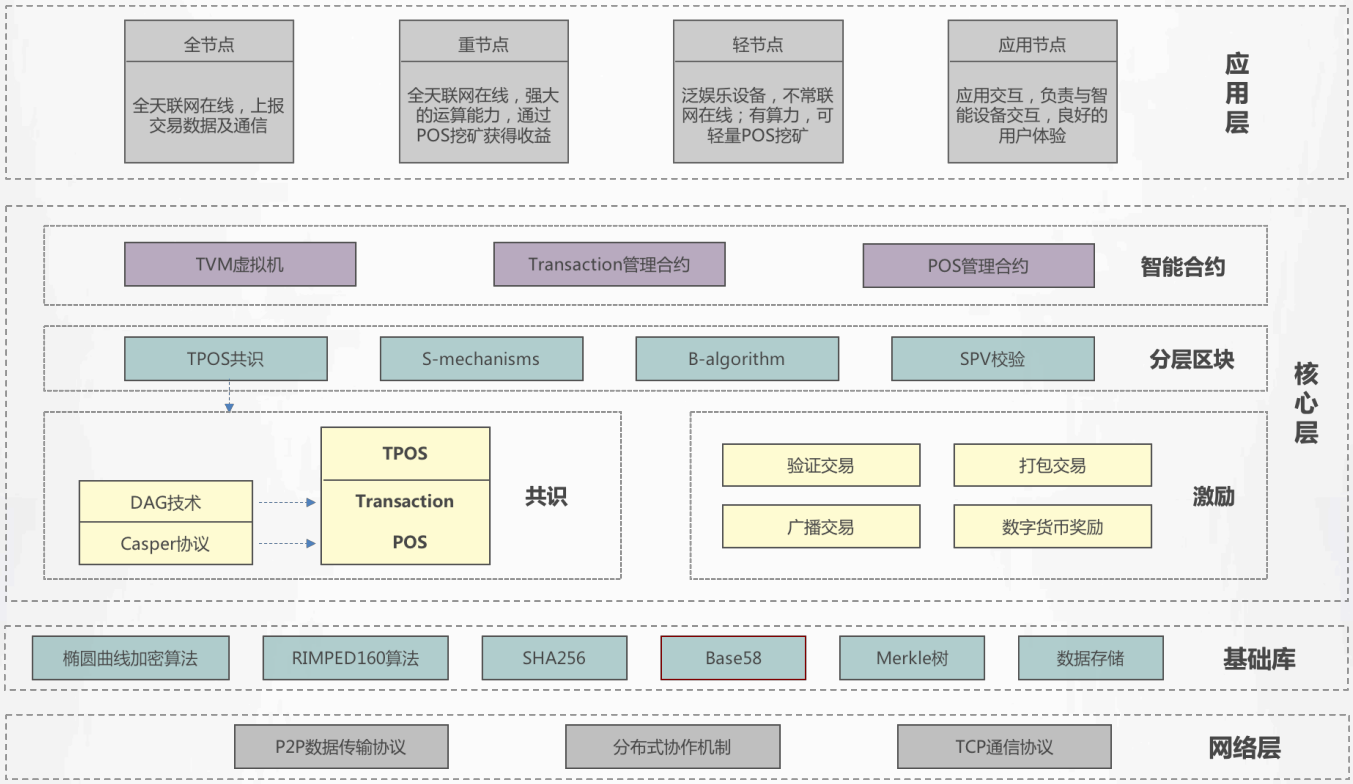


长江源头就是区块网络开始区，主区块网络如同长江主干道，区块网络上的无数分层区块网络如同长江主干道上的无数个支流，主区块网络分层的各子区块网络写入的新交易数据就如河水流入各支流。小河流之间不能直接流通，同理子区块网络也不能直接交互数据。但是可以使用反射功能，通过对应的父区块网络反查对应的子区块网络数据。这样数据是分层隔离的，因此每条子区块网络的数据总量是包含这条分层上所有父区块网络(如同:小沟–>小溪–>小河–>长江)。在网络系统中区块数据隔离机制，可以大大的减少全网区块数据冗余，从而减少了单节点的数据容量，系统的负载也会变轻。可以预测经系统运行一定时间后，交易数据经过系统机制越是重要数据越会存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

