一个让互联网出版商和内容行业可以使用智能社交货币的协议

介绍

Steem为可公开访问和不可篡改的内容提供了一个可扩展的区块链协议[1]，同时带来快速和低费用的数字代币(称为STEEM)[2]，使得人们可以运用他们的脑力赚取代币(被称为“脑力证明”)。此协议的两个部分，区块链和代币，互相依赖对方的安全性、不变性和持久性，相互依存。Steem已经成功运营一年多，目前已经在处理的交易数量上超过了比特币和以太坊.[3]

相比其他区块链项目，Steem以首个能公开访问的、以明文形式保存不可篡改内容并内置奖励机制的数据库脱颖而出。这使得Steem成为一个公共出版平台，任何互联网应用可以从从中获取和共享数据，并奖励那些贡献最有价值内容的人。

在加密货币领域，和其他代币如比特币和以太币相比，STEEM的独特性质使它显得“智能”和“社交”。这源于两个新的代币特性。第一个是致力于激励内容创建和筛选的代币池(称为“奖励池”)。第二个是投票制度，利用大众智慧来评估内容价值和分配代币。当这些独特性能组合时，我们称为脑力证明(Proof-of-Brain)，这是基于工作量证明(Proof-of-Work)[4]的双关语，旨在强调分配代币给社区参与者的所需人力工作。脑力证明定位STEEM作为一种工具来建立不断成长的社区，鼓励其成员通过内置的奖励架构来增加社区的价值。

除了在区块链和代币技术的这些进步，Steem为系统提供额外的高级功能来提升用户体验，如被盗账号恢复[5]，托管服务，用户内容推广，信誉系统和储蓄账户。这一切都已经完成并且同时用户的所有交易仅需三秒确认时间和零收费。所有这些使得它能够支持在互联网上为出版商和社区建设者带来智能社交货币的使命。

脑力证明：智能社交代币

一个奖励用户的代币系统，当用户为基于代币的社区贡献价值，需要有机制来建立和评估内容的社交价值：我们称之为“脑力证明”。

奖励池(“代币从哪里来”)

Steem区块链其中一个最创新的(和最被人误解的)的是从“奖励池”把代币分发给有价值的内容创造者。要了解奖励池是什么，首先需要理解在基于DPoS的区块链中代币产生方式是不同于基于PoW区块链。在基于工作量证明的传统区块链，代币定期产生并随机分配给那些用机器在计算的人(矿工)。

不同于纯PoW的数字货币，在Steem里代币以固定的速度每三秒产生一个区块。基于区块链定义规则，这些代币被分发到在系统里各个参与者。这些参与者，如内容创作者、见证人和筛选人，以专

---

1 Delegated Proof of Stake Position Paper. Grigg, 2017. https://steemit.com/eos/@iang/seeking-consensus-on-consensus-dpos-or-delegated-proof-of-stake-and-the-two-generals-problem

2 To differentiate it from the term for its blockchain, the correct spelling of Steem's native digital token is STEEM.

3 Transaction Volumes: Transactions Per Second Report. Steem Witness and user “@roadscape”. https://steemit.com/blockchain/@roadscape/tps-report-2-the-flippening

4 Proof-of-Work. Wikipedia. https://en.wikipedia.org/wiki/Proof-of-work_system

5 Stolen Account Recovery initiation for Steemit.com users: 07-13-2017 https://steemit.com/recover_account_step_1

门的方式竞争代币。不同于传统的PoW方式里矿工以原始的算力竞争代币分配，Steem网络激励参与者以增加网络价值的方式来竞争。

从2016年12月开始，新代币的年产生率为9.5%，每250000个区块下降0.01%，每年大约减少0.5%。通货膨胀率将继续以这样的速度下降，直到大约20.5年后，达到0.95%。

Steem区块链每年供应的新代币里，75%组成“奖励池”分配给内容创作者和内容筛选人。15%分布于既定的代币持有者，10%分配给见证人，即在Steem DPoS共识协议里合作的区块生产者。

