Stacks 2.0: 比特币的应用程序和智能合约

Muneeb Ali

白皮书文稿 v0.1
2020年12月

Stacks

引言

本文概述了Stacks 2.0区块链，这是一个一层区块链，为比特币带来了智能合约和分布式应用。我们引入了首个两个区块链之间的一致性算法。Stacks 2.0将智能合约和分布式应用与比特币的安全性、稳定性和经济实力融为一体。

区块链是互联网自30多年前诞生以来最重要的升级。有史以来第一次，您可以使用开放协议来定义和参与数字资产，释放出前所未有的新业务模式和功能。

比特币是最早最安全的区块链。它提供了一种任何一方都无法控制或改变的新型货币 [1]。比特币网络不仅为比特币加密货币提供了基础，也为通用结算协议提供了基础。

区块链使新型计算机程序成为可能: (a) 可以在区块链发布的智能合约以无需信用的方式执行，任何人都可以验证它们的输出，(b) 用户拥有的分布式应用程序，避免集中服务器。以太网展示了智能合约的力量，Stacks将这些能力带到了比特币中。

我们的论点是，分布式应用程序和用例最终将建立在比特币这个最强大、使用最广泛的区块链网络上，而不是分散的其他网络上。在互联网的早期，曾有几种相互竞争的协议。后来，TCP/IP成为了胜出的标准，其他一切都建立在它的基础上。比特币就是加密标准。

鉴于我们将比特币作为价值结算标准的论点，我们建立了首个两个区块链之间的共识算法，称为传输证明(PoX)，它连接了比特币和Stacks区块链，并扩展了比特币的功能。领导者选举发生在比特币链上，而新的区块被写入连接的Stacks链上。

Stacks 2.0区块链将 (a) 带来交易的可扩展性和 (b) 把通用智能合约引入比特币，而同时无需修改比特币。Stacks矿工使用比特币(BTC)开采新铸造的Stacks (STX)。Stacks持有者可以一致锁定他们的STX来赚取比特币，这使STX成为一种独特的加密资产，在BTC本链定价，并提供BTC收益。

Clarity语言是一个安全、可预测的智能合约语言，它会随着Stacks 2.0主网的推出而上线。它是由普林斯顿和麻省理工大学的科学家在过去两年中开发的。Clarity使智能合约的漏洞出现率大大减少，并允许开发人员直接围绕比特币状态编写逻辑。我们认为，将智能合约直接引入比特币可以让BTC变得更有价值，因为它让BTC可以被用于生产，而不只是一个被动持有的资产。

Stacks加密货币于2019年作为SEC首个合规加密货币面向公众发行。Stacks (STX)是Clarity智能合约的燃料。

声明: 本文不提供任何证券或代币，仅用于提供信息。论文中有一些前瞻性的陈述可能被证明不准确。此外，白皮书中的信息可能会过时。

为什么是比特币

比特币是最强大的主权区块链。比特币是防篡改的真理; 一个价值结算协议。一旦你有了真理的最终来源，其他分布式协议和用例就可以在此上建立。在传统的互联网上，TCP/IP协议是标准，人们不需要改变它就可以在其之上进行创新。协议一旦建立，就很难与之竞争。比特币是主权货币，是价值结算协议。全世界很可能会向一个价值标准靠拢。我们认为，考虑到比特币的网络效应、安全性和加密市场的主导地位，这一价值标准将是比特币。

人们有一种误解，认为比特币是"一招鲜"，除了储值之外没有其他用途。围绕比特币结算协议进行创新，启用通用智能合约和分布式应用，这都是可以实现的。比特币本身不需要改变。

在比特币上构建应用和智能合约有两个基本挑战:

1) 可扩展性: 比特币基链的交易能力有限。

2) 合同安全: 比特币区块链的脚本语言有限，不允许通用智能合约。这种设计选择确保了基础层的安全性。

Stacks区块链解决了可扩展性和安全智能合约的限制，并为比特币启用了应用和智能合约。我们通过 在两个区块链之间运行的独特共识算法来实现这一点。比特币区块链充当结算层和真理之源，而智能合约则在Stacks链上执行。

