链接价值 链接时间

TSC

白

皮

书

基于区块链节点的通讯资源交换社区

目 录

摘　要

中心化网络的数据安全、隐私保护、数据所有权等问题，使得中心化网络越集中越无法控制，区块链技术的兴起正在逐步解决这种问题，而当前的区块链网络除了交易处理性能无法满足正常的商业流程需要以外，也无法解决点对点对等安全的网络通信问题。

TSC 基于端到端的安全通信技术，致力于提升区块链点对点对等网络的业务的支撑能力和应用落地，从区块链的基本交易入手，以链接价值为目标，为每个参与者提供基于对等网络技术的安全通信能力。

1. 背景

1.1. 全球即时通信领域

即时通信（Instant Messaging,即 IM）是指能够即时发送和接收互联网消息等的业务。随着时代的发展和科技的进步，即时通信不再是一个单纯的聊天工具，它已经发展成集交流、资讯、娱乐、搜索、电子商务、办公协作和企业客户服务等为一体的综合化信息平台。随着移动互联网的发展，互联网即时通信也在向移动化扩张。目前，微软、AOL、Yahoo 等重要即时通信提供商都提供通过手机接入互联网即时通信的业务，用户可以通过手机与其他已经安装了相应客户端软件的手机或电脑收发消息。

腾讯 QQ、微信是基于强大用户基础创造出强有力优势的通信领域生态圈，中国网民惯用的即时聊天工具腾讯 QQ 从 1999 年 2 月诞生到现在，注册用户已超过 8 亿，现阶段每天同时在线人数约在 2 亿。

腾讯 2018 年第一季度发布的财报中显示，微信以及 QQ 的合并账户数超过 10 亿，这两款即时通信工具为腾讯公司带来了丰厚的收益与口碑。

Facebook 是美国目前最大的社交网络服务网站，于 2004 年 2 月 4 日上线，2012 年 3 月 6 日发布Windows 版的桌面聊天软件Facebook Messenger（飞书信），主要创始人为美国人马克·扎克伯格。Facebook 是世界排名领先的照片分享站点，截至 2013 年 11 月每天上传约 3.5 亿张照片。截至 2012 年 5 月，Facebook 拥有约 25 亿用户。

上述公司都拥有海量的用户群体，并在用户手里获得丰厚的报酬。庞大的用户群体和海量的用户数据把用户信息的安全性、隐私性等问题变成必须解决的问题，而这个问题在传统的技术中是很难解决的。下面将一一阐述这些行业痛点， 并说明如何利用区块链技术加以解决。

1.2. 即时通信的中心化痛点

1.2.1. 数据的安全性

以中心化服务器为基础的互联网面临着数据安全性的挑战，互联网已几乎成功的连接了在其网络上的所有用户，但这同样也引起了人们关于隐私和数据安全性的担忧。手机应用每天被用于处理海量的数据流，而所有数据都经由一个有中心节点的中心化的服务器传输。在这类中心化系统中，侵入一个中心连接节点是很方便的，这会提供给不法分子浏览海量网络数据的通道，同时也给黑客盗取或者篡改数据提供了机会。现在，用户几乎没有办法在使用网络的同时避免隐私泄露或被黑客攻击的风险。

随着计算机和网络技术的发展，数据的存储模式也由个人集中式的存储发展为分布式存储——分布式存储就是将数据存储在多台独立的存储服务器上。分布式存储通过备份、冗余编码等手段，可以提高系统的可靠性、可用性和存取效率， 还易于扩展。因此，越来越多的用户将自己的大量数据外包给存储服务方进行分布式存储。这种模式在给用户带来方便和快捷的同时，也带来了新的问题。由于分布式存储通常以提高可靠性为目的——为提高可靠性，存储数据的一般方法是

通过编码增加冗余信息，利用纠删编码的原理，对数据进行纠删编码，将编码后的各个数据片段分布式地存储于异地的存储服务器中。因此，用户对于可以不用担心个人信息被泄露、安全通信的分布式不可破解网络的需求愈发强烈。

1.2.2. 用户隐私权和数据的所有权

不论个人还是企业，对信息所有权利都很看重。有些数据是可以公开的，有些则需要保密，分清这两类信息是保护信息隐私的起点。隐私权法往往将隐私数据和公共数据严格分开，但在现实中，公共数据和隐私数据的界限并不总是那么明确，这对如何在法律上区分进行造成了很大的困难。这种法律上区分，至少在最初阶段，就是找出谁是数据的初始所有者。确定究竟是谁对数据拥有所有权将成为分析的主题，辅助确定可能需要联系或分析的对象，以明确他们对数据隐私的要求。

现有的网络很容易被屏蔽或盗用，而且用户没有自己数据的所有权。当涉及到互联网交易时，用户信息的使用并不能被有效地控制。这些信息在用户使用巨头们的服务时，被要求同意留存在服务器上，而信息的归属实际上已经默认成了服务器的所有者，也就是这些互联网服务巨头们。与此同时，巨头们利用这些数据迅速提升自己的服务水平和竞争优势，不断发掘数据的更多潜在价值。毫无疑问，数据的价值是巨大的。然而，鉴于这些数据引起的用户隐私泄露的担忧无处不在，用户也无法分享数据产生的价值。

1.2.3. 中心化通信集权焦虑

中心化通信造成舆论控制的焦虑越来越强烈。不管是推特还是脸书，还有微信等全球通信巨头，对于用户数据的分析挖掘，已经逐步超越商业用途，开始影响舆论走向。目前，社交网络上的聊天机器人十分流行；这种控制通信账号的自动化系统，可以根据用户的特性，有导向地增强某些舆论方向，并能够推送给更容

易接受所倡导观点的人群。这些聊天机器人会污染线上舆情，甚至控制思想情绪。最近，已有研究课题专门讨论如何控制量化机器人通信系统。

除此之外，用户账户的所属权可能也是个问题。某互联网巨头所制定的规则中提到，该公司可根据相关使用条款，在一定条件下收回、注销用户账号。

研究表明，通信巨头对数据的挖掘、分析和应用，能够毫无痕迹地影响被分析人群的讨论观点。

- Facebook、WhatsAPP 和 Google 在中国境内是被禁用的。（India Today, 2017）
- WhatsApp 最近在群聊中被发现设有“后门”。（Greenberg, 2018）
- WeChat 微信监控用户的会话，并在多个设备上同步。 （WeChat, 2018）
- Telegram 积极地监控内容，并在不久前被伊朗禁用了。（Toronto Star, 2018）
- Facebook 和 Google 将用户活动分享给广告商们。（Facebook, 2018; Google, 2018）

1.3. 区块链和通信的窘境

比特币刚诞生的时候，并没有“区块链”这个概念，人们用 bitcoin（小写 b）表示比特币，用 Bitcoin（大写 B）表示其底层技术，也就是现在的区块链技术。2015 年，经济学人发布了封面文章《重塑世界的区块链技术》后，区块链技术在全球掀起一股金融科技狂潮，世界各大金融机构、银行争相研究区块链技术，仅 2016 年就有数十亿美元投资到区块链相关企业当中。2017 年 9 月，中国政府网（www.gov.cn）发表文章《我国区块链产业有望走在世界前列》，公开支持区块链技术发展，并向 13 亿中国人民普及了区块链技术。区块链在金融、保险、零售、公证等实体经济领域的应用开始加速落地。