(/\) TECHNOLOGICAL INNOVATION

TOS 技术架构图&技术创新

TOS 技术架构



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。记录在高层级区块网络，流通性更好，安全保障更高。

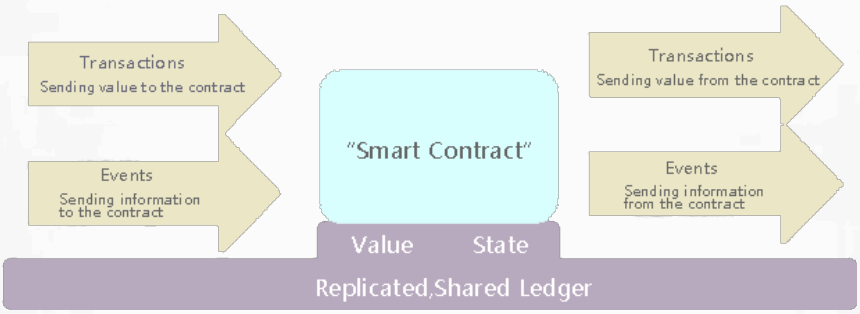
2) SDAG 拥有无限分层区块网络能力

SDAG 通过 S-mechanisms 机制与 B-algorithm 算法实现区块网络分层。B-algorithm 算法监控区块网络的经济价值，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网络分层一个新的子区块网络，并把新的交易生成的区块写入子区块网络，达到无限分层区块网络能力。

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

根据物联网的分层体系结构，TOS 分别针对感知层、传输层和应用层设计了对应的标准协议，确保在物联网的每一环节和层次都得到安全防护与管理和控制，从而保证数据安全和信息的公开与透明。

5.1) 感知层

感知层通过电子标签、RFID、射频或近场等技术进行识别，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。

(九) 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为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种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。

(十) 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

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，合约资源集合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。

–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

–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。看房时在网上进行预约，预约成功暂扣 1 个月房租担保金，并将在 1小时内有效的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，租房免押金，租金每月定时扣 DAPP TOKEN，并将门锁密码设置成租客专用，房租缴纳逾期门锁自动换密码。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

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。

–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

•支持超小额支付和超低手续费交易，方便小额支付，满足数据碎片化的交易需求

–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 DAPP TOKEN，可以用DAPP TOKEN 在 4S 店冲抵保养费，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 TOS COIN，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产品及私募、众筹、债券等合约。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，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

–举例：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Token。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Token 结算，保障参与者获得收益内容。

物联网大数据交易平台

TOS 数据交易平台作为 TOS 生态中的 DApp 应用方，其 DAPP TOKEN 是 TOS 系统中交易的重要基础。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。

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。TOS 的数据交易平台目前包括 2 个核心模块：智能广告传播和数据交易中心。

1）智能广告传播

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）数据交易中心

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，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。通过智能金融服务、智能合约系统、数据交易三大板块，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私募、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 区分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。

–特色：

•解决智能硬件企业的金融服务问题

•提供从数字股权、数字产品、数字债券等智能合约内容

–举例：某智能硬件公司产品需要大量的研发费用，传统的金融服务成本又高。利用TOS 的智能硬件合约，可以直接基于硬件产品进行数字化，其数字产品可被当作支付媒介获得对应的 TOS COIN，最终帮助企业获得研发费用。企业产品研发成功后，通过售卖产品得到 TOS COIN，再用 TOS COIN 通过智能合约回购硬件产品。

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。

–特色：

•提供智能物流的数字化商业流转

•智能物流中的物流、金流与信息流三者相结合

–举例：某个运输公司，可以使用智能物流平台 DApp 进行数字化物流。首先，运输公司在 TOS 智能物流平台中需要交纳一定数量的 TOS COIN 作为信用保证金；之后，运输公司就可以承担物流环节的运输工作。当运输公司在规定地点收到指定的货物时，在 TOS 系统中非质同 DAPP TOKEN 自动转移到运输公司账户上，非质同 DAPP TOKEN 的信息记录着货物的信息，用于检验货物，保障货物可回溯不被调包，货物交割后运输公司将收到相应的 TOS COIN 作为服务费用。整个物流过程中可做到全程公开、透明、安全，又能提高效率，雇佣双方的成本也能得到最大的降低。

(十一) TOS ECOSYSTEM AND VALUE
TOS 的生态系统及价值

上面讲到 TOS 的应用场景可分为四大块: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，通过这四大块构建 TOS 的生态系统。

1）例如在企业级智能硬件平台中，主控类智能合约可以应用于房屋租赁的共识经济，根据租房的市场需求在 TOS 系统里面可以开发对应的租房 DApp 应用，DApp 应用中的 DAPP TOKEN 做为租房用来结算，把用户的需求和结算在 TOS 应用中形成一个闭环，也可以间接增加 TOS COIN 的流通性。