直接在比特币上实现可扩展的智能合约一直以来都是瓶颈，而Stacks区块链解锁了这一功能。我们在不修改比特币的情况下实现了这一点，比特币是实现此类应用和智能合约的关键设计要求。

比特币目前被用作(被动的)价值存储，比特币加密货币是比特币区块链的主要使用案例。目前在其他区块链测试的成功用例可以简单地移植或直接使用比特币构建。

赚取比特币:

利用比特币网络的安全性和直接用比特币链上的加密资本(BTC)是我们设计的优势。此外，我们的设计为Stacks加密货币带来了独特的经济效应，在这种情况下，STX持有者可以锁定他们的STX，然后从共识算法中获得BTC奖励。

比特币的固定、有限的供应和作为对冲通胀的用途，使得赚取 BTC货币具有吸引力。此外，随着智能合约在Stacks区块链的使用量增加，BTC的收益率也会增加 (见第6页)。

Stacks 2.0 设计

Stacks 2.0是一个第一层区块链，它连接到比特币以获得安全性，并支持分布式应用程序和可预测的 智能合约。Stacks 2.0实现了PoX挖矿，它锚定了比特币的安全性。领导人选举在比特币区块链进行，STX矿工在相连的Stacks区块链上写新的区块。有了PoX，就没有必要修改比特币来启用智能合约和应用程序了。

PoX共识机制有两种参与者: (a) STX矿工和 (b) STX持有者。

STX 矿工可以在比特币区块链和Stacks区块链上查看状态。STX矿工通过在比特币区块链上发送交易来参与领导人选举，可验证随机函数(VRF)随机选择每轮的领导人 (同时给予较高的BTC出价更多权重)，领导人在Stacks链上写入新的块。STX矿工获得新铸造的STX(代币奖励)，支付给他们的STX交易费用，以及每个区块的Clarity合同执行费用也用STX支付。STX矿工会有BTC采矿成本和花费BTC参加领导人选举。STX矿工可以将一个新的Stacks区块的总价值建模为BTX/STX链上交易对，如果他们从采矿中获得的STX比从外部交易所获得的更便宜，他们将参与采矿。

STX 持有者可以参与共识，并通过参与一个名为“Stacking”的流程获得BTC奖励。这个流程是用户将他们的STX锁定一个奖励周期 (大约两周)，运行或支持一个完整的节点，并通过STX交易在网络上发送有用的信息。积极参与Stacking的STX持有者将获得该周期的比特币奖励。与权益证明不同，STX持有人没有被slashing也可以叫“罚没”(协议规定的经济处罚)的风险。

Stacks 1.0是一个功能有限的初始设计，于2018年秋季在比特币之上推出。Stacks 2.0是一个重大的升级和功能完整的设计，预计将于2021年1月在主网上上线。本文仅涵盖Stacks 2.0，它取代了Stacks 1.0的技术设计[2]。

交易的可扩展性:

Stacks区块链的交易可以独立进行扩展，不依靠比特币链; 它们只是依靠比特币来达成最终目的。成千上万的Stacks交易在比特币上会产生一个散列; 作为共识的一部分，Stacks交易会自动在每一个比特币区块上“结算”。此外，Stacks引入了微块的概念，可以在几秒钟内进行初步确认。微块是未来可扩展性研究的主要领域，理论上，更快的共识算法可以在每个比特币块的比特币上建立数据的微块上运行。

比特币被Stacks用作结算协议。它是终极真理的源泉，也是Stacks区块散列历史的档案。交易的终结性目前与比特币联系在一起，我们相信比特币提供了一个强大的终结性概念，我们的设计从中受益。