区块链有几大特点，其中之一就是全球流通。区块链首先是基于互联网的，只要有互联网的地方，区块链就可以进行流通。这里的互联网可以是万维网，也 可以是各种局域网，所以，区块链是全球流通的。区块链的第二大特点是匿名性， 即无法知道别人的区块链资产有多少及其转账记录，这种匿名性是分不同程度的。

区块链的第三大特点是记账去中心化。发起转账时，不会因为记账机构要放假，所以延迟几天到账；不会因为记账机构要盈利，所以要付很高手续费；更不会因为记账机构作弊，而受到损失。

点对点对等网络的流行，在全世界掀起一股商业协同模式的革命热潮。全球各种商业组织和政府机构都对对等网络技术寄予厚望。遗憾的是，目前的区块链网络对于承载正常的商业应用仍然力不能及，特别是在性能上更是差强人意：比特币网络 1 秒钟仅能完成 7 笔交易，而以太坊 1 秒钟仅能完成 15 笔交易。智能合约的兴起，让人们对点对点对等网络的应用落地充满期待。但是，目前的 DAPP 也仅能完成简单的游戏和交易功能，更复杂的功能都受限于网络的吞吐量和协同能力。

区块链唯一成熟的货币化应用——数字货币正在全世界发展得风声水起。然而，让区块链从业人士诟病的，是其仅仅实现了为点对点对等网络对价值的转移提供了良好的支撑，并保证了安全性，但更多的商业应用仍留在了中心化网络上。对此，虽然点对点对等网络不得不在各种监管和政策的变化中不断调整，却始终没有解决商业闭环交流上的安全性。

安全的通信环境，正是点对点对等网络亟待解决的商业闭环上的关键问题。点对点对等网络实现的通信网络，将会解决当前中心化通信网络的集权焦虑，同时，通信应用也将突破点对点对等网络的性能瓶颈，最终推动端到端的安全通信和点对点对等网络的迅速普及。

1.4. 区块链技术构建点对点对等信任网络

自中本聪实现比特币网络开始，区块链通过共识算法、共有的公开账本、点对点对等网络，创造了一个分布式的可信网络原型。在此基础上，各种公链不断提高点对点对等可信网络的应用范围、改进共识算法、提高网络共识协议的确认效率，点对点对等网络正在逐步解决中心化网络的集权焦虑问题。

点对点对等网络的特性能够有效降低当前商业流程中的信任成本。一般商业

行为需要参与方通过自律保证交易的最终完成，一旦有欺诈行为，参与商业交易的另一方将损失惨重。在中心化网络特性下，只有超大的集权系统才能获得较为稳定的信任基础，而参与商业应用的其他中小主体，则需要承担较大的信任成本。

对等网络技术的出现，使得参与商业行为的任何主体都同样可信，并且信任成本很低。通过区块链、智能合约、零知识证明等对等网络技术的应用，点对点对等网络上的商业运营成本将逐步降低，以此推动社会优化生产关系，并提高生产力。

2. TSC

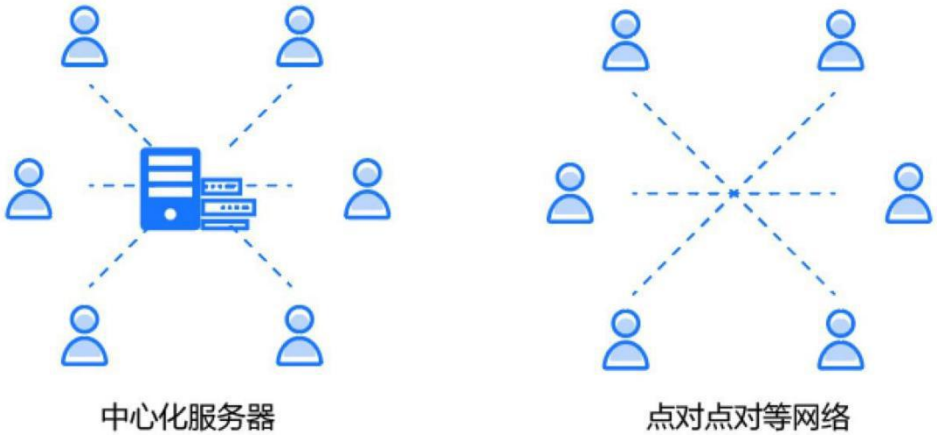
2.1. TSC 是什么？

TSC 正是为了完成点对点对等网络商业闭环而生的安全即时通信平台。它颠覆了传统的封闭范围的通信，让线上交流真正回归于点对点安全通信。

TSC 团队一直致力于推动点对点对等网络在通信领域的应用落地。在解决点对点对等网络吞吐量问题的基础上，推出基于点对点对等网络的安全即时通信平台。

传统意义上，通信平台依赖于一个中心化的服务器来处理信息和储存客户间的数据交流。然而，基于区块链的点对点对等网络，信息不再集中储存在单

一地点。因此，网络黑客不可能一次性盗取大量用户数据，网络罪犯也无法再通过潜入单一中心服务器的方式来控制整个系统。进一步说，黑客或其他网络罪犯如果想把信息从区块链上抹除、更改、迁移到别处，或以任何其他方式干扰整个系统，都将变得极其困难。分布式系统所使用的不可篡改的共识技术创造出一个透明且安全的框架，这个框架还有着广阔的应用场景。



