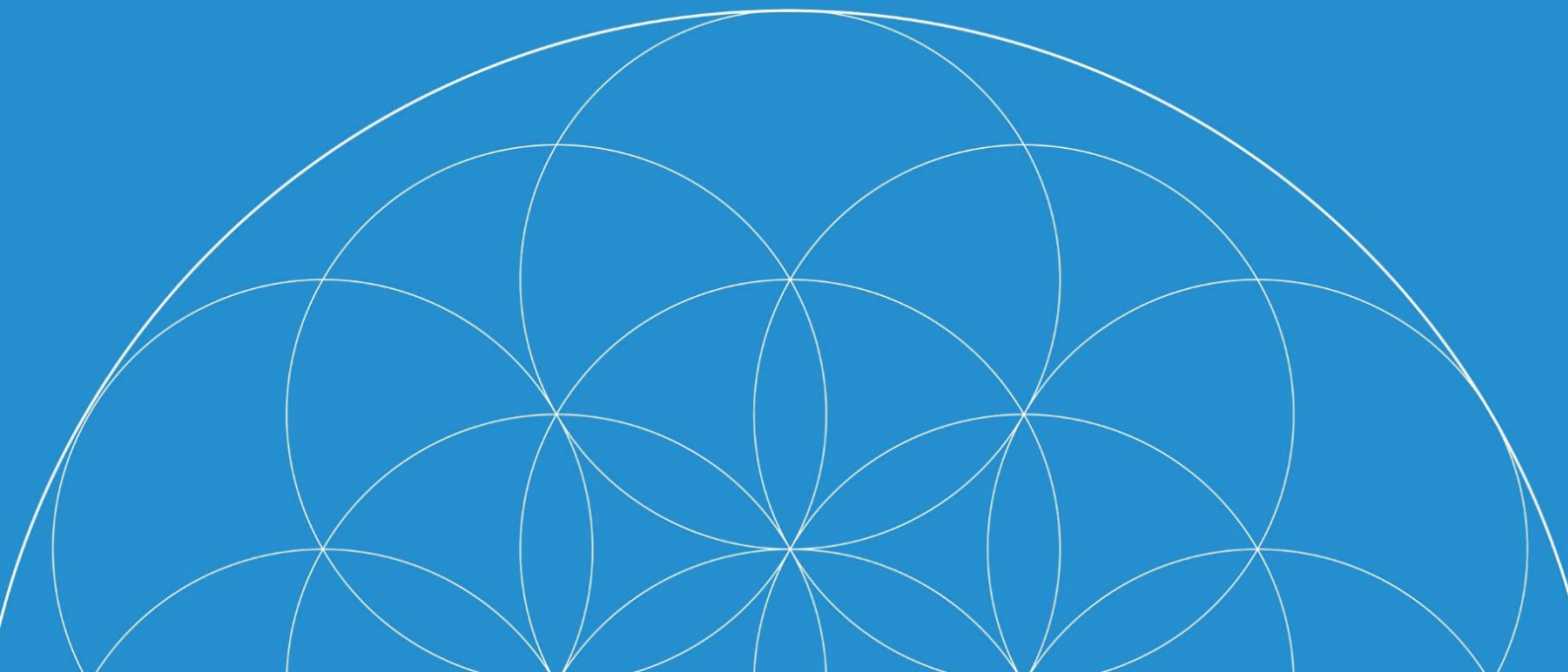
DasCoin™

信任的货币

Michael Mathias

2017 年 3 月 31 日



摘要

达斯币（DasCoin）旨在解决储存和交换价值固有的核心问题。

达斯（DasCoin）区块链是一个共同分布式分类帐，可生成并分配加密资产，确保其安全储存和交换。达斯区块链构成数字资产系统——达斯生态系统（DasEcosystem）的核心，该系统旨在提供价值交换解决方案，增强其安全性、提高实用性、可扩展性，使其接受范围更广、效率和性能更优。

混合货币达斯币是该系统的核心，其设计将分布式加密货币的优点与集中货币的强项相结合，并摒除各自的弱点。达斯币是可转换"储值"单位，是数字资产系统的基础。该系统旨在提高个人、企业、金融机构、合作社和商户之间价值交换的质量和效率，增加全球财富。

达斯币并非基于商品的支持或政府的声明，而是基于优质、健全的底层系统实现其价值。信任是该系统的基础，转化为数字模式（而非系统地消除），最终，通过更广泛、更有效、更好校准的价值系统，全球来自各行各业的更多的人将会享有更多的财富。

介绍

基于技术的货币现已成为现实，并且会持续发展数代。比特币一直引领这一新兴领域发展，证明了货币系统数字化的可能性，在过去 8 年中已获得巨大的成功。自别特比诞生以来，其他加密货币也应运而生，但很少对市场产生真正的影响。

比特币的主要影响力来自创新的 “区块链”底层技术。区块链是在最少第三方参与下对交易进行验证的工具，且不泄露买家和卖家的名字，只需他们在系统中的地址，而且这些地址可被进一步遮蔽。区块链技术构成“共同分布式分类账”。“共同”是指节点由社区共享，而不是由中央机构拥有。“分布式”是指节点分布在多个位置。而“分类账”在该系统中是交易的连续记录。

组合起来，系统就成为一个不可篡改、不得变更的交易记录，该记录在一个用户社区中共享并储存在多个位置。2 种主要加密货币模式（“工作证明”和“权益证明”）都有明显的缺陷。比特币的工作证明模式是一个极其低效的系统，其分散的结构可导致严重的治理问题（正如正进行的区块规模辩论所证明的那样）。权益证明的山寨币饱受预分配问题的困扰（“预挖矿”可在没有透明度或理由的情况下分配币）且天生缺乏有效性（由于“没有权益”问题）。

每个价值系统都必须建立一些基本元素。这些包括定义：初始货币供应、初始分配、价值基础、货币供应扩张/收缩机制，控制生产手段及通胀分配（和/或信用分配）。

达斯币提供了混合的架构来解决与这些经济学要素相关的问题。私有许可的区块链体系架构因其更高的安全性、固有的效率以及更易扩展的能力（由于部署控制）已被纳入。而巩固这一安全基础的是采用银行标准 KYC（了解您的客户）要求对所有用户进行身份验证并实施“硬件要求的”数字钱包系统。此外，达斯系统还集成了一个强大的营销机制，其奖励通过推介口碑推广实现的增长。最后这个数字价值系统可提供最佳的安全性、世界级的性能，并将迅速被全球大众市场所采纳。

关键设计特点

“价值证明”分配方法
确保任何直接从达斯区块链分配了达斯币的个人已向系统提供了经过定义和认可的价值形式（具体以“周期 Cycle”为单位，这是一种闭环专用货币，只能通过使用比特币或欧元购买系统许可证获得）。没有任何一方（无论是高管还是开发人员）能够为自己预先造币、预先挖矿或预先分配达斯币。只能通过向系统转移价值来换取“周期 Cycle”，而“周期 Cycle”必须提交给系统，以便通过造币过程直接分配达斯币。