Stacks 2.0区块链是用Rust写成的。协议细节和开源代码可以在Stacks GitHub库中找到 [3]。

PoX 共识

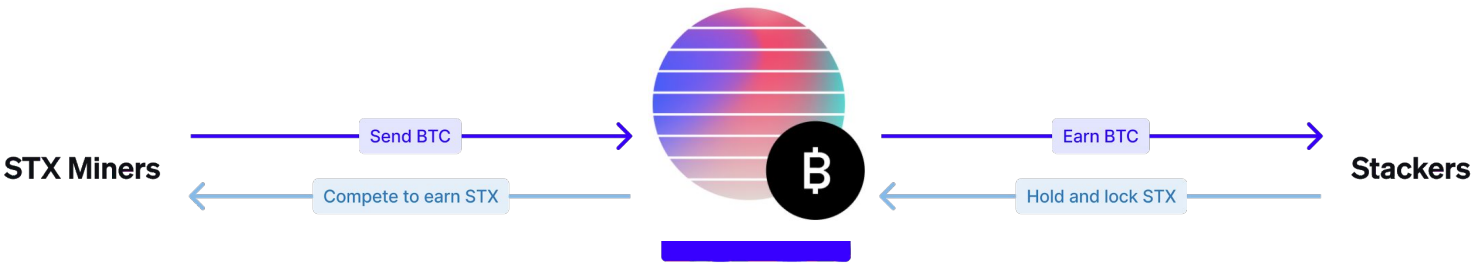
传输证明(PoX)是首个两个区块链之间的算法。具体来说，我们使用比特币作为基本链，Stacks作为连接链。在PoX中，领导人选举发生在比特币区块链上。PoX没有工作证明的烧电，而是将已经铸造的比特币作为"计算证明"重新使用，矿工直接用比特币作为他们的开采成本。

STX矿工竞拍争取成为下一轮的领导人。该协议使用可验证的随机函数(VRF)来选择每一轮的获胜矿工(即领导者) 。这位领导者撰写Stacks区块链的新块，并铸造奖励: 该块新铸造的Stacks，智能合约和交易的费用。

用于矿工出价的比特币被发送到一组特定的地址，这些地址对应于积极参与共识的Stacks(STX)币持有者 。因此，在挖掘过程中消耗的比特币不会被销毁，而是根据这些Stackers持有的Stacks和参与Stacking算法的情况，作为奖励，流向有贡献的Stacks持有者。

PoX 参数:

- 区块奖励: 前4年1000 STX/区块; 后续4年500 STX/区块; 此后4年250; 然后是永久性125 STX/区块
- 区块时间: Stacks区块链以与比特币相同的速度生产区块。比特币块大约每10分钟产生一次，因此这将是Stacks 2.0主网的速率。然而，值得一提的是，微块可以给出更快的初始确认。
- 区块奖励到期窗口: 100个区块，意味着如果矿工赢得一个区块，他们将在100个区块后获得该区块的代币奖励。
- Stacking参数: 每块2个奖励地址; 奖励周期2000块 (约2周), 总共4000个奖励槽。
- Stacking阈值: 所需的最小STX数量是基于参与度的动态值。当参与度在25%至100%之间时，该阈值为STX参与量的0.025%，当参与度低于25%时，阈值水平始终为STX流动供应量的0.00625%。



Proof of Transfer consensus mechanism

PoX共识的更多细节见PoX技术文件 [4]。

Clarity 智能合约

Clarity是一种新的智能合约编程语言。Clarity语言优化了可预测性和安全性。Stacks 2.0将Clarity智能合约锚定在比特币上，使智能合约能够根据在比特币区块链上看到的行为进行操作。

设计良好的智能合约可以防止错误，但设计不良的合约会加剧问题。这一点尤其重要，因为智能合约是用来保存数字货币的。通过Clarity，我们采取了“所见即所得”的方法。Clarity使智能合约的行为 、成本和性能对开发人员和自动验证都是透明的，并引入了附加安全条件 (post-conditions)。

可判定的语言:

Clarity是一种可判定的语言。如果一个人能够从代码本身确定地知道程序将做什么，那么该编程语言是可判定的。我们刻意将Clarity设计为图灵不完全(Turing incomplete)语言，因为它避免了“图灵复杂性”。这意味着Clarity允许对智能合约的整个调用图(call graph)进行完整的静态分析。此外，对类型和类型检查器的支持可以消除此类的所有错误，如非预期的强制转换(casts)、可重入错误(re-entrancy bugs)和未初始化值的读取。最后，Clarity代码的运行时成本和数据使用情况都可被分析。开发人员可以预测某个Clarity程序将做什么，以及它将有多少花费。