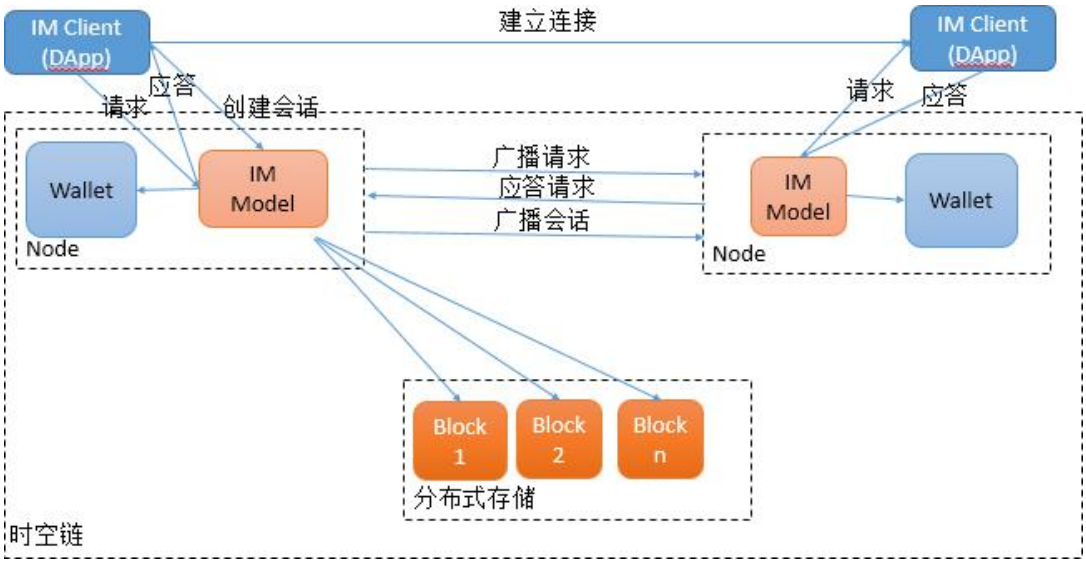
TSC 基于点对点对等网络的即时通信，同时还保证了用户的隐私和数据所有权。通过特有的共识性算法和自定义用户名的匿名认证方式，用户将保留个人信息、数据和通信交易的所有权。用户可以自己构建众人参与的社区，或同其他用户进行一对一会话，而这些内容都将是私人且保密的。这个网络将允许客户通过发送信息、通话、视频、文件传输等方式，进行无缝 P2P（端到端）交流， 并能够提高用户在通信、身份管理和无限安全通信交易等方面的体验。通过分布式区块，TSC 网络能够在根本上解除当前互联网通信系统中的安全风险，并将持续采用新型的安全技术。

由于区块链技术本身的加密特征，TSC 这种新型聊天通信手段有机会将私人通信提升到军事级的水平，而这种提升并不需要付出巨大的研发使用成本。也许，这就是区块链即时通信工具相比于传统互联网即时通信工具最大的一个竞争力。

2.2. TSC IM 和 TSC Token

TSC IM 是基于点对点对等网络实现即时通信 DAPP 应用，TSC 将构建一个点对点对等的通信网络，补全点对点对等网络中关键的商业环节，进行安全地沟通。

TSC IM 为每个用户创建一个点对点对等网络钱包地址，作为通信网络中用户的唯一 ID，该 ID 可用于发送消息，也可用于发送智能合约或者数字货币。TSC IM 在点对点对等的安全通信网络中运行，该网络基于端到端的安全通信算法构建，性能高效。



当两个用户进行通信时，发起通信的用户通过 TSC IM 生成一个连接请求，连接请求通过整个共识网络同步到接收方；接收方收到请求后，生成一个应答交易；接请求和应答请求都包含双方的签名，确保双方可信。请求方收到应答交易后，开始创建加密的通信连接；共识网络为该连接创建一个由双方签名的密钥， 该密钥对通信连接进行加密，在连接双方都在线的情况下创建成功，并开始进行通信。使用 TSC IM 通信双方发送的消息都使用会话密钥进行加密，根据会话创建相应选项，确认消息的保存或是销毁。

TSC IM 请求方发起连接交易时，如果接收方不在线，连接将无法建立。用

户可选择发送离线消息给接收方，接收方上线后会收到离线消息。离线消息也可以设置超时销毁。TSC IM 的消息都将使用安全的分布式加密存储，仅会话双方可以查看该会话存储的消息内容。TSC IM 可以发送文字、图片、语音、视频、文件、智能合约等多种消息类型，这些消息都基于加密通道传输。

TSC IM 非常适用于商业活动中的沟通场景，例如甲公司和乙公司可以在 TSC IM 的可信安全网络中，就合作协议细节进行充分沟通，并保证沟通消息不会被传播。

TSC Token 则用于支持在即时通信平台中进行价值的转移和核心功能的运营。除了发送、接收消息，TSC IM 同时也是 TSC Token 的钱包，可以存储和控制资产。TSC Token 用于激励参与 TSC IM 点对点对等网络的建设，构建更丰富的基于点对点对等网络的通信应用。通过引入 TSC Token，TSC IM 点对点对等 通信经济网络可以解决当前中心化集权网络中的激励错位问题；同时在治理层面， 赋予网络中持有TSC Token 的参与者一定的权利，赋予他们发声的机会和能力， 来影响未来通信经济网络的发展方向。

传统的通信网络的一个主要缺点，即用户对于网络本身基本没有影响力，他们在平台上没有发言权，仅能使用平台提供的现有功能。TSC IM 和 TSC Token 的目标则是使这项权利大众化，通过点对点对等网络的共识算法，用户能够通过拥有 TSC Token，直接对网络中的一切进行决策，包括软件功能的开发。

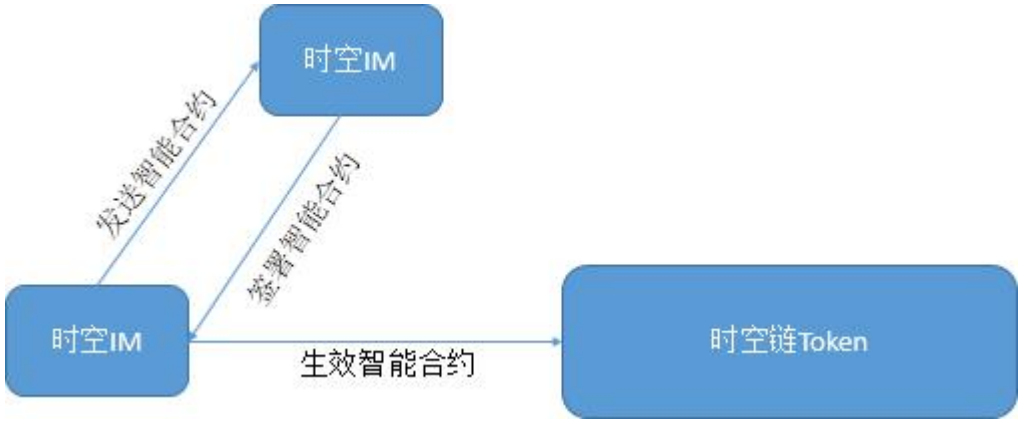
TSC Token 的核心功能是让用户能够享受优质安全的点对点通信，从而在点对点对等网络中完成商业应用中每一个环节的交互。同时，TSC Token 也使核心用户能够选择、决策自身所使用中的点对点对等通信网络软件的开发方向。不仅持有 TSC Token 的用户可以提供建议决策，任何用户均可提出建议，而 TSC Token 的持有数量则是衡量的表决权重的依据，同时其建议内容并不会影响该权重。

TSC Token 让用户在平台软件开发方面做出关键性决策，用户也可以通过设置赏金来激励某些功能的开发。TSC Token 基金也将在通信网络平台设置赏金，

来奖励平台的代码贡献者。基金和 Token 持有者相互协作，共同影响通信平台的开发方向。

默认情况下，用户可以在 TSC IM 平台免费发送小数据量的消息内容，用户的身份通过 TSC 公钥鉴别。用户的状态，包括是否在线状态，通过交易形式在 TSC IM 网络传播存储。TSC Token 在资产链存储，而 TSC IM 网络和资产链独立互通。

