The BOScoin White Paper

Initial Version: 20161101 / Current Version: 20170322

Han-Kyul Park, Changki Park, Yezune Choi, Jake Hyunduk Choi

BOScoin是用于 Trust Contracts的去中心化决策体系的加密货币平台.

摘要：BOScoin是一个使用了数据区块链及其它多项新技术，能够规避去中心化系统弊端的加密货币。（1）Trust Contracts是一个基于Owlchain的，拥有可决策性程序化框架的，能够安全运行的协议。Owlchain是具有可决策性的程序化框架，由Web Ontology Language Language(OWL)与 Timed Automata Language组成。该构成可以保障Trust Contract的安全运行，并能够克服既有智能协议因为不具有决策能力(undecidability)而造成的诸多问题。. (2) Congress Network作为 BOScoin 网络的决策机构，可以改善在分散型组织发生的支配管理问题，并促使系统能在坚固的生态圈中不断进化。

1. 引言

a. 背景

数据区快链是2008年由中本哲史在论文“Bitcoin: A Peer-to-Peer Electronic Cash System”中首次提出的新概念，并于第二年通过比特币的核心技术得以实现。比特币是一个可以公开记录个人货币传输信息的金融交易分类帐，使用了数据区块链技术。比特币是为了解决双重支付问题，而使用数据区块链的最早案例。虽然，没有中央集权管理者，它仍然成功实现了1.8亿个 P2P(peer-to-peer)交易，并达成了10亿美金以上的市值。

随着比特币的成功，应用数据区块链技术的系统层出不穷。目前，已有数百个加密货币百花齐放。据IBM近期报告所述，90%以上的银行正投资于数据区块链技术[1]。货币交易虽然是数据区块链技术最为普遍的应用，在金融商品及服务、物流信息、财产所有权、身份信息等其它数字资产使用数据区块链技术进行管理的尝试也不断增多。

2016年加密货币Ethereum获得了世人的瞩目。Ethereum是一个可以应用于任意状态变化函数实现的协议生成的，内嵌图灵-完整程序语言的数据区块链[2]，以向数据区块链提供智能协议为目标。

Ethereum的目标是让用户使用的所有程序或者协议能够应用于数据区块链。与比特币一样，Ethereum可以让试图使用数据区块链与协议机制，伪造恶意的节点内容的协议，最终被数据区块链清除。比特币可以让账户间传输的比特币量保持完整。而Ethereum也需要保障所运行的协议完整性。

智能协议能够让去中心化应用程序开发实现模式更替。即使程序不在中心化服务器运行，也可以在任何地点运行相同的逻辑。智能协议可以应用于诸如以去中心化市场、货币交易平台、去中心化全球超级计

[1] *Leading the Pack in Blockchain Banking: Trailblazers Set the Pace*, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN&

[2] Vitalik Buterin, *Ethereum Whitepaper*, https://github.com/ethereum/wiki/wiki/White-Paper

算机开发为目标的 Golem[3]项目。

但是Ethereum所使用的图灵-完整语言所具有的自由性与灵活性特点，成为了导致许多严重的问题的诱因。由于图灵-完整语言无法进行决策，所以不适于制定智能协议[4]。由于它不具有决策性，以图灵-完整语言为基础的智能程序将无法预知其运行后的情形。Ethereum试图应用相关计算工作的费用（煤气），来解决该问题。但是在开发、运行智能程序过程中所使用的语言内部固有的问题，将会引发一系列安全缺陷[5]，并导致类似于The DAO[6]的失败案例发生。

b. 建议

Trust Contracts.作为该问题的解决方案，BOScoin使用了可以让普通用户也可轻松读懂，并且能够通过数学证明其智能合同是否可以进行计算化决策的域细化语言(domain-specific language)。所以我们的目标是通过BOScoin，开发基于 Trust Contracts-Owlchain的技术，使协议平台能够安全运行。

同时，我们希望通过BOScoin解决加密货币所常见的问题。

决策问题 去中心化的系统缺乏一个系统化决策流程。在加密货币的世界里，有几个由于缺乏决策流程而导致问题出现的案例。BOScoin为了持续改善软件与整个生态圈，搭建了一个由组成议会网络的节点运营者参与的，能够提交Proposal，参与投票，称作'议会网络'的管理系统。BOScoin为了提升自治权及整个系统的公正性，设置了通过议会投票制定的，具有相当数量的，称作公共预算（Commons Budget）的公共预算。

防止中心化协议的算法 . 只使用PoW类型合约协议的类似于比特币的加密货币，由于其经济利益与政治利益未被分割，而导致了一些问题出现。通过购买更多的采掘（Mining）设备，用户可以提高其在数据区块链中的控制力（政治层面），并增加采掘收入（经济层面）。而BOScoin使用了区分经济利益与政治利益的合约机制（详情见下文），克服了这些问题。想要获得政治权利与经济收益，需要增加对系统的投资。用户可以通过扩充节点数增加投票数（运营中的一个节点意味着议会中的1票）或通过投资预存补偿金或区块生成补偿金（与节点数相挂钩的货币量之补偿），可以最大限度增加采掘收入。在这里所使用的合约协议的能量效率更高、更快。

应用程序生态圈. 由于去中心化的货币因其有限的使用场景，常常会成为投机的温床。我们认为货币价值应与该货币本质上的效用相关。所以，我们BOScoin小组推出了使用BOScoin的两种应用程序。已经开发完成的 Stardaq 及 Delicracy不仅可以提升该币的交易价值，对于增加用户也会有所裨益。

Features	Bitcoin	Ethereum	BOScoin
Coins	Bitcoin	Ether	BOScoin
Core Features	Financial Transactions (Bitcoin script)	Smart Contracts (Solidity, Serpent, etc)	Trust Contracts (OWL 2 profiles, SDLang, TAL)
Decision Making Process	Non-systematic	Non-systematic	Democratic Congress (One node = One vote)