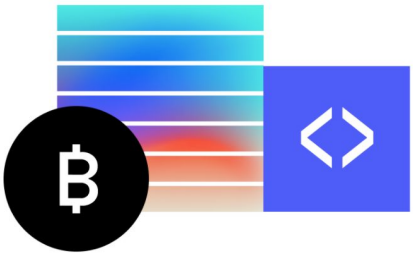
以太坊上合约的实现语言Solidity是一个不可判定的语言: 在某些情况下，如果不实际执行合约，就不可能准确地知道合约将如何运行。这两种编程语言都有优点。但是，当涉及到锁定数十亿美元到代码中的智能合约时，将风险降至最低至关重要。

没有编译器:

Clarity除了是一种可判定的语言之外，它也是解释性语言(interpreted)。合约源代码本身由区块链节点发布和执行。删除任何中间的、编译过的代码(例如，Solidity的EVM字节代码)进一步最小化了引入漏洞的机会。发布合同源代码也提高了可读性。在区块链上，编译器错误的破坏性是加倍的，因为尽管程序源代码可能没有错误，但最终到达区块链的程序可能会有错误。任何这样的错误都需要有争议的硬分叉——这种纠正可能是不可行的。

比特币状态的可见性:

Clarity合约可以看到比特币的状态，这意味着合约逻辑可以基于纯粹的比特币交易来触发。Clarity合约为比特币提供了内置的SPV证明，可以让开发者更容易与比特币状态互动。Clarity合约用比特币分叉，开发者不用担心比特币分叉和智能合约需要根据分叉调整的极端案例。



Stacks (STX) 加密货币

Stacks加密货币(STX)的设计主要是作为“燃料”来执行Clarity智能合约。Stacks还用于其他网络功能，如注册数字资产、支付交易费用，以及在区块链上发布Clarity合同。

Stacks可以被STX持有者锁定，参与共识，赚取比特币奖励。这个过程叫做Stacking。参与意味着STX持有者运行一个完整的节点，锁定他们的STX，并定期在网络上发布有用的信息。比特币奖励的年收益率取决于几个因素。例如，如果50%的流动供应量参与，以及其他假定的参数都参与其中，那么收益率大约为9%。查看详情 [5]。

Stacks加密货币是美国历史上第一次由SEC认证的代币并面向公众发行，共有4500多人/实体参与发行。

PoX共识机制在STX和BTC之间建立了本地交换对，使STX成为一项独特的资产，因为您可以锁定它以获得比特币收益。这不同于传统的权益证明资产，因为那些资产是以同样的加密货币给收益。

长期价值:

与其他加密货币一样，Stacks加密货币有几个风险因素会对该加密资产的价值产生负面影响。读者应查看2019年证券交易委员会发行的风险因素部分，了解这些风险的全面列表[6]。

Stacks的长期价值基本上取决于Stacks网络的增长和Clarity智能合约的需求量。要在网络上执行Clarity合约，用户需要支付STX作为燃料(燃气费)。例如，用Clarity合约构建的去中心化交易所需要STX作为费用以便用户在交易时执行交易所合约的逻辑。

鉴于比特币收益的独特属性，我们预计STX流动性供应的一个子集将被锁定，并从有效流动性供应中取出。这样的长期持有者希望赚取比特币奖励，就积极参与共识。比特币奖励对STX持有者的价值取决于 (a) 代币奖励和 (b) 网络使用。如果网络上执行了更多的Clarity合约，那么比特币的Stacking奖励也会增加。在最初的几年里，每个新块会释放1000个STX作为新铸造的代币(挖矿奖励)。除了代币奖励，合约和交易费用也决定了矿工对一个区块的估值。如果网络使用率上升，那么由于更高的合约和交易费用，区块对矿工的价值就会上升。这意味着矿工用比特币出价会更高，也就有更多BTC奖励流向积极参与共识的STX持有者。