2.3. TSC IM 和智能合约



TSC IM 除了发送和接收消息及数字资产外，还能发送、签署智能合约。商业社会每一次交易，实际上都是对一个合约的履行。TSC IM 通过对智能合约发布和签署的支持，完成通信经济网络的搭建。TSC IM 双方或者多方，可以在点对点对等网络中创建和发布智能合约；智能合约在签署之前，仅存在于安全的分布式存储中，智能合约的参与方可以在 TSC IM 中通过安全高效的沟通和协作，共同完成智能合约的调整，最后通过 TSC IM，发起共同签署。智能合约签署后，将在 TSC Token 的资产网络生效，但是交易的关键数据并不对外公开，仅合约参与方可以查看智能合约协议的具体资产及数据内容。

TSC 通过非对称多重密钥加密的方式存储智能合约，但智能合约的执行条件是显示可见的，并不加密。智能合约的资产交易部分严格加密，仅对合约参与人可见。

TSC 智能合约的签署能力，在点对点对等安全可信的基础上，大大降低商业社会的线下合约签署成本，为商业化通信网络提供了新的方向。

2.4. TSC 技术特点

2.4.1. POW+POS 混合证明机制

TSC 采用POW+POS 混合证明机制，POW 矿工来创建区块搭建区块链；POS 矿工来确认这些区块的合法性，保护用户的权益。公平地按持币数量与工作量分配投票权重，可以实现社区自治。在社区里，开发者与爱好者可以提出改进或者增加现有功能。通过社区投票来决定执行与否，即聚集群体智慧，进行决策与执行。

实现具备：参与性（participative）、协作性（collaborative）、合作性（cooperative）、分布式（distributed）、去中心化的（decentralized）、自治的（autonomous）的高效社区。以混合机制来实现广义上 DAO（去中心化自治组织）的高效运行。采取混合机制使得数字货币的持有者可以直接参与项目的重大决策，而不需要购买昂贵的矿机。

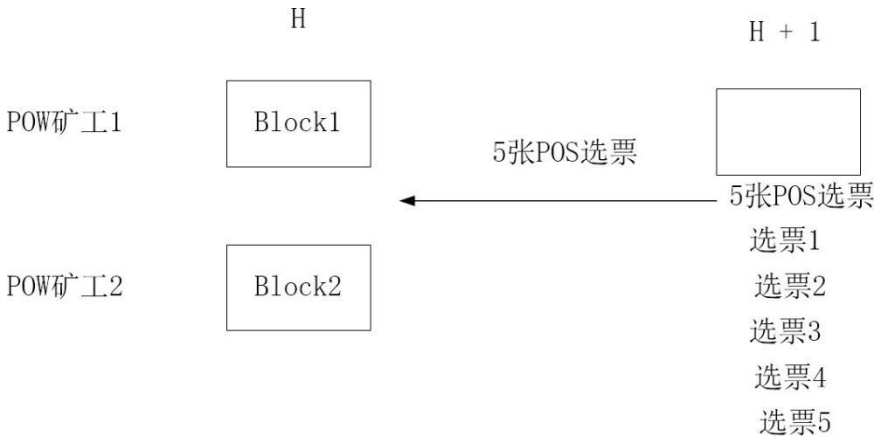
采用混合共识机制后，通过 POW，使得 TSC 有挖矿的硬性成本作为币价的保证。矿工是几乎不会低于成本价出售数字货币的，而随着算力的提高，不断上涨的挖矿成本也会使币价处于稳定向上的状态，又制约了单独 POS 机制里数字货币过于集中的问题。

另一方面，POS 让中小投资者着眼于项目的中长期的发展，中小户更倾向于把币放在钱包里进行 POS 而不是放在交易所随时准备交易。这使得 TSC 生态更加健康，人们会将注意力更多的放在 TSC 技术与落地应用上，而不是仅仅关注短期的价格波动。

在安全性上，单一的 POS 系统具有不稳定性，股权持有者能够很容易生成相应的时间戳历史（从而易于伪造区块），而混合机制避免了 POS 的伪造问题，

同时由于 POW 必须通过 POS 的验证才可生效，POW 矿工不能自行决定并改变网络规则，还有效的抵挡了单一 POW 模式的 51%攻击。

2.4.1.1. POS 投票



比特币的挖矿中，在区块高度为 H 时，矿工 1 只要率先计算出了正确哈希值，他立刻向所有矿工广播，其他矿工验证他的哈希值是否正确。大多数矿工认为他正确，他就可以获得这个区块的奖励和记账权，矿工 2 的劳动是无意义的。其他矿工则开始计算 H+1。

在 TSC，同一区块高度，一定时间内，不同矿工都可以生成区块，Block 1 和 Block 2,由系统从投票池中随机选择五张选票，进行投票选择，哪怕出现矿霸，优先算出的区块也不一定采用。而且，如果 POW 矿工违背大家的利益，他们的区块奖励也会被剥夺。

2.4.1.2. 投票池

为了使投票权相对公平，TSC 使用投票池机制。通过 360 个区块（约 12 小时）的投票票价调整，投票池里面总票数控制为 40960。系统随机选择，选中者成功参与投票后，系统会返还购买选票的费用。

2.4.1.3. 购买选票

投票池中的票是需要 TSC 的持有者购买的，可以从钱包中买选票。总购票成本为选票价（Ticket price）加上 选票费（Ticket fee），选票费是支付给 POW 矿工，将新选票放入新挖区块的费用。

用于购买选票的 TSC 会被系统锁定，并且投票完成前不可退回。刚买的选票，需要被矿工打包记录在区块里才能生效，存放未被打包选票的地方叫内存池（mempool）。内存池中，选票费高的更容易被矿工选中（赚钱），更快的进入选票池（Ticket pool），因为每个新区最多能记录 20 张新选票，内存池中的选票存在竞争关系。

矿工打包完成，选票在区块链中一经记录，这张票就成了准选票（immature ticket），按照英文版直译是未成熟选票。叫它准选票是因为这时它还不在选票池中，不具有被选中资格，同时选票费也无法退回，只能等 256 个区块（约 20 小时）进入选票池，它才能成为真正选票。

如果内存池（mempool）中的选票过多，经过一定时间没有被矿工打包记录，那么选票价（Ticket price）和选票费（Ticket fee）会被退回。该过程和比特币交易打包很像，矿工费过低的数据包最终可能会被退回。

选票池大约 40960 张选票，每个区块确认只需要 5 张选票，系统随机决定，被选中的可能性服从泊松分布函数。简单来说，28 天内被选中的概率是 50%，142 天内被选中概率是 99.5%，如果 142 天仍然没能被选中，选票价还给你，选票费不退，被旷工收走。

选票池中的选票被系统选中，参与投票,获得收益。这里就出现了一个问题，个人钱包要保持时刻在线，投票时间之内没有执行投票操作，选票价就会被退回。绝大多数社群成员是没有全天候投票的条件的。成员们可以把自己选票交给TSC 的 POS 矿池来代投。