“许可证证明”共识方法
达斯币采用许可证制度，而非挖矿设备。共识是通过一种算法实现的，该算法随机定义哪个被许可节点将制造下一区块。

固定供应
2 的 33 次方，约 85 亿个单位（分布在一个未定义期限内，取决于系统内部动态，目前预计将会持续 12 年）。

完全身份验证的网络
每个用户都将通过由中央机构执行的银行标准 KYC 流程进行身份验证。

可转换性
达斯币通过从“周期 Cycle”转换造币进入流通。造币完成后，就可直接转移为或转换成各种法定货币和比特币。现有达斯币最终将在各种交易所进行交易，届时可将法定货币直接转换为达斯币。

分布式生态系统
支持数字资产系统价值的是全球硬件和软件系统网络以及该系统内提供的相关产品和服务（包括交易交换功能和支付解决方案）。这个系统网络将全球许多司法管辖区互联起来，并具有设计用于确保顺利持续运行的冗余设施。

激励式营销
基于推荐的营销系统，支持全球认可达斯币并有兴趣通过此数字资产系统交换价值的团队，促进这些关系紧密的团队发展。

混合特点

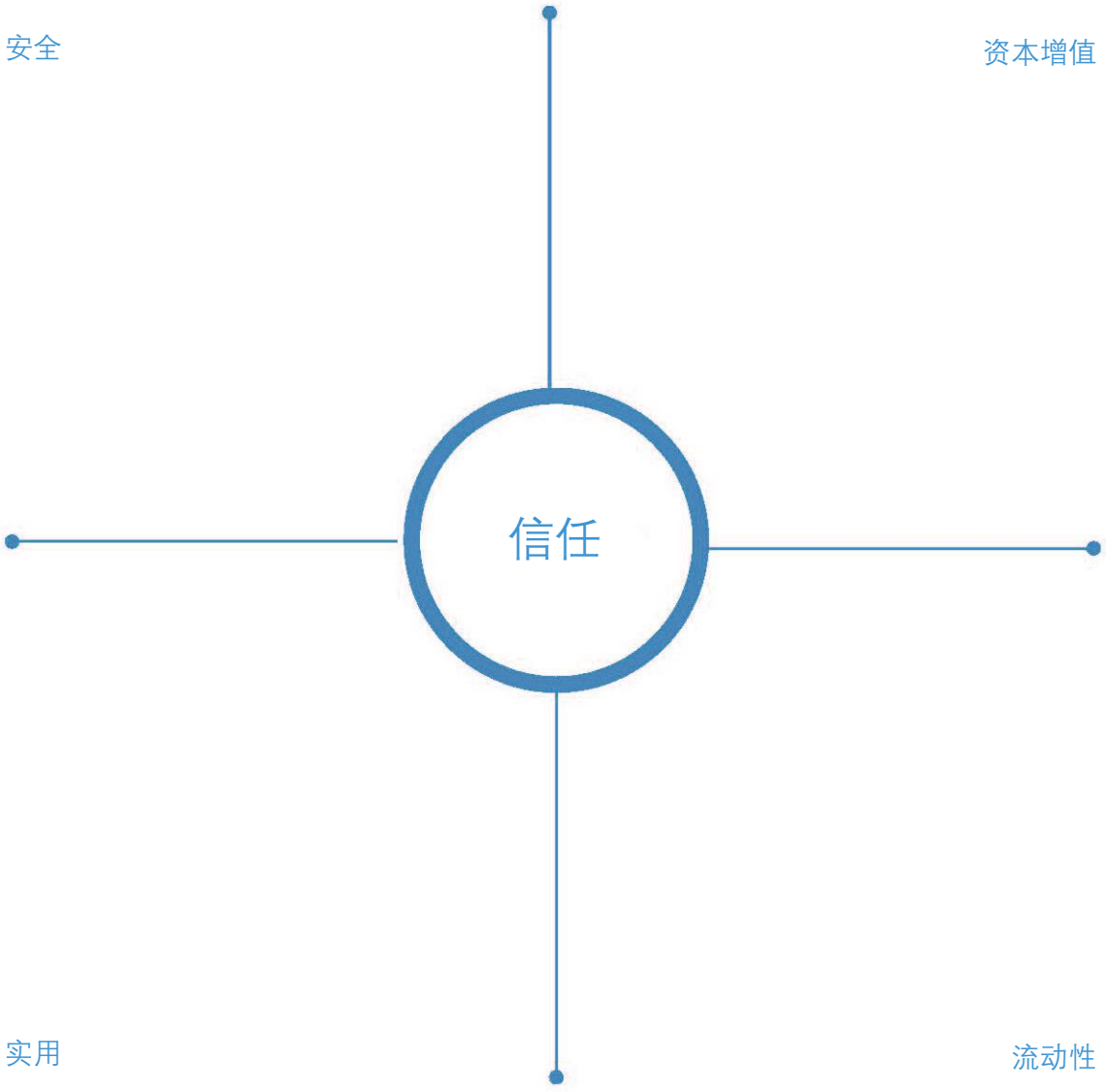
通过达斯币，已将集中式和分散式方法组合起来，只为解决问题并最大化用户收益。

- 集中发行货币。
- 分散分配货币。
- 获得许可的区块链，独立认证。
- 经中央身份验证的用户群采用银行标准 KYC 流程，支持参与者之间的信任。
- 分布式、去中心化的生态系统。
- 分散式数字钱包系统：发行后，货币只能通过拥有货币的经身份验证一方的数字钱包私钥进行控制。没有其他人、公司或机构可转移、没收或扣押此货币。
- 隐私性与透明度（并且无匿名）兼具，确保交易进行和记录。
- 完全符合法规：遵守主要司法管辖区和制定的行业标准。
- 即时交易，验证速度设置为 6 秒。
- 分散式通胀分配（通过造币队列和“价值证明”进行分配）。

主要目的

达斯币的目的：

- **安全：**整个达斯币系统必须安全。
- **流动性：**必须能将达斯币单位换成其他价值形式。
- **实用：**在市场中必须有多种渠道使用达斯币。
- **资本增值：**单位必须发挥真正的储值功能。随着生态系统内的价值增长，达斯币单位的价值也必须增长。



指导原则

信任：达斯币的首要目的是利用数字资产系统的基础设施建立一个有效的信任网络，以让所有参与者及利益相关方实现共同的目标：提高网络价值、拓展网络。网络将通过以下方式实现此目的：

1. 向特定主体（例如 达斯币董事会和链机构）授予信任，以执行链管理，并最大限度提高网络效率和效用。

2. 通过编程，确保正确定义每个被信任的主体，且不超越其权力界限。

3. 向遵守网络共同利益的行为提供激励，并确保不得出现任何不端的行为，且对违反规则的行为进行惩罚。

4. 确保由合格的第三方会计公司核实，确保获得许可的区块链准确运行，保证其运行水平。

5. 运行高度透明，并确保系统所有参与者的隐私权得到正确保护。

通过这种方式，达斯系统可实现创新迭代进行必要的更新，以满足网络乃至全球的环境。最终，系统将会创建一套约定的规则来创建和传递价值，并通过区块链软件加以执行。换言之：法律就是代码。