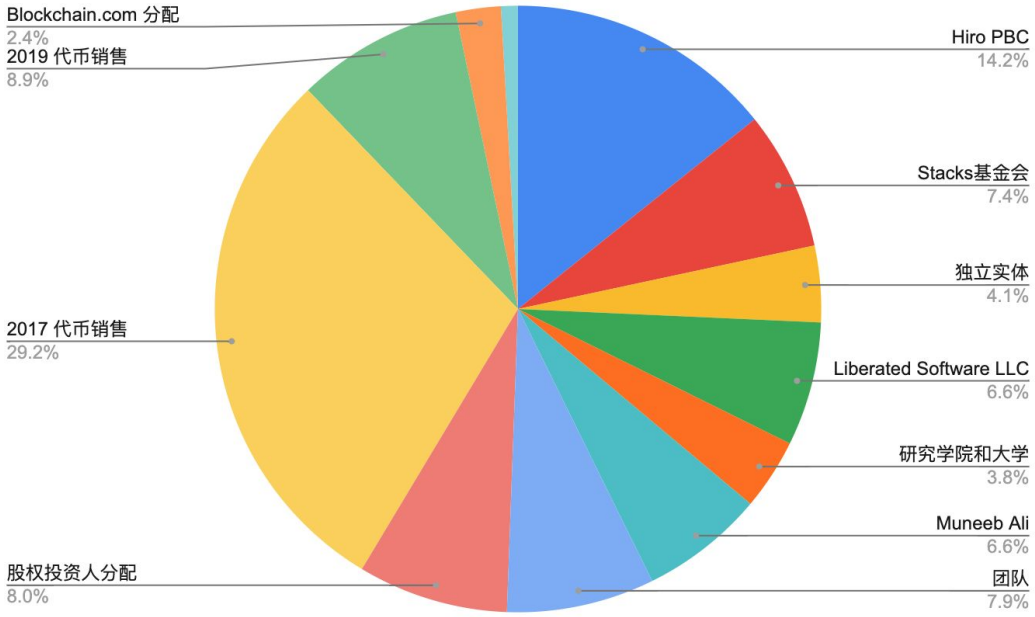
挖矿STX奖励	Clarity费用	交易费用

* 挖矿奖励STX遵循固定的预定时间表。
* Clarity费用和交易费用随着网络的使用率上升或下降。

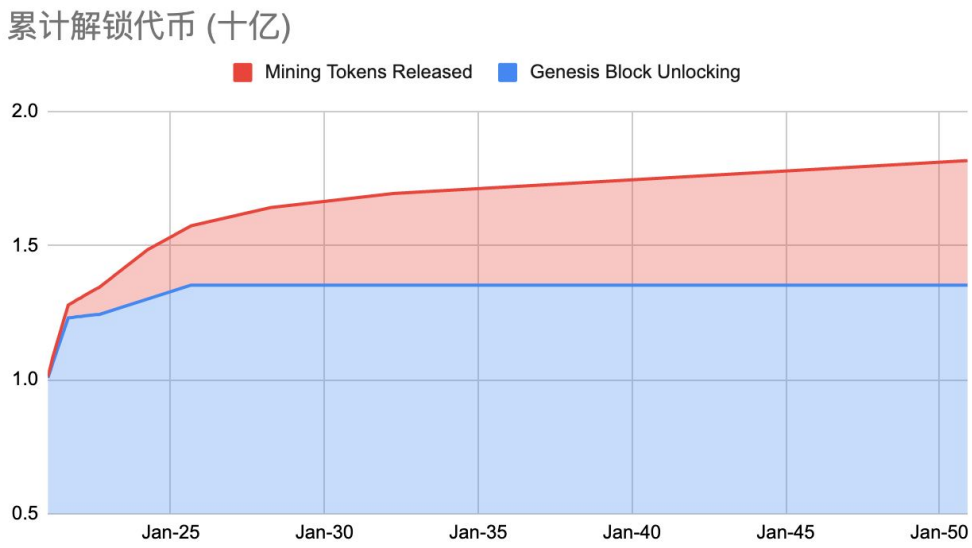
[BTC的出价与STX区块价值成正比]

代币经济

Stacks加密货币的创世区块中有13.2亿个STX [14]。这些STX在2017年和2019年通过几次发行进行了分发。2017年发行的STX价格为0.12美元，2019年的Reg S发行价格为0.25美元，2019年的SEC合规发行价格为0.30美元。下面的图1给出了创世纪块中代币的细分。