智能设备是数据生产方， 可以通过数据售卖获得 TOS COIN，并且在 TOS 系统中存在大量的全节点设备，它们 24 小时连接在 TOS 网络中。因为 TOS 中的 PoS“虚拟挖矿”机制，所以一些具备一定算力且存储能力较强的设备是可以进行 PoS 挖矿的。在生态系统中，早期设备可以产生数据、售卖获得 TOS COIN，再用 TOS COIN 进行 PoS 挖矿，这些设备的工作能为 TOS 网络带来稳定，同时设备的自造血能力也可以刺激整个生态中更多的智能设备参与到其生态环境中， 形成互利互赢。

TOS 的智能合约， 可以创建设备数字化、股票数字化、私募股权、众筹、债券等金融衍生品。例如，智能设备厂商可以针对每个不同类型的设备， 铸造发行非质同 DAPP TOKEN (既每个 Token 的价值是不一样的，且不可分割)，也可称为数字化商品。链上交易，用户从厂商购买非质同 DAPP TOKEN，其真实的设备被托管在厂商，由厂商负责其安全，用户提取智能设备时，需要提供私钥生成设备数字摘要和链上的非质同 DAPP TOKEN，由设备厂商验证设备数字摘要真实有效性之后，把数字化商品对应的非质同 DAPP TOKEN 进行销毁。这样，每个设备都可数字化成一种数字商品，通过 DAPP TOKEN 流通起来，买卖智能设备可通过交易对应数字化商品 DAPP TOKEN。区块链技术不可篡改的安全特性，保证数字化商品的唯一性，智能设备的市场流通，都可以通过交易其设备的数字化商品的所有权，TOS 在其中它是一个实现价值交换的去中心化技术平台， 也是价值互联网的基石。

2）例如在物联网大数据交易平台中，TOS 的数据交易是 TOS COIN 流通的基础。TOS 的网络中存在海量的数据，设备厂商可以建立采集数据、销售数据的渠道，把这些设备生产的数据通过拟定数据交易合约，实现数据的价值交换并自动完成结算，同时结算的 DAPP TOKEN 自动转入涉卖方的账户。可以根据用户的数据画像精准定位用户，更高效、更透明的将广告与目标消费者匹配达到推广效果。如智能广告应用在 TOS 网络中的电视、冰箱、汽车等等都是其生态系统中的一部分， 智能广告应用可以在 TOS 网络中将用户的个人交易数据进行采集和分析，当然 TOS 也会把用户的个人隐私信息，包括 ID、姓名、详细住址等等进行严密保护， 最后广告主能在各智能设备上精准的对目标用户的筛选及提高推广效率。同样， 其数据唯一性和确定性也会被保障， 并且一旦应用中数据交易成功， 也将不可篡改。

TOS 为海量的设备生产方提供了一个良好的商业环境，对于整个物联网行业来说，有了一个可大量交易设备数据的实际场所。TOS 系统的数据交易可提供流通性， 结合其下游环节分析挖掘数据， 最后成为数据生产、加工、售卖、等一体的数据商业价值应用，也就是说 TOS 在数据交换及智能设备行业中都拥有着巨大的价值。

3）例如在智能金融服务平台中，为智能硬件企业提供了产品数字化、产品研发、上线等一条龙解决方案。通过企业级智能硬件平台、数据交易平台、金融服务平台三大板块，以智能硬件为入口融合在一起，从生态体系上帮助传统硬件和家电企业，解决金融方面的问题。硬件企业可以在 TOS 系统中数字化硬件产品，通过将数字化商品作为支付媒介的方式获得对应的 DAPP TOKEN，把 DAPP TOKEN 与硬件设备绑定，硬件设备本身具有价值，所以对应的 DAPP TOKEN 也有价值。由于 DAPP TOKEN 之间的流通只能使用 TOS COIN 做为交易费用，间而带动了 TOS COIN 的流通，TOS COIN 的价值也是随着对应的需求关系而增涨。