隐私权：该系统旨在保护个人的隐私权，而无需匿名。在系统安全或网络参与者隐私不造成损害的情况下，确保系统运行的透明。

便利：尽可能使系统实用操作更简单、方便。安全性和便利性通常相互抵触，但系统的设计旨在这两个重要方面之间找到最优的平衡。

简单：总体目标是保持系统尽可能简单，尤其是与所有用户交互相关的方面。

定义

私钥
用于访问和控制加密资产的密码。系统的私钥格式是随机生成的 32 字节数字。

公钥
可共享但与私钥配对的代码。系统的公钥格式是 secp256k1 椭圆曲线上的一个点。

达斯币生态系统
数字资产系统，可安全地创造、转移和记帐各种加密资产。该生态系统具有区块链、钱包和交换功能。

达斯网（达斯网）
达斯币和整个达斯生态系统存在的高速节点网络。

达斯区块链
私有、获得许可的区块链架构，具有更强的安全性、内在的高效和更好的可扩展性。

保管库帐户
数字钱包系统中的帐户，由经身份验证的个人或企业实体持有。此帐户保存该特定个人或商业实体的许可信息。

许可证
可让帐户能够参与达斯区块链的加密证书。

周期 Cycle
达斯区块链中定义的加密资产。“周期 Cycle”表示达斯网内的储存容量，用于网络服务或提交换取达斯币。

达斯币
数字资产系统中心的一种可转换“储值”单位。生产和分配达斯币以换取已提交给达斯网的“周期 Cycle”。

频率
转换因子，用于确定在造币过程中将产生达斯币的“周期 Cycle”数量。

达斯币造币
生产和分配达斯币以交换提交的“周期 Cycle”的过程。“周期 Cycle”提交给系统时形成一个队列。然后每 10 分钟创建一定数量的达斯币，并根据队列中的相关频率和参数进行分配。

定义

达斯币造币队列
已提交“周期 Cycle”以换取达斯币的用户排列。队列按照先进先出的原则运行。

达斯币造币区块
每个造币间隔结束时分配的达斯币数量。

达斯币造币间隔
达斯币造币区块之间的持续时间为 10 分钟。

达斯币造币率
在达斯币造币间隔过后分配的达斯币数量。

WebEuro
达斯币区块链中定义的加密资产，代表欧元面额。

交易分类帐

运算

运算是构建交易的基础。其使用 C++ 编程语言进行定义，允许在区块链上创建动态和广泛的活动。运算是对个人或节点可执行的潜在逻辑的描述。这可在批准软件更新后实时添加和更新。这意味着能够提供定制的数字合约，这些数字合约以编程形式，通过区块链及其节点网络得以强化。

交易

活动计划执行的运算汇总就是交易。定义一组运算后，交易参与者必须用其私钥正确签署相应的运算。这将会被检查和验证，并包括到期日期、区块号和区块号的哈希引用。在填写了所有必填字段并且每项运算都由相应密钥签名后，就可成功将其包含在区块中并写入区块链分类账的历史记录。

区块

区块是更新区块链分类账状态的一组交易。区块链的基本元素是区块。由称为“主节点”的授权实体产生各个区块，每个区块通过加密方式链接到上一个区块。

区块间的加密连续性确保了分类账中改动的余额保持一致。重放区块序列将显示当前现有状态，区块序列应用意味着区块链上的帐户余额之不会存在任何不一致的情况。

区块不可改变，因为它们包含时间戳，由主节点签名批准，并将与未来的区块串联起来。这意味着，进行交易时，交易是不可逆的，无法在不完全影响系统的所有其他方面的情况下进行修改。任何无效签名都将被拒绝，因此没有人可以轻易改变或修改区块链的现有历史记录。

造币区块

造币区块是在每个造币区块间隔（目前设置为 10 分钟）结束时发生的新造达斯币的直接分配。由主节点产生各个造币区块，并以加密方式链接到上一个造币区块。生成的达斯币根据造币队列将直接转移到网络钱包（WebWallet）保管库中。

交易分类帐

深层保管库合约

深层保管库合约是达斯币区块链上的一种智能合约。它要求网络钱包保管库的所有者在约定的一段时间内（合约期限）将一定数量的达斯币转移到深层存储中。在深层存储中，达斯币在期限到期之前无法转移，并且将自动转回原始保管库，除非合约持有者同意将余额转入另一期。

作为同意储存一定数量的达斯币的激励，将向达斯币的所有者提供一个奖池份额。奖励收益直接从达斯币区块链分配到合约持有者的深层保管库中。每个初始深层保管库合约都值得收到一个奖池份额，并且在此期间所有当前合约持有者都将分享该奖励。

深层保管库合约分为 3 种。每一种都需要不同的合格转移、不同的承诺期限，并且每个都提供不同的奖池。每个都让合约持有者在系统中有一定数量的投票影响力。

投票合约

此合约要求 1 万个 达斯币承诺 2 年期限。此合约的奖池是每周所有造币达斯币的额外 10%，且每周分配一次。对个人或实体可以持有的投票合约数量没有限制。

分类账合约

此合约要求 10 万个 达斯币 承诺 3 年期限。合约持有者还必须运行 10 个分类账节点才有资格参与分类账奖池。系统将在分配合约持有者奖励份额之前验证这些节点在整个期间内都处于活动状态。此合约的奖池是在 2 周内所有造币达斯币的额外 6%，每 2 周分配一次。对个人或实体可以持有的分类账合约数量没有限制。

交易分类帐

主合约

此合约要求 100 万个 达斯币 承诺 5 年期限。合约持有者还必须运行主节点才有资格参与主奖池。系统将在分配合约持有者奖励份额之前验证在此节点整个期间内都处于活动状态。此合约的奖池是在 3 周内所有造币达斯币的额外 3%，每 3 周分配一次。每个个人、实体或相关方最多有 3 份主合约。

合约	合格转移	承诺期限	奖池	投票
投票合约	1万个达斯币	2 年	10%	1
分类账合约	10万个达斯币	3 年	6%	20
主合约	100万个达斯币	5 年	3%	300

延期

每个合约持有者在当前期限届满前同意申请延期，将会获得额外奖励。通过“延期”其合约，合约持有者将获得奖池的 2 份奖励，而不是通常情况下的 1 份。每延一期，可获得来自奖励池的一份奖励，因此在同意第二次延期时，合约持有者在下一个期限内将获得 3 份奖励，而非通常的 1 份额。在下一合约期限内，每次延期协议都将增加额外 1 份奖励。

交易分类帐

超级区块
超级区块是在特定间隔更新区块链分类账状态的大型分配交易。每个超级区块由一个主节点根据一系列智能合约构成，其通过上一标准区块的加密链接集成到达斯区块链中。超级区块的生产不会延迟或干扰造币区块的生产，因此不会影响造币队列。