Stacks加密货币有一个预定的未来供应量，到2050年将达到约18.18亿 (比之前的20.40亿有所减少[14])。到2021年1月底，创世纪块中大约13.20亿STX中的10.06亿STX将是流动的，其余的将每月按照各个解锁方案解锁。例如，分配给创始人和员工的STX遵循3年解锁，其中一部分将在2021年1月至2021年11月之间解锁。图2显示了截至2050年Stacks总循环供应量的增长情况。详见[7]。



Stacks 生态系统

Stacks生态系统是一个独立实体、开发者和社区成员的集合，他们致力于在比特币上建立一个用户拥有的互联网。

项目历史:

该项目于2013年在普林斯顿计算机科学系启动，旨在建设一个更好的互联网。Muneeb Ali和Ryan Shea在2014年通过了Y Combinator，并招募了其他普林斯顿计算机科学家进行初步研发。早期投资者包括Union Square Ventures (USV)、Naval Ravikant、SV Angel等。Muneeb 2017年的博士论文为建立在区块链基础上的用户自有互联网奠定了技术基础 [8]。

该项目在2017年通过发行Stacks加密货币筹集了4700万美元，并在2019年作为首个获得美国证券交易委员会(SEC)资格的加密货币公司在美国Reg A发行和Reg S发行额外筹集了2300万美元。超过4500名Stacks持有者参与了此次发行，包括USV、Lux、DCG、Winklevoss Capital、Blockchain Capital、Foundation Capital、Hashkey、分布式资本 (Fenbushi)和其他公司。

分布式生态系统:

Blockstack PBC是一个公共福利公司，在2017年A轮融资后，致力于早期的R&D、协议设计和公共基础设施。公共基础设施建设阶段于2020年末完成，Blockstack PBC现更名为Hiro Systems，在Stacks 2.0发布后将专注于开发人员工具。

2020年，随着去中心化的路径，Stacks生态系统出现了几个独立的实体。其中包括非营利的Stacks基金会，一个以社区为中心的实体Freehold，一个以矿业和亚洲市场为中心的实体地灵科技 (Daemon Technologies)，以及专注独立用户端的New Internet Labs和主要做中文移动STX钱包和用户端的密钥工作室 (Secret Key Labs)。Stacks生态系统中已有 400 多个由独立开发者和实体开发的应用。

2020年秋天，Blockstack PBC发布了一份法律备忘录摘要，详细说明了Stacks(STX)加密货币在美国向非证券状态的过渡 [9]。

Hiro

Stacks Foundation

地灵科技
DAEMON TECHNOLOGIES

FREEHOLD

New Internet Labs

secretkey
LABS

Stacks 2.0 主网启动

Stacks 2.0的发布目前预计在2021年1月14日，与其说是Stacks 1.0的升级它更接近于一个全新项目的发布。Stacks 2.0是我们的主要计划，解决了比特币两个长期存在的问题: (a) 交易的可扩展性和 (b) 在不修改比特币区块链本身的情况下实现智能合约。

开始挖矿:

Stacks 2.0 主网的推出需要至少20家独立矿商。矿商们需要在.miner矿商命名空间登记处登记并遵循其他步骤 [10]。随着采矿的开始，每个区块的1000个STX将作为新铸造的STX发行 (作为STX采矿者打包/ 写入新STX区块的激励)。采矿的开始可以被认为是生态系统中一个新的小型去中心化交易所。每天大约有15万STX将通过BTC/STX链上对的挖矿进行“交易”。像其他区块链一样，挖矿公司只有在有利可图的情况下才会开采新的区块。对于Stacks 2.0，这意味着与目前支持BTC/STX对的其他交易所 (如币安) 相比，矿工可以通过BTC/STX采矿对获得比其他交易所更便宜的STX。与普通交易所相比，矿业交易所对的“交易量”预计相对较小，因为像币安这样的交易所目前的交易量约为数百万STX (相比之下，矿业交易所对的STX上限为15万)。

赚取比特币:

随着Stacks 2.0 主网的推出，流动STX供应的一个子集可能会被锁定，以积极参与共识。如果50%的流动供应与其他假定参数一起参与赚取BTC回报，那么BTC的收益大约为9% [5]。