2.4.2. 跨链技术

2017 年以来，随着大量的区块链项目被开发与推广，越来越多的人力与资金被投入到这些项目中。如今，规模与种类不一的区块链项目数量呈井喷状出现，随之也诞生了一系列问题。比如，在区块链项目数量增长的同时，没有及时的匹配上相应的措施，从而导致了大多数的区块链之间无法通信与连接。换句话说， 每个区块链项目都是一个个的”信息孤岛”，这极大地限制了区块链的应用空间。因此，有效的跨链技术是解决这些问题的关键。跨链技术可以把众多的区块链项目从一个个的“信息孤岛”中拯救出来，为它们建立起一个个互通的桥梁。

跨链技术是实现区块链向外拓展的手段，很大程度上决定了区块链项目的发展上限。TSC 采用的跨链技术主要基于安全性、高效性和实现的难度来设计。

关于跨链技术的历史，早期的跨链技术更多关注资产转移，以 Ripple 和 BTCRelay 为代表；现有的跨链技术更多关注跨链基础设施，代表有 Polkadot 和 Cosmos。

最新出现的 FUSION 实现了多币种智能合约，这意味着可以在整个市场中产生多种跨链金融交易。

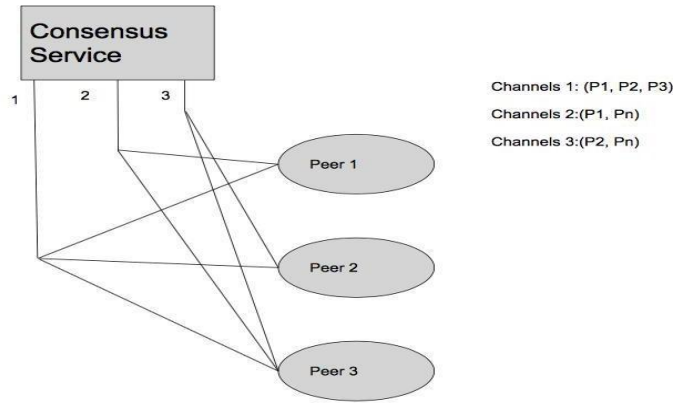
A. 公证人机制

主要代表是 Ripple Interledger 协议，它适用于所有记账系统，目标要实现全球统一的支付标准。

B. Corda

Corda 是一种“类区块链”技术架构。交易双方共同选出一个具有高可行度的公证人，让公证人来检验数据的有效性和唯一性。若公证人证实该交易可行， 那么交易就会达成，此时交易公证人的账本会进行同步。这么做的好处在于，保证安全性的条件下，交易处理将更加高效。

Fabric 新定义的概念包括链、peer、通道和共识服务。Peer 可以参与多个账本使得 Fabric 具有扩展性，Peer 之间具有事务隔离、账本隔离等特点。



C. Cosmos

Cosmos 是 Interchain Foundation 的跨链开源项目，专注于解决跨链资产转移，该区块链网络主要由 Zone 和 Hub 构成：

1）Cosmos Zone 是单独的区块链空间；

2）Cosmos Hub 中心是一种多资产权益证明加密货币网络。

Hub 是中继链，由去中心化的验证人组来记账。一个 Hub 与多个 Zone 进行通信，每个 Hub 具有与它相关联的多个 Zone 的账单信息，以此来产生一个多资产中心账本。Hub 保证资产在不同的 Zone 转移的过程中，里面的资产总量保持不变。

Cosmos 过程如下：

首先，Hub 和 Zone 的跨链通信由 IBC 协议来达成。假设 Zone1 想要和 Zone2 进行跨链交易。

1）Zone1 生成交易信息，并发布在 Hub 上；

2）Hub 生成 Zone1 的跨链信息包存在的证明，并且发布在 Zone2 上；

3）Zone2 受到消息包，并且在 Hub 上发布已收妥的证明信息；

4）Hub 给出 Zone2 已收妥的证明的证明，并且把消息发在 Zone2 上。

Cosmos 优点包括：

1） 每个 Zone 里面的代币转移都会通过它们共同连接的 Hub，因此每个 Zone 里面的资产都会被记录；

2） 若有一个 Zone 发生故障，不会使得其他有效的 Zone 产生影响；

3） 新加入的 Zone 可以轻易地被加入到 Hub 中心里来。

D.跨链交易

跨链技术是实现区块链向外拓展的手段，很大程度上决定了区块链项目的发展上限。关于跨链技术，目前主流的跨链技术包括：公证人机制（Notary schemes）、侧链/中继（Sidechains/relays）、哈希锁定（Hash-locking）、分布式私钥控制（Distributed private key control）。

TSC 将使用中继技术和类似于 Polkadot 和 Cosmos 这样的未来协议，以支持不同加密币种之间的跨链交易。TSC 采用的跨链技术主要基于安全性、高效性和实现的难度来考虑设计。TSC 跨链协议的核心技术是中继链，该技术使得 TSC 不仅具有 Polkadot 的可伸缩性、可扩展性，也具有 Cosmos 的兼容未来区块的特点。跨链协议支持不同币种之间的跨链交易，允许用户实现 TSC 和 BTC、ETC、ZCash 等代币之间的交易。打破各个币种之间的交易障碍，使得一个个“信息孤岛”在 TSC 中完成无障碍的转移、交易与兑换。TSC 中继链对于区块链不同币种间的交易与兑换起到巨大的推动作用，为新兴的区块链相关公司提供十分新奇的技术与思想指导，对区块链行业的蓬勃发展有重大创新意义。

跨链协议设计原则：

1） 安全性：这是跨链设计的基石，在实现跨链的同时具有绝对的安全性。跨链过程中产生的历史数据是极其难以修改的；

2） 性能：跨链的效率也是一个很重要的考虑因素。在保证安全性的条件下，尽可能地提高吞吐量和跨链确认的速度。换句话说，就是让跨链每秒处理的交易笔数达到一定的数量，使得用户享受较好的交易体验。

中继链是使用类似于 Polkadot 中继链和 Cosmos 的跨链协议来综合设计的，主要起到记录交易地址与交易金额和验证交易是否合法的作用。一条交易链上具有多个交易单元，每笔跨链交易必须由至少一个交易单元进行记录和验证。每种和中继链连通的外币中，产生的合约必须由中继链的中转单元进行审核。而且， 每个外币的某节点的交易地址肯定在中继链上有一个映射地址，每笔交易金额都