投票区块
造币区块生产 1 周的 10%。直接分配到深层保管库帐户。

分类账区块
造币区块生产 2 周的 6%。直接分配到深层保管库帐户。

主区块
造币区块生产 3 周的 3%。直接分配到深层保管库帐户。

司库区块
造币区块生产 4 周的 1%。直接分配到由达斯币董事会控制的司库帐户。这些区块的收益将用于支付该系统的管理（执行董事、职员和董事会董事）以及宣传营销活动。

超级区块的生产仅仅是最终分配的达斯币总数的重新分配。该系统不仅是通过生产造币区块来分配最终数量的达斯币，更是激励达斯币的持有者储存（或保存）其持有的部分。这种动态有利于系统的整体稳定性。由超级区块创建的社区节点也会使系统受益。这将使权利更加分散，增强达斯网基础设施的整体稳定性。

去中心化的共识机制

主节点
主节点的作用是聚合用于产生区块的交易。只有主节点有权将交易写入区块链分类帐历史记录。每个主节点都知道其他节点，并且它们必须由治理系统投票。主节点的新颖在于用加密密钥授权。这意味着每个主节点都必须注册其公钥，并在区块生产期间用其私钥签名。因此，可让任何一个特定主节点对其行为负责。

分类账节点
分类账节点对达斯币区块链进行非授权维护。换言之说，分类账节点不会产生区块，但会聚合交易并将它们传递给主节点，加入到区块中。账本节点能够验证交易，因此有助于扩展达斯币共识网 络，实现更远距离的链接，而不需要授权节点。得益于分类账节点，交易传播的速度变得更快。

投票节点
投票节点是达斯币区块链的非授权影响者。这些节点不控制达斯币系统的任何日常功能，但完全控制达斯币董事会成员，控制系统提交的方案。投票节点是指重要利益相关方，其已证明（通过他们承诺持有至少 1 万个达斯币 2-5 年）自身长期看好达斯币，因此被授予对链治理有影响力的特权。每个投票节点都可用其相应的私钥签署交易，从而就链治理问题发表意见。

在网络钱包专门区域进行投票，需要由专用的双因素硬件设备（即验证器）进行验证。投票可单独进行，也可在多个投票区块中进行，例如特定钱包帐户有多个深层保管库合约或一个或多个高级深层保管库合约。任何合格的投票节点都可发起提议。达斯董事会负责组织并向投票节点用户群提交提议。投票系统中还有一个机制，可让投票节点直接邀请其成员进行全体投票，而无需通过董事会审核流程（以防止董事会拒绝投票节点的某个提议）。

每个帐户持有人都可承诺期望数量的投票合约，并在系统中获得对应的票数。每个投票在链选举和全体投票中都具有同等权重。投票合约旨在强制用户锁定达斯币余额作为系统中的权益，因此在信守其承诺方面拥有既得利益。

去中心化的共识机制

合约期限（2 年）的设定预期是，投票将合理偏向长期价值增长，而非短期增长，因为承诺被锁定，无法从短期市场动态中获利。

区块生产

每个主节点都有平等机会来生产区块。在每个主节点参与产生区块之前，其顺序会再次随机排列。这可防止任一主节点控制区块生产，进而导致网络不稳定和交易未在分类账中得到确认。每 6 秒钟选择一个主节点，其负责为索引生成区块。如果其不能生产区块，那么下一主节点将接管为相同索引生产区块。将遵循此协议生产区块链中的所有类型的区块。

软件更新

区块链软件将要实现超时升级，表现为系统的完善和功能的落实。因此，即使在技术处于运行状态时，也有可能对其进行升级。至少有 51% 的主节点必须批准软件更改，才能将其整合到网络的整体效用中，从而达斯币利益相关者可提出功能需求，开发人员可对软件性能进行优化。

由于系统采用混合架构，当软件更新获得至少 51% 的主节点批准，就可进行集中部署。集中部署消除了所谓的“硬分叉”（货币系统分为两个独立的网络）的可能性。这是系统生产节点内部不一致造成的结果，将导致许多负面结果。由于其运算结构，在所有分散式加密货币在统计上，硬分叉是不可避免的。而在达斯系统中，硬分叉是不可能的。在批准软件更新后，所有核心节点都会更新，并且所有社区节点也会在协议中更新。该群体将占至少 51% 的主节点，并将继续运算达斯区块链。拒绝软件更新的任何其余社区节点在达斯区块链运算中将不再被识别，并且将不再接收其超级区块分配。

隐私权

达斯区块链是一个被许可系统，这意味着所有用户帐户都必须由注册机构（在用户帐户通过数字钱包系统处理）进行验证和批准。

我们将“状态”定义为关于用户数据（帐户、余额等）的共识。与比特币衍生产品不同，用户状态存在于所有节点上作为内存数据，并可自由访问。

中心化的共识机制

通过跟踪最长的可用区块链达成网络共识来维护该状态。节点可通过按顺序应用每个记录的交易，回放最长的路径，达到当前的状态（或过去任何区块的状态）。

因为节点应用程序定期访问和修改状态，因此无法以加密格式储存在磁盘上（事实上，为提高性能，数据必须驻留在 RAM 中，造成访问控制更加困难）。

达斯区块链内的假设是区块链上的所有数据都是公开的。用户帐户（以及与帐户 ID 关联的余额）不会储存个人身份信息。所有私人数据都以加密冷存储形式储存在独立私人身份验证服务器上。因此，只有用户自己知道其帐户 ID，确保外部人士无法获取用户的隐私信息。

为了实现透明操作，达斯区块链必须向公众开放。这要求区块浏览器（即 DasCoinExplorer.com）显示未筛选过的区块以及交易的所有数据。通过参与深层保管库合约，用户可部署自己的分类账节点以观察区块链并查询状态（余额、帐户和其他数据）。

验证服务器应显示用于 KYC 验证目的的用户数据，以符合法律法规。用户能够了解这一情况（以及守法的必要性）。

在此隐私模式下，用户必须信任达斯网络的身份验证服务。用户仍可对系统期望合理的隐私权，因为其余额不为外部各方所知。KYC 信息也根据法定要求在当前加密货币交换系统中提供。因为会损害网络价值，身份验证服务有合理的理由不向外部其他方泄露私人信息。它也减少了用户必须对网络持有的信任程度。由于所有交易都是公开的，因此不可能操纵余额和用户状态。

唯一的要求是确保验证服务器不被入侵。然而，相比保护整个网络来说这比较简单，因为攻击面更小，因此可以严格管理访问控制。如果数据得到正确的保护和共享，那么潜在的入侵不会导致隐私完全丧失，因为攻击者仅能获得一定的私人数据。

高速节点网络

主节点只需储存其私人签名密钥，并与网络其余节点进行验证，达斯生态系统作为区块链和加密货币可提供新的功能和可能性。这意味着主节点只需要在生成区块之前根据历史记录验证交易。节点验证所有签名和余额越快，就能够越快产生区块并继续。因此，确认和交易将以前所未有的速度进行。