参与共识所需的最小STX数量是动态的，取决于参与占流动供应的百分比。假设50%的流动供应参与，950万流动供应，则至少12万STX必须参与Stacking。但是，STX持有者可以使用共享服务，并且Stacks网络支持用户采用委托服务。

Clarity合约:

随着Stacks 2.0 主网的推出，执行Clarity智能合约的能力将得到实现。所有交易费和Clarity合约燃气费将以STX形式支付给矿工。

升级指南:

Stacks 2.0主网启动等于是Stacks 1.0的硬分支，所有STX余额和数字资产的所有权将自动转移到Stacks 2.0。Stacks 1.0和Stacks2.0之间不需要任何代币交换。STX持有者将需要升级到Stacks 2.0钱包 [11]，交易所和其他节点运营商可以遵循集成指南 [12]。

总结和未来工作

Stacks 2.0给比特币带来了应用和智能合同。我们的论点是，来自各个区块链的实验结果最终将在比特币上实现。比特币的网络效应意味着围绕比特币的智能合约可以获得更多的加密资本，并受益于更高的安全性。我们相信比特币可以成为更好的用户自有互联网的基础，就像传统互联网的TCP/IP一样。

Stacks 2.0为用户提供了一种通过积极参与共识来赚取比特币的新方式。我们的工作将被动的比特币资本转化为主动部署的资本，并为比特币生态系统带来更多应用和智能合同，使比特币变得更有价值。

在Stacks 2.0发布后，某些改进，如区块空间拍卖、更高的微块吞吐量和速度，以及高级Clarity语言 功能[13]，可能是Stacks基金会和广大社区未来努力的方向。

参考文献:

[1] S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”, Oct 2008. https://bitcoin.org/bitcoin.pdf

[2] M. Ali, R. Shea, J. Nelson and M. J. Freedman, “Blockstack: A New Internet for Decentralized Applications”, Whitepaper Version 1.1, Oct 2017.

[3] Stacks GitHub repository. https://github.com/blockstack/

[4] M. Ali, A. Blankstein, M. J. Freedman, L. Galabru, D. Gupta, J. Nelson, J. Soslow, P. Stanley, “PoX: Proof of Transfer Mining with Bitcoin”, Whitepaper v1.0 May 2020. https://blockstack.org/pox.pdf

[5] M. Ali, “Stacking Earnings Model: Projecting Consensus Participation Rewards for STX Holders”, Oct 2020. https://blog.blockstack.org/stacking-earnings-model/

[6] Blockstack Token LLC, SEC Offering Circular, May 2019. https://www.sec.gov/Archives/edgar/data/1719379/000110465919029828/a18-15736_1partiiandiii.htm

[7] STX future supply spreadsheet. https://github.com/zone117x/stx-supply-schedule/

[8] M. Ali, “Trust-to-Trust Design of a New Internet”, PhD dissertation, Princeton University, June 2017. https://muneebali.com/thesis

[9] M. Ali, “Stacks Cryptocurrency Expected To Reach Non-Security Status in the United States”, Dec 2020. https://blog.blockstack.org/stacks-cryptocurrency-expected-to-reach-non-security-status-in-the-united-states/

[10] D. Gupta, “[RFC] Stacks 1.0 → 2.0 Upgrade Process”, Nov 2020. https://forum.stacks.org/t/rfc-stacks-1-0-2-0-upgrade-process/11346

[11] Stacks 2.0 wallet. https://wallet.blockstack.org

[12] Stacks 2.0 Integration Guide, https://docs.blockstack.org/stacks-blockchain/overview

[13] J. Nelson, “After Stacks 2.0: Potential Features for Stacks 2.1”, Nov 2020. https://forum.stacks.org/t/after-stacks-2-0-potential-features-for-stacks-2-1/11376

[14] M. Ali, "Stacks Token Economics and Incentive Mechanisms", Whitepaper Ver 2.0.7, Oct 2019.

[15] V. Buterin, “A next-generation smart contract and decentralized application platform,” Ethereum whitepaper 2013. https://ethereum.org/en/whitepaper/.