会储存在中继链中的中转单元中。

中继链为解决 TSC 和外币的跨链交易提供了技术和平台支持，也为不同外币之间的跨链交易提供了空间与机会。中转单元由验证者轮流发布，其主要作用如下：

1）对所有未经验证的交易进行合法性验证；

2）为上一个中转单元收集投票；

3）若上一个中转单元作恶，则发布惩罚。

其结构示意如下：

```
Transfer
{
version:0000...0001，
previous:DC32...1CD1，
height:999，
verify:...，
punishment:...，
direction: output/input，
sourcelink:TSC，
targetlink:ETH，
amount:99ETH，
public_key:12ea...df94，
signature:84ec...edf6，
hash:57da...96c2，
}
```

version:表示版本号。

previous:指向上一个中转单元。

height:表示当前中转单元的高度。

verify:验证过的交易和投票。

direction:表示方向，分 output（输出）和 input（输入）。

sourcelink:表示源链，input 情况下可以是 ETH、BTC 等，output 情况下只能

是 TSC。

targetlink:表示目标链，output 情况下可以是 ETH、BTC 等，input 情况下只能是 TSC。

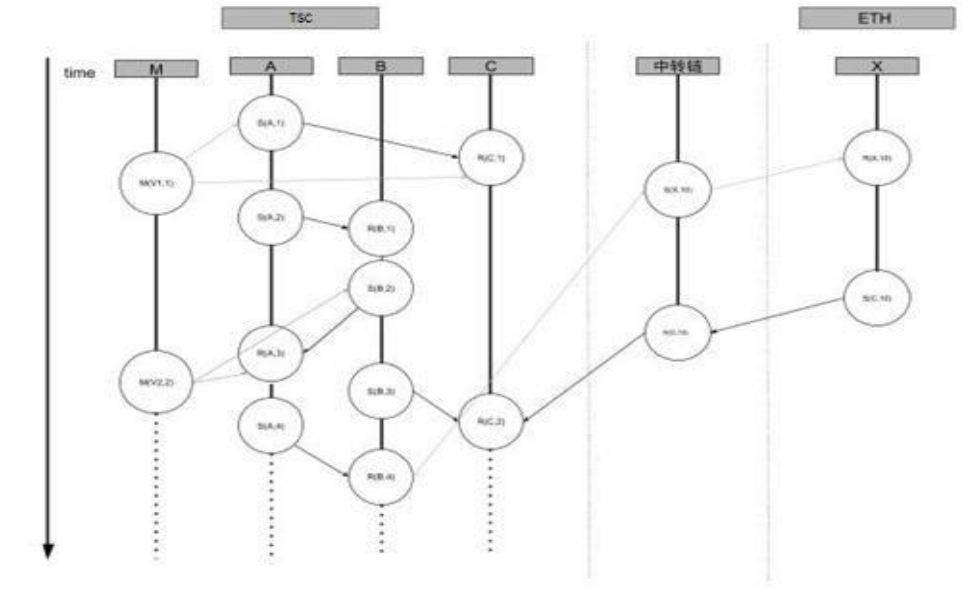
amount:表示金额，需要自带单位。

punishment:对未通过投票的作恶验证者进行举证并惩罚。public_key，

signature:对单元进行签名，保证该单元为验证者发送。

hash:对整个单元进行 hash 运算，保障交易单元在网络传输的过程中不被修改。

以 TSC 与以太坊（ETH）跨链交易为例：



输入交易：

1) 假设以太坊上的帐户 X 需要向 TSC 帐户 C 支付 10ETH。X 需要在以太坊上申请一份中转合约，中转合约应包含 TSC 账户 C 地址和发送金额，并由账户 C 签名；

2) 中继链主动监测到 ETH 有 TSC 账户相关的合约；

3) 中继链中某一中转单元记录审核该合约，并由验证者进行数字验证；

4) 如果数字验证通过，则在账户 C 末节点增加关于该交易的记录，并在 ETH

中锁定 10ETH，使之暂时不能在 ETH 中流通；如若不通过，则合约作废，交易失败；

5） 最终由 TSC 验证链中的某一验证单元对账户 C 的末节点进行验证，达成 TSC 全网共识。

输出交易：

1） 假设 TSC 账户 B 需要向以太坊上的账户 X 支付 10ETH。账户 B 需要向 TSC 中继链发送一条交易请求，该交易请求应包含 ETH 账户 X 的地址和金额，并由账户 B 签名；

2） 中继链接收到 TSC 账户 B 的请求并记录；

3） 中继链中某一中转单元记录审核该交易请求，并由验证者进行数字验证并且签名；

4） 若验证通过，则账户 B 的末节点增加一条扣除 10ETH 的交易记录，并由中继链转化账户X 的地址在 ETH 的映射，并释放 ETH 中锁定的任意 10ETH；

5） 最终由合约将该 10ETH 发送给 ETH 中的账户 X。

TSC 的跨链交易技术不仅仅局限在某一单一币种。TSC 的中继链可以与BTC、ZCash、EOS 等衍生空间连通。换句话说，市面上现在的大部分币种衍生出来的区块空间都可以接入到 TSC 的中继链上。而且任何新诞生的币种只要和 TSC 签订合约并且达成共识，都可方便快捷地被后续接入到 TSC 中继链。这样就可以使得 TSC 实现很大规模的无限扩展，这样的方式大大满足了全球交易的需求。不仅如此，现在市场上的大部分币种甚至可以通过 TSC 中继链进行直接交易， 比如 BTC 和 ETH 可以在TSC 中继链上直接进行交易。这样就无需在BTC 和 ETH 直接建立渠道或者平台，大大节省了技术和人力成本。TSC 中继链可作为市场上一个巨大的跨链平台，实现不同币种之间的交易。

为确保 TSC 中继链上的跨链交易的即时性、安全性，TSC 原子互换实现将会被采用。TSC 原子互换是一种新技术，允许 TSC 币与在其它类型的数字资产之间实现无需信任的点对点交易。这种交易可以在瞬间完成，任何一方都没有机

会违反协议。而且当交易其中一方中途退出的情况下，数字资产会在一个规定的时间后退还给双方。这种技术对加密数字货币的未来具有重大意义，因为这种无缝的跨区块链加密数字货币互换能力开启了一种新的应用。TSC 原子互换可以打通各种加密数字货币之间的交易阻碍，确保交易正确。如果用户想要在 TSC 币与其它类型加密数字货币之间进行交易，那么这种技术可以让用户完全控制自己的资金。

TSC 原子互换的工作原理：

假设一个例子，M 和 N 是数字资产交易的双方，M 在 TSC 在有自己的帐户，N 在以太坊、TSC 上有自己的帐户。现在 M 和 N 通过电话、网络等途径谈妥了一笔交易，也知道了双方在各自的 TSC 账户。根据达成的交易，M 准备把他在 TSC 上的 100TSC 转到N 在 TSC 的帐户下，N 将通过 TSC 向 M 支付 200ETC。

为了完成 TSC 和 ETC 的交易，双方依次执行以下步骤：

- 为了原子性地完成这笔交易，首先 N 自定义一个指令 X，计算得出 V:=Hash（X），X 现在只有 N 自己知道；
- N 在 TSC 上发布一笔转账交易，有条件地转让 200ETC 给 M。但和普通的转账交易不同，这笔交易附带一个哈希锁定条件：M 只有在 4000 秒内向 TSC 出示一个满足 Hash（X’）==V 的指令 X’才能将 100ETC 入自己账上（采用账户模型还是 UTXO 模型没有本质区别），若 M 超时未能领取 ETC，则 N 可以通过在 TSC 上发起一笔退款交易把 100ETC 返回自己账户上。哈希锁定条件中的 V 和超时时间都是公开的，M 当然也看得到；
- M 现在在 TSC 上看到N 发起了这样一笔交易，但他不知道解锁指令 X 是什么，所以他必须向 N 通过 TSC 支付 100TSC 以买到这个指令 X。于是 M 在 TSC 上给 N 发送一个附带同样哈希锁定的指令转帐，有效期 2000 秒，超时若 N 未领取则转帐金额会自动退款。这个哈希锁定的指令转帐原则上很容易实现，其逻辑是：当 N 点击指令转帐后会弹出一个对话框，要求 N 输入一个满足 Hash（X’）==V 的指令 X’，如果输对了，指令转帐中的 TSC 会转入