硬件和网络配置质量较高，就可更好地捕捉世界各地的交易，极大地提高了商业可靠性和稳定性。因为这些进展，网络可在 6 秒内确认交易并允许余额更新。区块链软件的优化将大幅减少确认和传播区块所需的时间。

中间件

达斯网是一个先进的网络，其设计用于区块链托管和全球访问交易捕获和验证。因此，达斯币托管在专门设计的最先进的网络架构上，其可提供可靠的网络并实现全球扩展。

硬件基础设施
主节点专门托管在数据中心内，满足了对服务器机架的访问进行物理保护的要求。通过直连线支持稳定而高度连接的带宽，主节点协调地与世界各地的其它数据中心连接起来。此方法以让达斯网能够控制数据中心之间的整个路径，并且可防止保持区块链及其服务连接的节点免遭中间人攻击以及拒绝服务和分布式拒绝服务攻击。

除上述核心基础设施功能之外，达斯网还有 2 层用于处理交易捕获和网络连接。服务器配置包括最先进的优质组件和威胁预防保护和硬件防火墙解决方案，这通常在银行和其他高度安全的环境中使用。此外，达斯网托管在性能强大的服务器上，每台服务器运行 44 核，空间使用和功耗极为高效，能扩展到适合全球使用的极高流量和使用率。

达斯网在全球 33 个地区的数据中心共有 33 个核心主节点。核心主节点安装将以每月大约 2 个的速度推进。达斯网上还将运行大约 3000 个核心分类帐节点。此外，深层保管库合约还要求在达斯网基础设施中添加成千上万的社区主节点和分类账节点。

软件基础设施
与达斯区块链的连接也依赖于软件级服务，在保持高度隔离性和安全性的同时提供对核心服务的访问。这些服务提供并支持核心服务负载平衡以及冗余和易扩展性，，更多可能需要的网络资源将随着网络使用率增长。

对达斯区块链的访问需要配置授权方从区块链及其内部运算传输相关信息。进行每天 24 小 时，每周 7 天的监控和支持，维护外部服务和核心服务的关键参数。所有这些组件和服务将实现高速区块生产率并保持运算完整性。所有活动之间不可变的加密连接保护着达斯区块链和达斯网的原则。

中间件

核心开发团队
核心开发团队负责实施和维护硬件基础设施。

所有软件基础设施也是由核心开发团队开发和维护。董事会负责确保核心开发团队的行动是基于整个生态系统的最佳利益。主节点由生态系统高管、董事会董事和 达斯币 社区的重要利益相关方控制。在达斯网基础设施内，不允许任何个人或公司控制 3 个以上的主节点。

许可制度

个人或实体若要成为这个经身份验证的网络的活跃参与者，他们必须获得许可证。区块链软件允许授权服务以连接和注册新帐户。（以欧元或比特币计算）许可证级别将由所贡献的价值决定，这决定了个人或实体参与网络的范围。购买许可证后，收件人必须注册钱包帐户才能充分利用许可证带来的机会。

保管库帐户

保管库帐户保存用户个人信息，其实际上是接收许可证的帐户。帐户注册到达斯区块链，许可证由许可证颁发机构指派。授予许可证后，保管库帐户将收到"周期 Cycle"。保管库帐户的转移限制具体取决于许可证级别和身份验证级别。若要使用保管库帐户，必须将其连接到钱包帐户。保管库帐户也是将"周期 Cycle"提交给 达斯币 造币队列的帐户。

钱包帐户

钱包帐户为 达斯网 的参与者提供交易服务。此帐户可接受来自保管库帐户的转移，并可执行汇出交易以及将资金转移到网络上的其他钱包和保管库帐户。钱包帐户持有者还可通过钱包使用各种功能，包括投票和社区分类账节点或社区主节点（对应于深层保管库合约）的运算。

捆绑

所有保管库帐户必须连接到钱包帐户。然后这两种帐户捆绑在一起，不可拆解。钱包帐户可连接到用户愿共享的任意数量的保管库帐户。捆绑流程包括同时从保管库和钱包帐户签名以执行成功的捆绑交易。该过程由许可实体通过电子邮件和短信组合发送的安全邀请发起。

KYC & AML（了解您的客户和反洗钱）

每个保管库帐户必须获得许可证才能让个人或实体访问 达斯网。许可证级别和相应的 KYC 级别还将决定保管库帐户有资格向钱包帐户转移的每日金额。较高的许可证级别能让个人或实体提高其身份验证水平，并因此增加其在系统内的访问范围和取款权限。通过这种方式，达斯区块链和 达斯网 可完全符合全球法规，其要求帐户持有者在与 达斯生态系统的其他参与者进行商业交易之前确认身份且信誉良好。这种身份验证协议可提高参与者的诚信水平，并可能在全球范围内受到更多地区接纳。

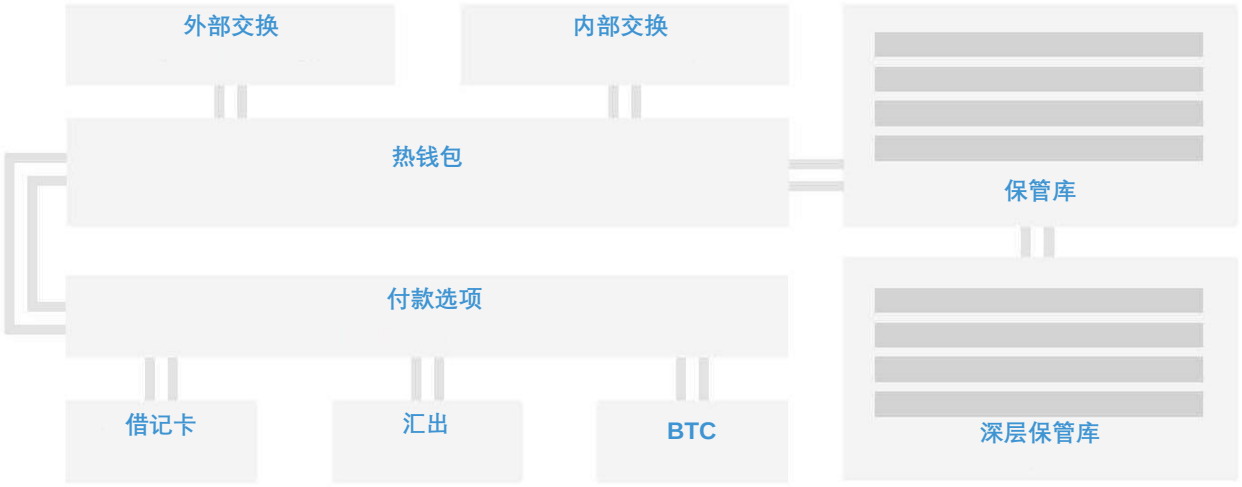
网络钱包

网络钱包是用户访问达斯区块链上相关数据的安全访问点，并通过签署交易与全局状态进行交互。它是一个加密的网络钱包，客户端前端运行在用户浏览器上，应用服务器后端托管在互联网网络服务器上。网络钱包是用户进入安全达斯网络的入口点。每个网络钱包 帐户都将用户链接到其保管库和钱包，并用于储存和验证个人 KYC 和 AML 信息。通过网络钱包 进行身份验证的用户能从全局区块链状态访问其相关数据，即保管库余额、许可证购买、交易历史记录等。