内容创作者和筛选人的奖励

生产内容的用户通过创作内容将新用户吸引到平台上，同时也保持现有用户参与和娱乐，从而增加了网络的价值。这有助于将代币分配给更广泛的用户群并增加网络效应。而花时间对内容进行评估和投票的用户在代币分配中扮演着重要的角色，把代币分配给对添加最大价值的用户。区块链通过股权加权投票系统集合大众智慧，决定这些活动的价值并进行相应奖励。

以股份代币投票来决定分配奖励

Steem在一币一票的模式下运作。在这种模式下，以账户余额衡量最多，对平台贡献最大的个人，对内容如何计分贡献有最大影响。股份可以购买或赚取。用户不能通过拥有多个账户来获得额外的影响，因为持有一定数量股份的单个账户和共享相同数量股份的两个不同账户有相同影响力。用户增加平台影响力的唯一途径是增加他们的股份。

此外，Steem只允许成员以STEEM投票，即承诺行权周期为期13周的Steem Power。在这种模式下，成员有经济奖励的动机以最大限度地提高STEEM的长期价值。

Steem区块链的速度和规模

Steem的设计是现有的最快和最有效的区块链项目之一，因为这必须要能够支持预计流量比Reddit还大的社交媒体平台。Steem已经在交易数量上超过了比特币，并能扩展到每秒支持10000个或更多交易。

委托权益证明(DPoS)

受限于工作量证明的瓶颈(PoW)[6]，许多区块链速度不能超过每秒三笔交易，而这只相当于是世界金融流量的一小部分。Steem需要有比PoW能提供的更大规模和更快速度，所以一个鲜为人知的称为委托权益证明股权(DPoS)[7]的算法，用来成为适合数十亿用户的区块链基础。

因为DPoS，Steem区块链以最小的计算量每隔3秒就生成一个新区块。这意味着，区块链可以处理更多的交易和存储更多包含用户内容的信息。

通过定义硬分叉发生时的规则，在DPoS框架内当选的见证人可以快速有效地决定是否继续进行一个被提议的硬分叉，从而允许Steem区块链协议可以比其他技术更快发展。Steem区块链已经成功进行了18次硬分叉[8]，每次硬分叉之后只有一条链会被保留下来。

---

6 Bitcoin Scalability Problem
https://en.wikipedia.org/wiki/Bitcoin_scalability_problem

7 DPoS Whitepaper
https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

8 https://steemit.com/steemit/@steemitblog/proposing-hardfork-0-20-0-velocity

链库技术(ChainBase)

链库技术[9]是区块链栈的数据库部分，在2016年取代了石墨烯区块技术[10]。链库技术有更快的加载和退出时间，支持并行存取数据库和比其之前技术更好的防瘫痪。它的数据库损坏频率更低，允许即时“快照”整个数据库的状态，可以在相同的内存服务更多的RPC请求。

应用库技术(AppBase)

应用库技术是创建多链FABRIC的第一步。应用库技术模块化了Steem区块链的许多组件，即通过创建额外的非共识区块链专用插件模块。因为他们不需要回放整个区块链，这些插件可以很快更新。这使得steemd[11]更有效、更易维护和扩展。

实际上，应用库允许不同的内核，甚至不同的计算机，来维护Steem区块链的不同部分。这比要求每个内核和网络中每台计算机维护整个区块链更显著高效。区块链模块化能够充分利用计算机的模块化性质。这是创造一个完全并行、全面优化的区块链的长期过程中必要的第一步，。

Steem的平台特性

Steem区块链有两大目的，即作为一个数字代币处理系统，以及主流的社交媒体平台。由Steem区块链提供的特性需要满足这两个目的，并在使用平台方面为用户提供世界一流的用户体验。

