一个使网上出版商和内容行业可以使用智能社交货币的协议

介绍

Steem为公开的、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、费用低的数字代币（称为STEEM[2]) 使人们运用他们的脑力赚取货币（被称为“脑力证明”）。此协议的两个部分，即区块链与代币，相互依赖以达成安全性、不变性与持久性的目的，因此两方对彼此而言都是必需的。Steem已经成功运营一年多，现在已经在交易处理的数量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的数据库脱颖而出，并内置奖励机制。这使得Steem成为一个公共出版平台，任何互联网应用可以获取和共享数据，并奖励那些提供最有价值内容的人。

在加密货币领域，和其他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永远成长的社区，鼓励其成员通过内置的奖励架构来增加社区的价值。

除了这些区块链和代币技术的进展，Steem为系统提供额外的高级功能，提升用户体验，如被盗账号恢复[5]，托管服务，用户推广内容，信誉系统和储蓄账户。这一切都已经完成，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")

其中一个最创新的（和最被人误解的）的Steem的区块链方面是“奖励池”从代币分发给有价值的内容创造者。为了了解奖励池是什么，首先需要理解代币产生方式在基于DPoS的区块链是不同于基于PoW区块链。在基于工作量证明的传统区块链，代币经常生产但随机分配给那些有机器在计算的人（矿工）。

不同于纯PoW的有数字货币，在Steem里代币以固定的速度每三秒一个区块产生。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。这些角色，如内容创作者、见证人和筛选人，以专门的方式争夺代币。不同于传统的PoW方式里矿工以原始计算能力竞争分配，在Steem网络里参与者以激励竞争的方式给网络增加价值。

新代币的产生率从2016年12月开始每年为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，同时也让现有的用户继续参与其中并得到娱乐，从而增加了对网络的价值。这有助于将货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。通过股权加权投票系统，区块链在相对于他们价值的基础上，集合大众智慧来奖励这些活动。

以股权代币投票来决定分配奖励

Steem在[一STEEM一票]的模式下运作。在这种模式下，对平台贡献最大的个人，以他们的账户余额衡量，对如何计分贡献有最大影响。可以购买或赚取股份。用户不能通过拥有多个账户获得额外的影响，因为一个持有一定数量股份的账户将有两个不同账户共享相同数量的股权的影响相同。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企图成为当前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在比Reddit还大流量的社

交媒体平台。Steem已经在交易次数上超过了比特币，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(PoW)[6]，许多区块链不能扩展超过每秒三笔交易，而这只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括内容的信息。

通过设计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进行一个被提议的硬分叉，以允许Steem区块链框架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可以被保留下来。

ChainBase

ChainBase[9]是区块链栈的数据库部分，在2016年更换了石墨烯Graphene[10]。ChainBase有更快的加载和退出时间，支持并行访问数据库和比其前任更好的防崩溃。它也有不频繁的数据库损坏，允许即时“快照”整个数据库的状态，可以相同的内存服务更多的RPC请求。

AppBase

AppBase是创建多链FABRIC的第一步。AppBase使Steem区块链的许多组件成为模块，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更有效和更容易维护和扩展[11]。

实际上，AppBase使不同的内核，甚至不同的计算机，保持Steem区块链的不同部分。这是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区块链有双重目的，即服务作为一个数字代币处理系统以及主流的社交媒体平台。由区块链提供的特性需要支持这两个目的，并为用户在使用平台方面提供世界一流的用户经验。

内容应用的原始设计

Steem提供用户独特能力，以明文形式发布和存储不同类型的内容直接、永久地保存到区块链里不可篡改的账本上。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在区块链与内容直接进行交互。开发人员可以使用的几个区块链原始数据包括账户名称、帖子、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，使得这些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自己的钱包地址，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 Blockchain Dollars (SBD)

许多被介绍数字货币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传统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，一个被称为Steem Blockchain Dollars(SBD)新货币被创建。

SBD代币设计成紧密锚定美元，所以用户收到他们可以大概知道它们相当多少“真正的美元”的价值。SBD代币还提供了一个相对稳定的货币为用户认为如果他们希望保持其账户价值相对于美元。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公共、去中心化、点对点的市场来交换他们的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直接和交易所交互，或使用一个GUI如Steemit.com.[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，用户可能不安，如果其他用户不遵守承诺，他们也无法把自己送出的代币收回来。Steem区块链提供给用户发送金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。

分层密钥结构

Steem使用一种分层密钥系统来方便低安全性和高安全性的交易。低安全性交易往往是社交性的，如发帖或评论。高安全性交易往往是代币发送和密钥更改。这允许用户取决于密钥允许的访问权限，为密钥实现不同级别的安全性。

这些私钥分发帖，活跃和所有者。发帖密钥允许账户发帖，评论，编辑，投票，转发[15]，关注/静音其他账户。活跃账户是更敏感的任务，如转移资金，启动/关闭交易，转化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必要时使用。它是最强大的密钥，因为它可以更改帐户的任何私钥，包括所有者密钥，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，仅在帐户的密钥需要更改或恢复受损害的帐户时使用。

Steem也方便使用主密码来加密这三个私钥的使用。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，以防止不正确的密钥在任何服务器上传输，从而在维护安全的客户

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。

多重奖励的受益者

对于任何一个给定的帖子，可能会有许多不同的人对奖金感兴趣。这包括作者，可能的共同作者，引荐人，主机提供商、博客评论和工具开发者。任何用于构建帖子或评论的网站或工具都有能力确定该评论的报酬是如何分配给各方的。这允许各种形式的合作，以及平台是建立在Steem区块链顶部来收集来自用户的部分奖励。

智能媒体代币(SMT)

此协议层正在开发中。该白皮书将被发布在这里。

被盗账号恢复

如果用户的帐户受到损害，他们可以使用他们的所有者私钥来更改密钥。在这次事件中，攻击者可以危及所有者私钥和更改帐户密码，用户有30天的时间通过Steem在区块链行业里第一个账号被盗恢复功能提交以前功能的私钥，并恢复他们的帐户控制。这可能是由一个人或一个公司的人提供注册服务给Steem。注册者不须向其用户提供这项服务，但可增加注册者其用户的用户经验。

通过时间锁的安全

如果用户的活跃密钥或所有者密钥被攻破，攻击者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，用户没有办法得到他们已经被偷了的钱。

Steem区块链允许用户存储他们的STEEM和SBD代币在储蓄账户上，使得资金在三天的等候期后才能提现。此外，Steem在13周的等待期举行只能达到1/13每周抽出，初始等待期后七天。这些时间锁定可以防止攻击者能够立即访问用户资金的全部，以便合法所有者在收回其所有资金之前有时间重新控制其帐户。

低费用操作的带宽速率限制

因为见证人是完全通过新代币生成来获得支付，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，它使用了他们的一部分带宽。如果用户超过其带宽津贴，他们必须等待，直到他们的带宽可以

执行其他操作。

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，用户有更高的带宽允许。一个帐户所允许的带宽数量和其所有的Steem Power成正比，因此用户可以通过得到额外的Steem Power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Steem最终成主流用户进入数字货币的入口。区块链的性能是以人们普遍采用的货币和平台设计。当结合闪电般快速的处理时间和低费用少的交易，Steem的定位是成为一个领先的世界各地的人使用的区块链技术。

文献

[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-thetwo-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

[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

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

[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