网络钱包依靠加密硬件存储来管理密钥并安全签署区块链交易。这种专有硬件设备被称为验证器，能够生成和储存与用户区块链保管库相对应的 ECDSA 私钥。验证器还有 PIN/密码保护，防止密钥误用和被盗。

签署区块链交易时，网络钱包与验证器硬件设备接口。用户需先解锁其验证器，然后在确认交易时将所需的 ECDSA 私钥传输到 JavaScript 客户端应用程序的浏览器内存。没有此加密硬件设备进行验证就无法进行达斯币交易。该系统在交易认证中提供了最高级别的安全性和安防性。密钥储存在内存中的时间极短，仅在签署交易后就从客户端内存中清除。私钥永不会“变热”，即永远不会穿过线路，即使是加密形式。

用户可以备份 24 字组成的助记符，用作生成私钥熵。硬件设备被盗或丢失时，用户可使用助记符重建原始私钥，恢复对其帐户的访问。



达斯币造币

生产和分配新 达斯币 的过程称为造币。这可让个人或实体以达斯币的形式储存价值。为了获得达斯币，用户应将“周期 Cycle”提交给网络，然后在 达斯币 造币队列中被指派一个位置。根据先进先出原则，达斯币 被分配到分配队列中下一个帐户。在每个 达斯币 分配间隔中，特定数量的达斯币将分配给队列中的参与者。

要收到的 达斯币 数量由一个称为“频率”的可调转换因子进行调节，这样提交的“周期 Cycle”数除以“频率”就等于将要分配给此人的 达斯币 数量。在提交时以及分配时，将从该帐户扣除“周期 Cycle”，达斯币 会由区块链软件自动转移到帐户中。

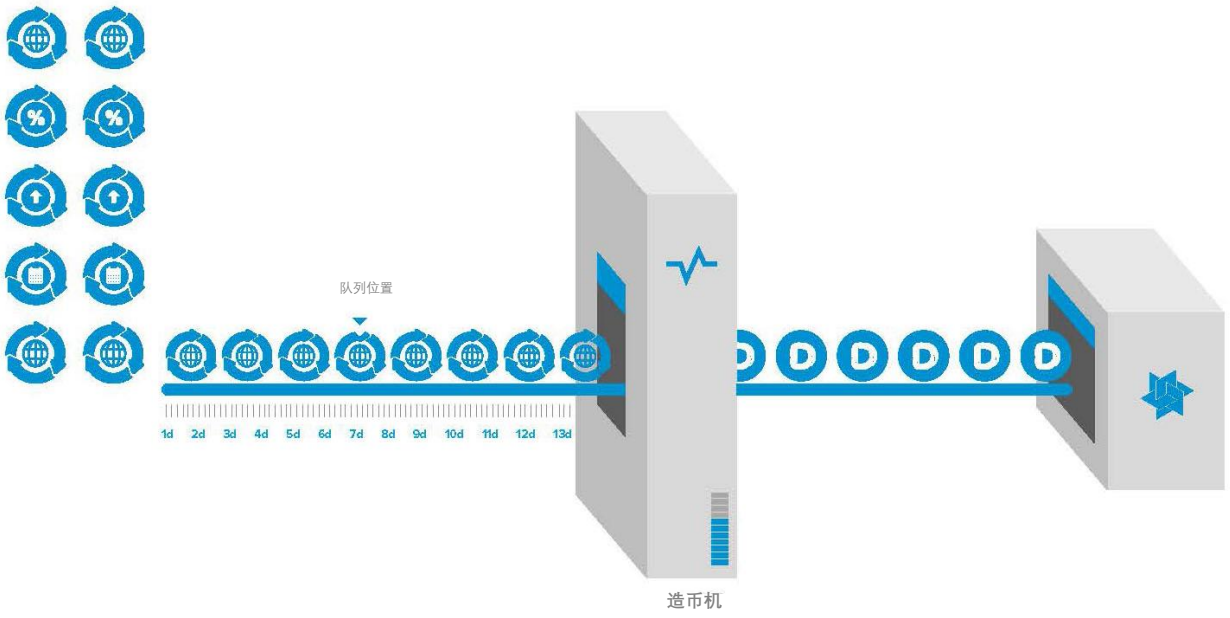
分配按照以下算法完成：

```
While amount_to_distribute > 0 and not queue.empty() do
        element = queue.front()
        If element.frequency_lock exists then
                Dascoin = element.cycles/element.frequency_lock
        Else
                Dascoin = element.cycles/global_frequecy
        End if
        If amount_to_distribute >= dascoin then
                queue.pop_front()
                issue dascoin to element.accaunt_id
                amount_to_distribute = amount_to_distribute - dascoin
        Else
                If element.frequency_lock_exists Then
                        cycles_to_remove = amount_to_distribute * element.frequency_lock
                Else
                        cycles_to_remove = amount_to_distribute * global_frequency
                Endif
                issue amount_to_distribute to element.account_id
                element.cycles = element.cycles - cycles_to_remove
                queue.update_front(element)
        Endif
Loop

当要_分配的_金额 > 0 且没有队列.空() 时
        元素 = 队列.前部()
        如果元素.频率_锁定存在 则
                达斯币 = 元素.周期Cycle/元素.频率_锁定
        或者
                达斯币 = 元素.周期Cycle/全局_频率
        结束如果
        如果要_分配的_金额 >= 达斯币 则
                队列.弹出_前部()
                向元素.帐户_id 发放要_分配的_金额
                要_分配的_金额 = 要_分配的_金额 - 达斯币
        或者
                如果元素.频率_锁定_存在 则
                    要_移除的_周期Cycle = 要_分配的_金额 * 元素.频率_锁定
                或者
                    要_移除的_周期Cycle = 要_分配的_金额 * 全局.频率
                结束如果
                向元素.帐户_id 发放要_分配的_金额
                元素.周期Cycle = 元素.周期Cycle – 要_移除的_周期Cycle
                队列.更新_前部(元素)
        结束如果
重复周期Cycle
```

达斯币造币

按照预先确定的升级间隔，所有“周期 Cycle”余额都会定期进行升级，帐户余额将翻倍。如果“周期 Cycle”已在 达斯币 造币队列中，这些“周期 Cycle”将不会受到影响（除非它们与频率锁定的帐户关联）。