4）例如在智能物流平台中，从仓储到配送每个环节都较繁琐，涉及的人员众多，针对这些特性，在 TOS 中将货物数字化为对应的非质同 DAPP TOKEN，货物在物联网的各个商业环节中流转，就必须在 TOS 网络中使用非质同 DAPP TOKEN 交易，同时也需要使用 TOS COIN 在每个物流过程的交易环节中进行费用支付与实时结算。比如说跨境物流，TOS COIN 的使用可以实现自动海关申报、税务计算和整条供应链的快速结算，且不会出现各国汇率兑换的成本问题。TOS COIN 在整个物流供应链中的流通记录将被记录在区块链中，实现对物流业务的信息流、物流、资金流等三流合一的数字化管理。随着平台的发展，TOS COIN 需求量会不断增大，TOS COIN 的价值也会越高。

(十二) TOS FOUNDATION
TOS 基金会

TOS（ThingsOpreatingSystem）项目是由基金会驱动的全球性智能物联网络开放协议项目。

TOS 基金会的设立

基于 TOS 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

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 TOS 社区决策委员会根据持有 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 平台推崇去中心化的 DAO(distributed Automomous Organization)治理模式，认为所有 TOS 项目参与者，共同享有 TOS 平台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，投票事项限于 TOS 平台，不涉及 TOS 基金会。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；同时，TOS 数字通证持有者的权限仅限于 TOS 平台相关事宜，对 TOS 基金会的组成及决策不享有任何决定权。

TOS 审计

TOS 基金会将保持高度的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 TOS TOKEN 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。

(十三) ROAD MAP
开发工作路线图

Q3 2017 年

第 1 阶段

基金会成立
TOS FUNDATION
核心团队成立
TOS GROUP

Q4 2017 年

第 2 阶段

开发 TOS 核心技术
DEVELOPING TOS CORE TECHNOLOGY

Q1 2018 年

第 3 阶段

TOS 早期基石投资
TOS 项目私募
TOS CORNERSTONE INVESTMENTS AND PRIVATE PLACEMENT

Q2 2018 年

第 4 阶段

TOS 基础模块完成测试
Transaction 共识完成测试

Q4 2018 年

第 5 阶段

POS 共识完成测试
SDAG 完成测试钱包完成测试

Q1 2019 年

第 6 阶段

TOS 代码审查和审计
TOS V1.0 上线测试
第一个物联网合作伙伴入驻

Q2 2019 年

第 7 阶段

智能家居/智能物流的端到端测试
硬件提供商与 TOS 的整合

Q3 2019 年

第 8 阶段

TOS 2.0 版本上线

(十四) DISCLAIMER
免责声明

特别声明：下文中 TOS TOKEN 的所有免责条款同样适用于 TOS COIN。

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 TOKEN 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，不以任何方式涉及公开发行股票或融资，亦不以任何方式涉及在任何司法管辖区的证券发售。TOS TOKEN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 TOKEN 并非本基金会的贷款。TOS TOKEN 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。无论通过 Token 发售还是其他途径获得 TOS TOKEN，并不表明向 TOS TOKEN 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 TOKEN 未授予参与本基金会或其资产的权利。TOS 基金会未向 TOS TOKEN 持有人提供本基金会的任何所有权或其他利益。获得 TOS TOKEN 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）。TOS TOKEN 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 TOKEN 不可退款。本基金会不会出于任何原因为 TOS TOKEN 持有人提供与 TOS TOKEN 相关的退款，TOS TOKEN 持有人不会收到代替退款的金钱或其他补偿。关于 TOS TOKEN 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 TOKEN 拥有任何特定价值的保证。

(十五) APPENDIX

附录

TOS TOKEN & TOS COIN 功能描述

[1] TOS TOKEN(TOS ERC20 Token)享有 TOS 公有链的数字货币(TOS COIN)等权作用；

[2] TOS TOKEN(TOS ERC20 Token)与 TOS 数字货币(TOS COIN)都可参与 TOS 自治化投票选举委员会；

[3] TOS TOKEN(TOS ERC20 Token)是数字资产，在 TOS 公有链协议的初始阶段发布和出售，以资助其项目的研发；

[4] TOS 公有链上线，TOS TOKEN(TOS ERC20 Token) 享有 1 比 1 兑换成 TOS 公有链的数字货币(TOS COIN)；

[5] TOS 公有链中交易的邮费需要消耗 TOS 数字货币(TOS COIN)；

[6] 基于 PoS 挖矿共识，需要 TOS 数字货币(TOS COIN)；

[7] TOS 数字货币(TOS COIN)可以在 TOS 公有链上具有数字资产流通作用；

(十六) 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 InternationalConference on Financial Cryptography andData 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-PeerComputing (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-miningelectricity-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-Huumo, 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.