N 在 TSC 上的账户，同时 TSC 会给 M 发送一个回复，告知 M 转帐已被领取，且在回复上同时显示 N 输入的指令 X。如果 N 输错了指令 X'，则 N 无法收取转帐金额；

- 现在N收到了指令转帐，及时点击指令转帐，且输入了N自己知道的指令X.因为 V==Hash（X），所以 N 成功拿到了 100TSC。根据程序逻辑，TSC 给M 发送一个回复，告知 M 转帐已被收取，且 N 输入的指令是 X，于是 M 知道了指令 X；
- 因为M 现在知道了指令X，他现在就可以在 TSC 上利用指令X 来提取那 200个悬而未决的 ETC。M 及时进行了操作，就在 TSC 上拿到了 200ETC；
- 至此，M 拿到了 200ETC，而 N 拿到了 200TSC。在交易过程中，以太坊和 TSC 完全不需要互相通信，但仍然确保了 TSC 和 ETC 的原子互换。

以上是正常流程，在异常流程下互换的原子性仍然是成立的。比如在上面的第 3 步中 M 没有通过 TSC 发出转帐，N既然看不到转帐也就不会输入指令 X 给M，M 拿不到指令 X 也就无法在 TSC 上提取 ETC，交易的原子性得到保证。

哈希锁定机制在以太坊等区块链上都很容易实现，至于 TSC 要实现上述哈希锁定的转帐也不会有太多的困难。

此外，由于两种转账都是指定对方的转账，程序可以被设计成可以由第三方提供指令帮助解锁，但资产仍然按原先指定的流转方式。这种设计使得用户在自身钱包失效或暂时无法访问 TSC 时，可以安全地委托他人代为操作。因此解锁指令在 TSC 中公开不仅不会带来安全问题，还会有额外的优势。

2.5. TSC IM 平台生态

2.5.1. 重构即时通信生态

基于 TSC IM 的全球生态圈布局，来自全世界的用户都可以在生态圈里通过

TSC Token 进行游戏、社交等，TSC IM 也会确保用户信息的安全性、隐私性等问题，这样就建立了一个完整的生态闭环。

2.5.2. Token 在生态中的应用

TSC IM 官方发行的数字资产名为 TSC，TSC 是基于点对点对等网络的数字加密资产。

TSC 的生态应用：

1、提供安全的通讯聊天功能室；

2、基于 IM 区块链的浏览器（通信宝）；

3、信息上链功能；

4、提供开发者社区。

5、游戏

6、代码开源

2.5.2.1. 提供安全的通讯聊天功能室（基础功能）

TSC IM 除了存储和管理 TSC 资产，在保证安全通信的基础上，也为其他数字货币提供钱包管理服务，包括发送和接收数字资产、数字资产红包等功能。聊天记录的存储也不再是被动默认，信息的上链也可自由选择或销毁。

同时，TSC 通信经济网络也开放扩展开发能力，并在 TSC Token 赏金支持下，为 TSC 通信经济网络提供更丰富的应用。TSC 也支持使用其他数字货币作为赏金来完成 TSC 的功能提升。

TSC IM 也为 TSC 用户提供了表情包功能。表情功能为用户提供了一种有趣的视觉沟通方式，来与他们的朋友和家人进行交流互动，还可以增加用户的参与度。表情包为用户提供了高效简洁的表达方式，也增加了沟通交流的趣味性，使得用户间面对屏幕沟通交流时，可以告别单一枯燥的文字交流形式。

TSC IM 的表情包市场，让每个参与者都有机会创建自己的表情产品，并在 TSC 网络进行价值传递。因为资源的贡献，版权之争也将不再是需要解决的问题。

2.5.2.2. 通信宝

为了方便用户查看自身与他人通讯情况，TSC 团队将开发通信宝，用户可按自身需求，通过免费和付费两种不同的方式获得所需信息。通信宝免费提供用户自身通信信息数量、Token 消费数量等。其也可在经过他人同意之后，支付一定 Token，查询他人相关信息。在TSC首页将设立用户的通信排行榜、消费排行榜。对于上榜用户，官方将会给予一定的 Token 奖励。

2.5.2.3. 信息上链功能

基于区块链技术，TSC推出了信息上链作为开启个人用户接入区块链世界的切入点，用户可以使用 TSC 将想要留存的信息（包括但不限于文字、图片等内容）一键上链，极大降低用户使用门槛。对于普通用户而言，此举门槛低、扩展性强， 他们只要迈出一小步，就能进入区块链领域的个人价值数字化新时代。由于区块链具有分布式数据存储、点对点传输、共识机制等技术特征，使得上链的信息永不灭失。而 TSC则可以作为个人数字价值世界的以太坊。随着 TSC 生态日趋完善，会有更多用户在上面发挥创造力和想象力，探索区块链时代的共享应用，未来围绕个人场景可以打造更多价值交换应用，如社交、电商、共享、广告、游戏、数字内容等。

2.5.2.4. 资产管理服务

资产管理服务为针对多种数字资产持有者的一个便捷资产管理服务。用户可

以在 APP 上集成自己的钱包管理，并解决传统银行资金转账过程中的各种问题。为了能够无缝支持资金在区块链上的转账，APP 计划支持比特币、以太坊、莱特币等，用户无需记住接收者的地址或特定数据，即可通过用户名或二维码直接进行转账。

2.5.2.5. 开发者社区

TSC 开放扩展功能 API 给开发者社区，开发者可以根据社区的功能列表进行提交开发、完成功能，开发的功能将根据功能点情况奖励 TSC Token。扩展功能开发也可以采取赏金开发模式，TSC 用户可以对自己需要的功能进行悬赏；开发者完成悬赏任务后，可以获得任务赏金。

2.5.2.6. 游戏

TSC 经过共识算法的优化，能够通过灵活高效的智能合约支持基于区块链的非同质 Token 形式的游戏 DApp 开发和运行，TSC 提供开放的游戏接入平台，让开发者可以在 TSC 链上自主开发各种 DApp 程序。同时 TSC 还提供以主链 Token 的方式，接入各种竞技类游戏，为游戏开发者提供更灵活的积分管理和积分流通能力。

2.5.2.7. 开源代码

在 TSC 的共识算法优化完成并成功上线主网后，TSC 代码将通过 TSC 基金会管理的技术委员会进行开源。开源后的 TSC 各项工程代码，均由 TSC 技术委员会进行管理和审查，并在 TSC 基金会的授权下，进行功能的升级迭代和后续技术演进的开发工作计划安排管理。