区块链内部交换

达斯区块链还包含一个去中心化的交易所，可自主交易、结算和清除区块链。这样获得许可证的用户就不必选择将其货币转移到集中式交易所的托管帐户，才能进行某种形式的交易。例如，WebEuro 也是与达斯币类似的加密资产，因此无需从钱包取款，持有者可直接在区块链上交易达斯币以换取欧元面额。

因此，第三方盗窃可能性大大降低，交易和转换为国家法定货币的摩擦将更为简单直接。使用汇出功能，达斯区块链的许可证用户可通过网络钱包 帐户从其银行帐户提取欧元。

网络治理

投票节点

达斯币 治理始于投票节点，其在钱包帐户中持有至少 1 万个 达斯币，并承诺通过深层保管库合约持有这些达斯币 至少 2 年。所有投票节点皆可通过在达斯董事会正式选举中投票，积极推选达斯董事会成员并参加未来关键问题的全体投票，籍此对网络运行发表看法。

达斯董事会

达斯区块链使治理董事会能够管理网络的参数。达斯币 董事会将由投票节点选出的成员组成。董事会的角色是：

1. 建议并修改链参数以支持网络的正常运行和增长。

2. 将某些高管角色委派给某些链高管（例如颁发许可证和所述许可证身份验证）。

3. 通过终止网络访问来约束所述高管的权力。

董事会本身无法控制数据库的状态或 达斯区块链的构建，并且计划性地组织其进行任何更改。由于网络本身管理和维护着状态及交易分类帐，因此做出恶意更改的唯一方法是推翻大多数主节点。

董事会设计由 7 名独立董事组成，每名董事均享有充分的投票权。一般而言，每位董事任期为六年，但初任董事任期可能重叠（2-6 年）以确保经验的连续性。达斯币 生态系统的治理至少需要 3 名董事，董事会最多可有 9 名董事任职。

此外董事会还有一名监察员，其不参与投票，也没有在董事会中担任任何职责，但其出席董事会所有会议并为董事会治理流程提供一定的独立性和透明度。

最后，还有一名执行董事为董事会工作，负责确保其所有决策和举措得到制定和实行。执行董事出席所有董事会会议但不允许投票。执行董事负责直接监督所有的链机构。

网络治理

区块链机构

链授权角色是为了将系统外部存在的用户数据顺畅地输入到区块链。完全分散式系统的问题是无法有可靠的输入：例如，比特币在比特币区块链内部创建，且只能转移。为使“价值证明”发挥作用，必须确保用户实际上为网络创造价值。如果没有独立的观察者，价值就无法存在，因此验证用户向系统提交价值的唯一方法是设立公正的观察者。

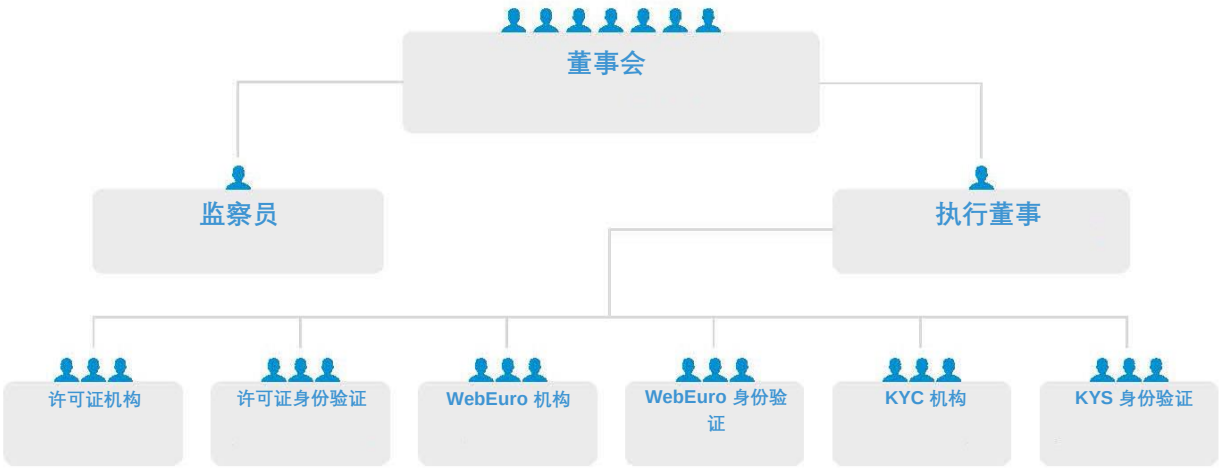
每个机构角色的设置方式如下：

1. 因为网络能恢复到故障安全状态，因此机构无法对网络状态产生有意义的不利影响。

2. 机构的行为由独立身份验证机构进行检查，且有程序措施确保共谋的可能性极小。

3. 出于网络的最大利益行动是有充分理由的。

4. 区块链机构的任何恶意行为都是透明的，并且会导致该帐户被标记为不可信，从而关闭网络并受到处罚。



网络治理

运营

董事会制定程序并要确保妥善执行以下内容：每两周间隔的“频率”水平；每个升级间隔开始时造币区块的大小；超级区块和司库区块的大小；提交给投票节点的建议；使用司库区块的资金；达斯网基础设施内主节点和分类账节点的授权；危机时期的干预以及其他因素（在董事会参数下列出）。

执行董事监督所有区块链机构和 KYC 职能的绩效，管理董事会建议审核流程，在超过相应阈值时启动全体投票，负责执行所有董事会举措和决策，并对系统内的所有运算对董事会完全负责。

在执行董事的监督下，链机构负责监督许可证和 WebEuro 的发放和身份验证。

“频率”每二周调整一次。该过程需要董事会选择哪套算法最能反映当前网络的增长状态。考虑的主要因素包括：系统中“周期 Cycle”总量；在最近的二周内授权的“周期 Cycle”数量；前几个期间“周期 Cycle”增长速度，以及系统内预计的“周期 Cycle”增长。

从启动 达斯区块链开始的 108 天后，系统将在特定日期自动进行升级。此间隔不会在将来的任何时候发生改变，但如果董事会认为有必要，仍可对其进行调整。所有深层保管库合约也可自动运行。实质上，造币过程、升级和深度保管库合约都是能自动执行并直接在达斯生态系统中产生的智能合约。

全局参数

下列是达斯董事会可提议更改的一组参数：

许可证颁发机构 - 有权将许可证指派到保管库帐户并确定许可证级别。

许可证身份验证机构 - 可在出错时取消为新帐户颁发的许可证。

WebEuro 颁发机构 - 有权将 WebEUR 余额转移到保管库帐户。

网络治理

WebEuro 身份验证机构
可在出错时取消向帐户颁发的 WebEUR 余额。

周期 Cycle 升级日期和间隔
升级的确切日期和升级间隔。升级间隔目前为 108 天，预计不会改变。

频率
作为造币过程的一部分，可将“周期 Cycle”换成达斯币的换算因子。

区块
累计交易的衡量尺度。系统当前根据指定期限记录一个区块，称为区块间隔。

区块间隔
确认单个区块交易所需的时间。
默认情况下，交易每 6 秒确认一次。将来，随着代码库进一步优化，这一时间将会减少。

造币区块
每个造币间隔结束时分配的 达斯币 数量。

造币间隔
创建造币区块所用的时间。系统的默认造币间隔为 10 分钟，预计不会改变。

维护期间
在区块链上执行维护之前必须通过的块数。

维护跳过槽位
在维护期间，一些区块将被跳过：此参数设置执行维护期间时系统应跳过的数量。

超级区块
在每种超级区块间隔完成时分配的 达斯币 数量。超级区块的大小表示为该超级区块间隔内由造币区块分配的累积 达斯币的百分比。有三种超级区块，每种都与特定深层保管库合约相对应：投票超级区块、分类账超级区块、主超级区块。