为内容应用程序而生

Steem为用户提供将不同类型的内容以明文形式直接永久地发布和存储到区块链里不可篡改的账本上的独特能力。一旦数据存储在区块链，即公开可为开发者使用。开发者能够利用API直接在区块链与内容进行交互。开发人员可以使用的几个区块链原始数据包括账户名称、文章、评论、投票和账户余额。

自然名称系统

许多区块链技术，如比特币和以太坊，历来使用的钱包地址是一长串的随机字母和数字。然而，用户无法凭记忆回想起这么长串字符的地址，这使得钱包地址很难在典型的线上社交媒体中与别人互动。Steem区块链以每个参与者的用户名作为其的钱包地址，支持那些试图发送代币的参与者可以凭自己的记忆来验证地址，提升用户体验。

Steem美元(SBD)

许多被数字货币介绍来这里的用户在努力了解这个平台奖励的“神奇网络代币”如何可以有真实世界里的价值。为了帮助缩小主流用户使用的更传统的法定货币系统和用户在这个平台奖赏所得数字货币代币之间的差距，Steem创建了一个被称为Steem美元(SBD)新货币。

---

9 ChainBase Release
https://steemit.com/steem/@steemitblog/announcing-steem-0-14-4-shared-db-preview-release

10 Graphene Documentation
http://docs.bitshares.org/

11 The component of the Steem blockchain framework responsible for processing transactions and the distribution of rewards.

SBD代币被设计成紧密锚定一美元，所以用户收到SBD可以知道它们大概相当多少“真实美元”的价值。如果用户希望保持其相对于美元的账户价值，SBD代币为他们提供了一个相对稳定货币。更详细的技术说明可以在Steem技术白皮书查看.[12]

去中心化交易所

Steem区块链提供去中心化的代币交易所，类似于Bitshares比特股交易所.[13]交易所允许用户通过去中心化、点对点的公共市场来交换他们的STEEM和SBD代币。用户可以下买单和卖单，由区块链自动执行订单匹配。还有一个可公开访问的订单簿和订单历史，用户可以使用它来分析市场。用户可以直接使用区块链API和交易所交互，或使用一个用户图形界面，例如Steemit.com的GUI。[14]

通过托管的支付

区块链交易的不可逆性质是一个重要的安全功能，但在许多情况下，当发送自己的代币给另一人，而对方没有履行协议并没有办法要回代币，　用户可能不舒服。Steem区块链提供给用户发送代币给彼此一个指定的第三方，作为托管服务的一种方式。作为代管服务的用户能够确定协议的条款是否已经满足，允许资金被释放给接收者或者返回给发送者。

分层私钥结构

Steem使用一种分层私钥系统来方便分别执行低安全级和高安全级的不同交易。低安全级交易往往是社交性的，如发帖或评论。高安全级交易往往是代币发送和密钥更改。这允许用户有不同安全级别的私钥，再取决于私钥允许的访问权限执行不同任务。

这些私钥分别是发帖私钥，活跃私钥和所有者私钥。发帖私钥允许账户发帖，评论，编辑，投票，转发[15]，关注和屏蔽其他账户。活跃私钥是设计为更敏感的任务，如转移资金，启动/关闭交易，转换Steem美元，投票见证人，交易市场下单，以及重置发帖私钥。所有者私钥意味着仅在必要时使用。它是最重要的私钥，因为它可以更改帐户的任何私钥，包括所有者私钥，并在帐户恢复期间证明所有权。理想情况下，它是脱机存储的，仅在帐户的私钥需要更改或恢复被盗的帐户时使用。

Steem也设计了主密码来方便加密这三个私钥。Webservices可以使用主密码解密并提供必要的私钥签名。主密码可以允许用户信任某些服务，以防止不恰当的密钥在任何服务器上传输，从而保持安全的客户端签名环境，同时增加用户体验。

多重签名权限

Steem区块链允许一个权限可以拆分给多个实体，这样多个用户可以共享相同的权限，或需要多个实体的授权才能使一个交易生效。这是和Bitshares比特股[16]同样的方式，即每个公钥/私钥密钥对

---

12 Steem Whitepaper
https://steem.io/SteemWhitePaper.pdf

13 Bitshares Decentralized Exchange
http://docs.bitshares.org/_downloads/bitshares-general.pdf

14 Steemit.com Currency Market
https://steemit.com/market

15 “Resteem” is the term used in the Steem blockchain for when a user shares the content with their followers.