3. TSC Token 分配及产出

TSC 将发行Token 总量为30 亿，前期通过 POS 的方式产出13 亿，其中 10.4 亿枚 TSC 会分发给用户，其余部分归 TSC 团队所有，用于项目的软件应用落地及硬件节点开发服务。

TSC 项目发布 6 个月内，前期 TSC 为 POS 挖矿，平均每 2 分钟出一个块，每块奖励 148 个 TSC，即新增约 0.194472 亿 TSC，则剩余 16.805528 亿 TSC 将会转为 POS+POW 机制，按照每 2 分钟出一个块，每块奖励 1600TSC，每两年减半的方式产出，其产出分配比列为80%奖励 POW 矿工，20%奖励POS 投票者。

我们在 TSC 生态引入自我燃烧机制，POW+POS 挖矿期间，交易手续费直接燃烧。

完整代码将会在 github 上开源，并保持实时更新。

4. TSC 核心团队

TSChain 技术总监-Dave Archer

南澳大利亚州 Noarlunga Tafe（TAFE / UNI）学士学位，计算机与信息技术与科学专业，超过 15 年的计算机经验，管理（DevOps），开发，编码和学习。历经 4 个大型区块链项目开发服务。

TSChain 首席技术官-Matt Baker

互联网、通信和信息安全融合领域专业人才，多项信息安全和通信领域专利发明人。拥有 10 年的软件开发经验。 Matt Baker 在后端开发、区块链技术和以太坊智能合约，以及后端 web 开发有着丰富的经验， 目前在 TSC 项目组负责硬件产品的研发与落地。

区块链工程师-John Wills

John Wills 有着丰富的区块链技术全栈开发经验。一直从事 REACT、PHP 和

JavaScript 开发工作，由他开发了许多大型应用程序目前正被区块链行业的数百万用户使用。

首席营销官-Ben Horder

数字货币早期投资者，10 年的市场营销传播管理经验、有着丰富商务及媒体资源，与业内领先的通信从业者建立了良好的合作伙伴关系，有着数百万用户的社交媒体和社区互动资源。

5. TSC 基金会

TSC 基金会由抱有崇高理想并拥有技术能力和营销能力的核心合伙人和社区代表组成。基金会以推进社区自治、推动平台按预定计划稳步发展为目标，推动形成进行民主决策的社区组织、自生循环的 Token 经济以及为此提供技术基础的区块链生态系统。

所有的参加者都是 TSC 基金会的重要成员，坚信根据平等的决策权，分享和推广集体共同的价值观。随时欢迎新的 TSC 投资者或 TSC 持有者成为基金会的成员。

TSC 基金会决策委员会由 5 名成员组成，任期为 4 年。第一届成员由 TSC 发起团队选出的区块链和企业运营方面拥有丰富经验的人员组成。任期结束后，下一届成员由 TSC 基金会代表人（主节点运营者）根据 TSC Token 持有量、持有时间、TSC 生态系统贡献度，进行选举并产生。

为了 TSC 生态的健康发展，TSC 决策委员会下设技术评审委员会、TSC 市场运营委员会和经济管理委员会的 3 个委员会组织，由决策委员会任命。各委员会的职责如下：

- TSC 技术评审委员会负责对TSC 采用的技术架构进行评审，决定改善的方向,推进技术进步，推动技术团队实现白皮书计划的功能。
- TSC 市场运营委员会负责 TSC 的宣传、市场营销、与社区的交流，以及 TSC

运用推广，用户培养维护等工作。

- TSC 经济管理委员会负责 TSC 的 Token 锁仓和解锁管理，并对 TSC 的费用使用进行审核公布。

6. 项目时间规划

	2018Q1 TSC0.7 团队组建 市场调研 设计产品模型架构
2018 Q2 TSC0.8 设计产品拓展功能 明确产品经济模型 完成白皮书初稿	
	2018 Q3 TSC0.9 白皮书发布 资产链发布
2018 Q4 TSC1.0 TSC IM 应用发布	
	2019 Q1 TSC1.1 信息上链功能发布 事件投票功能发布
2019 Q2 TSC1.2 POW+POS 挖矿发布	
	2019 Q4 TSC1.3 支持智能合约
2020 Q1 TSC1.4 通信宝发布	
	2020 Q2 TSC1.5 跨链交易功能发布

7. 免责申明

您承认并同意，在购买 TSC，持有 TSC，以及使用 TSC 的过程中存在以下诸多风险。

1.管辖和执法行动的风险

在许多司法管辖地区，TSC 以及其他区块链科技组织所相关的法律政策尚

不清楚或并未落实。无法预测如何、何时或是否有监管机构会针对 TSC 采取已有的或推出新的监管政策。这类监管行为可能会对 TSC 或 TSC 生态产生各种负面影响。如果监管行动或法律或法规的变化使其在此类管辖范围内经营是非法行为，或难以在必要的监管许可下进行商业活动，基金会（或其附属机构）可能在该司法管辖区停止经营。

基于与大量专业的法律顾问咨询讨论以及针对数字货币的发展和法律架构上的持续性分析，基金会对 TSC 的销售表示谨慎态度。因此，对于大众销售，基金会需要经常性调整销售策略以尽可能避免法律风险。

2.市场竞争的风险

存在以下这种可能，即一种可替代的网络科技出现，其使用和 TSC 或 TSC 生态相同或类似的代码和协议来搭建类似的设施。TSC 生态可能需要与这些替代性技术展开竞争，从而对 TSC 或 TSC 生态产生负面影响。

3.团队成员退出的风险

TSC 生态的发展依赖于现有的技术团队和专家顾问的继续合作，他们在各自的领域知识渊博、经验丰富。任何成员的退出可能会影响到 TSC 生态或其未来的发展。

4.发展失败的风险

因为各种各样的原因，TSC 生态的发展存在无法按照计划继续推进的风险，包括但不限于某种数字资产、虚拟货币或 TSC 的价格下降，不可预见的技术困难，以及平台经营发展所需资金的短缺。

5.安全的风险

黑客或其他恶意的团体或组织可能会以各种各样的方式试图干扰 TSC 或 TSC 生态，包括但不限于恶意攻击、拒绝服务攻击、共识基础攻击，Sybil 攻击，洗钱和欺诈。此外，还存在一种风险，第三方或基金会成员或其分支可能有意或无意引入某种漏洞，从而对 TSC 或 TSC 生态的核心基础设施产生威胁，并对 TSC 或 TSC 生态产生负面影响。

6.其他风险

除了上述风险，还有其他的风险（如特别设置了 Token 购买协议）与您的购买、持有和使用 TSC 有关，包括那些基金会无法预测的各种情况。这种风险还可能会演化成各种无法预期的情况或上述风险的组合。您应该对基金会及其附属机构做出充分的尽职调查，在购买 TSC 之前，需要理解 TSC 生态的总体框架和愿景。