网络治理

超级区块间隔
超级区块创建所需的时间。系统内有 3 种超级区块间隔，每个都对应一种超级区块。投票超级区块间隔为 1 周，分类账超级区块间隔为 2 周，主超级区块间隔为 3 周。

司库区块
司库区块间隔结束时分配的达斯币数量。与超级区块一样，司库区块表示为司库分区块间隔内由造币区块分配的累积 达斯币 的百分比。

司库区块间隔
创建司库区块所用的时间。司库区块间隔为 4 周。

最大区块大小
区块链规定区块可以容纳的最大字节数。（以字节为单位）。

最大交易大小
单笔交易所允许的最大字节数（以字节为单位）。

最大证人计数
这是可在网络上活动的主节点的最大数量。

帐户哈希/名称长度:	介于 3 到 63 个字符之间
交易大小:	1024B
区块之间时间:	6 秒。
维护间隔之间的时间:	1 天
维护持续时间（跳过的区块数）:	3 个区块
升级之间时间:	108 天
造币之间时间（造币间隔）:	10 分钟

整体系统效率

比特币和基于比特币分叉的链依靠 UTXO 对象数据库来追踪每个地址/帐户的代币余额。在比特币中，每笔交易都会消费（花费）上一交易的输出，并产生新的输出供未来交易消费，从而形成新的仅可消费一次的未花费交易输出 (UTXO)。虽然这个模型有一些有益的数学属性，并且可用来防止比特币的双重花费，但其也有严重的限制：它不够复杂，并且天生无状态，因此不适用于天生有状态的应用程序，例如操纵自定义资产并保存智能合约执行的状态。

而达斯区块链则依赖共享链状态，这是内存数据库中有关用户数据的状态对象，例如帐户、达斯币 余额（可能还有其他资产）、造币信息，如 达斯币 造币队列、关于智能合约执行的信息等。区块链节点通过应用先前区块的交易来形成状态。通过遵循节点可看到的最长链区块来达到状态共识。区块链状态通过按顺序应用交易可完全重现。

达斯区块链的主要目标之一就是快速交易。由于每个节点都在内存中储存共享状态，交易可在整个网络中快速验证。这极大增加了可包含在区块中的交易数量，进而提高了网络的整体吞吐量。由于签名区块不需要工作证明，每个证人均可快速对照全局状态收集和验证交易，形成有效交易区块，使用自己的区块签名密钥进行签名，并将签名区块传输到其余的网络。节点也可在遇到共识失败时快速回滚交易，既适用于区块被拒绝（由于在分叉解决期间在较短分叉上）也适用于由于交易过期而未被包括在任何区块中。

区块链完整性验证

达斯区块链是一个加密链接的区块系列。这些区块建立了一个永久的交易记录，这些记录已由维护和记录区块链权限的主节点验证和确认。由此，储存在区块链中的每个操作都有一个永久且唯一的标识符。

因为这些特点，区块链中的整个活动历史记录可随时重放并检查完整性。审计人员可被授权使用程序化工具来评估和检查所有操作的余额是否一致和正确。这就避免了区块链的中央参与者或操作人员或任何入侵者能够操纵区块链内容。所有操作均需要内容所有者的签名才可以实施新的更改。帐户所有者是唯一能够更改其余额并且操作人员无法恶意或强制转移或修改余额。

作为负责董事会监督协议的一部分，其要求聘请独立第三方会计事务所来验证所有区块链活动的真实性。事务所将通过董事会控制的司库资金得到报酬，并且可以访问至少 2 个分类账节点，其中他们可根据设计的验证协议进行全面的查询和测试。达斯区块链准确性和完整性的验证将在每月进行一次，这些测试协议结果将提供给 达斯网 系统内的所有参与者。

每月区块链完整性验证协议的目的是增加对系统的信任。该协议旨在保护网络的安全，维护参与者的隐私，同时还为第三方会计师事务所提供完全的访问权限，以查询系统内活跃的账本节 点，提高整个达斯币区块链上操作的透明度。

网络拓展

随着越来越多的人加入网络，系统的效用值也会增加。为了实现扩大网络的目标，已在网络软件中建立了推荐营销系统，旨在奖励每个参与者个人对网络增长的影响的相应贡献。因此，该网络不是利用资源来支付工作证明挖矿的成本，而是为参与者提供激励来扩大网络。

这种激励系统可通过许可证证明共识模式的内在效率来实现。达斯币 区块链没有因保护对等服务器公开配置网络而带来财政负担，其采用更为有效的方法促进达成共识。

通过平衡集中式与分散式的特点，该系统能够通过充分随机但高效的共识方法进行自我管理。通过采用封闭系统架构，网络能够受益于区块链协议的所有优势，但没有与分散式开放系统架构的所有成本、低效和安全问题。这种被许可的区块链模式与许可证协议相结合产生的效率使网络能够为宣传者提供激励，使其在全球推广和扩大网络的优势。

该系统旨在解决新网络固有的风险，并根据其对网络发展的贡献为参与者提供奖励。这种动态为网络的扩大提供了强大的营销信任。

结论

目前为止，还没有充分关注支持区块链部署的基础设施的要求，特别是与可靠性、可用性、可扩展性和可维护性有关的因素。这些是确保区块链在主流用户金融生活中发挥正常作用的关键因素。质量保证的整体水平取决于区块链技术，主要是因为大多数区块链技术的分散性本身的局限性。

达斯币旨在解决妨碍主流用户采用数字货币的问题。达斯币是基于提供更高安全性、效率、性能和可扩展性而创建。达斯生态系统还利用其基础设施的效率来激励其扩张。进而我们得到一个建立在稳健货币原则基础上的数字价值系统，其非常适合吸引全球主流用户。

达斯系统的结果是完全实现了网络信任，其中经身份验证的用户可通过专用虚拟私人网络交易各种资产。最终，所有种类数字资产的交易皆可跨越国界在世界任何地方任何时间进行，且可即时完成，安全无忧且成本几乎为零。而这只是达斯生态系统可能实现的第一阶段。

通过信任数字模式，我们能够实现所有这些可能性。信任是达斯币的货币，而达斯币是信任的货币。随着梦想成为现实，达斯币将在全球创造前所未有的财富。

DasCoin™