16 Bitshares Flexible Identity Management
http://docs.bitshares.org/_downloads/bitshares-general.pdf

都分配一个权重，以及给权限定义了门槛阈值。为了使交易生效，必须有足够多的实体签名，以便它们的权重之和达到或超过权限所需的门槛阈值。

多重受益人奖励机制

对于任何一个给定的文章，可能会有许多不同的人对奖金感兴趣。这包括作者，共同作者，推荐人，评论者和工具开发者。任何用于构建文章或评论的网站或工具都有能力设置报酬是如何分配给各方的。这促进各种形式的合作，建立在Steem区块链之上的平台也可以分得来自用户的部分奖励。

智能媒体代币(SMT)

智能媒体代币(SMT)是可以在Steem区块链上构建的原生代币。 STEEM是第一个SMT，而智能媒体代币协议的目的就是通过允许人们创建类似于STEEM的代币从而使得互联网上的内容网站和应用程序货币化。这些新代币可以通过定制适合不同在线社区激励行为的属性， 从而在任何网站或应用程序上面复制STEEMs的成功。

更详细的技术说明可以在SMT技术白皮书中查阅[17]。

被盗账号恢复

如果用户的帐户被盗，他们可以使所有者私钥来更改私钥。如果黑客盗取所有者私钥和更改帐户密码，用户有30天的时间里提交以前的私钥,通过Steem的账号被盗恢复功能来恢复他们的帐户控制。这账号被盗恢复功能可能是由提供Steem注册服务的个人或公司来提供。Steem注册服务提供商无须一定要向其用户提供这项服务，但这可增加其注册用户的用户体验。

通过时间锁的安全保护

如果用户的活跃私钥或所有者私钥被盗取，黑客可以完全访问其帐户中的所有资金。由于区块链的交易是不可逆的，用户没有办法收回他们已经被盗的资金。

Steem区块链允许用户把他们的STEEM和SBD代币存储在储蓄账户上，使得资金在三天的等候期后才能提现。此外，Steem提现需要在七天的初始等待期后，以每周1/13的速度提取。这些时间锁定可以防止攻击者能够立即访问用户的全部资金，以便合法所有者在损失其所有资金之前有时间重新控制其帐户。

免费操作的带宽容限

因为见证人是完全通过新代币的生成来获得支付，用户无需交费来运转区块链。收取手续费的唯一原因是为了防止用户进行不合理数量的交易，因为这可能会影响区块链的性能。

为了对系统的使用做出合理的限制，每个用户都有有限的带宽。每当用户执行区块链操作如代币发送，发帖内容和投票，即使用了他们的一部分带宽。如果用户使用超过其带宽容限，他们必须等待带宽充值后才可以执行其他操作。

---

17 Smart Media Tokens Whitepaper
https://smt.steem.io/smt-whitepaper.pdf

带宽限制是基于网络使用而调整的，因此当网络使用率较低时，用户有更高的带宽容限。一个帐户所允许的带宽容限和其所有的Steem权力成正比，因此用户可以通过得到额外的Steem权力来增加带宽津贴。

结论

Steem区块链代币提供的独特奖励和激励方案，都是为了使得Steem最终成为主流用户使用数字货币的入口。Steem区块链的性能是以考虑成为人们普遍采用的货币和平台来设计。当结合闪电般快速处理时间和低费用交易，Steem旨在成为一个世界各地的人使用的领先的区块链技术。