[3] *Golem*, https://golem.network
[4] Hodges, Andrew*, Alan Turing: the enigma,* London: Burnett Books, p. 111
[5] N. Atzei, M. Bartoletti, T. Cimoli, *A survey of attacks on Ethereum smart contracts*, https://eprint.iacr.org/2016/1007.pdf
[6] *The DAO*, https://slock.it/dao.html

Consensus Algorithm	Proof of work	Current: Proof of work. Future: Casper(?)	Modified FBA(Federated Byzantine Agreement)
Transaction Speed	7 tx/sec	25 tx/sec	1,000 tx/sec (target)
Block Interval	10 minutes	13 seconds	5 seconds
Block Size	1 MB	Dynamic	Dynamic

Fig 1. 加密货币比较

2. Trust Contracts

A. 概要

BOScoin将使用由 Web Ontology Language (OWL)[7]与 Timed Automata Language (TAL)构成的 Owlchain 技术。该技术的设计结构既可以扩张其表现力，还可以保持能够使协议安全、准确的运行的可决策性。基于BOScoin的OWLchain 协议被称为 Trust Contracts。

Features	**Smart Contracts** (Ethereum)	**Ricardian Contracts** (R3CEV Corda)	**Trust Contracts** (BOScoin)
Programming Language	LLL, Serpent, Solidity	Ricardian Contract + pure functions	Owlchain (OWL* + TAL*)
Decidability	Undecidable with gas(fee)	Undecidable (3rd party evaluation)	Decidable(TAL)
Blockchain type	Permission-less	Permission	Permission-less
Consensus	PoW*	various	mFBA*
Contract Inference	None	None	OWL Reasoning
OWL*: Web Ontology Language TAL*: Timed Automata Language PoW*: Proof of Work mFBA*: modified Federated Byzantine Agreement			

Fig 2. 数据区块链为基础的Contracts 比较

B．背景

在数据区块链开发的协议有两种形式。一种是在虚拟设备中使用灵活的程序语言，另一种虽然缺乏灵活性，但采用了具有可决策性特点的域细化语言(domain-specific language) 的方式。BOScoin小组选择了第二种方式。与基于虚拟设备的加密货币不同，推论引擎基于赛门铁克网页技术，所以在代码运行前，无法从代码推论相关信息。协议具有可决策性，可明确性的特点。这是一个搭建具有协议功能的安全的，可持续的货币系统的核心概念。Ethereum为了解决这个问题，使用了市场机制，适用了复杂性价格。然而，我们认为以更为严格的OWL及TAL方式开发以数据区块链为基础的协议，能够提供更为安全的环

[7] *Web Ontology Language Reference*, https://www.w3.org/TR/owl-ref

境。

C．**开发**

基于HTML, HTTP, RDF 及OWL等标准网页技术进行开发时，可以让电脑通过可预测性分析共享信息。OWL与RDF将用于搭建不模糊的、结构化的数据分类体系。Ian Grigg提出了利用这些特性生成一个与所有支付系统组成要素相关联的协议 Ricardian Contracts的概念。OWL与RDF虽然具有相似的特性，但现在的RDF标准不支持P-time完整性。然而，OWL标准由于使用了在已获知的信息或在公理集合中，进行理论化结果推论的道具Reasoners，能够保障P-TIME的复杂性。这意味着可以事先决定运行协议所需的时间。这些特性是OWL成为Trust Contracts基础语言的核心原因。

OWL DL(description logic)是OWL的子语言，既可以保持计算的完整性，还可以最大限度施展其表现力[8]。 OWL DL与 ISO20022样式相同，在事先定义的庞大的语言及分类体系中运行。与交易相同，BOScoin特化的功能不在OWL指令集中提供，所以，其相关词汇及分类体系需要在协议之外调用。为了解决这些技术性问题，我们建议在数据区块链生成事先定义的Name Space Domain的方法。该Name Space Domain可以在协议中调用非标准化基本类型（分类体系）。为了保持OWL的可决策性及分类学的复杂功能， 将会谨慎添加非标准化基础类型。

```
Ontology {
    “http://blockchainos.org/remittance”
    Import "http://blockchainos.org/ontologies/remittance-v1.owl"
    Individual type="remittance" {
        Sender addr="1KrGTeQs55sf1zyTWWR4Y5qhe9Zxg2ftpy"
        Receiver addr="1FZNMuL8HUmf9TLdac62K4cGGpD2JEwnax" balance=1000 unit=BOS
        Receiver addr="1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX" balance=500 unit=BOS
    }
    operator name="remitance" addr=“http://blockchainos.org/tal-repo/remittance-v1.tal”
}
```

Fig 3. BOScoin传输案例

针对数据区块链的图灵-完整协议的另一个问题是非专业性人士很难读懂图灵-完整语言。如果说“代码即法条”那么代码应让所有人都能理解。如今，使用协议用图灵-完整语言的货币，只有了解代码的人才可以对其进行检查。BOSCoin采用OWL标准 及与SDLang[9]相同的语言与语法，任何人都可以读懂协议内容，并正确理解其协议所指的意思。

[8] *OWL Web Ontology Language*, https://www.w3.org/TR/owl-features/
[9] Simple Declarative Language, https://sdlang.org/

```
// Sample Proposal using SDLang format
Ontology {
    "http://blockchainos.org/proposal"
    Import "http://blockchainos.org/ontologies/proposal-v1.owl"
    Individual type="proposal" {
        Title "BOS Across The World"
        Owner "BOS-in-USA"
        Monthly-amount  BOS=180
        Completed-payments "no payments occurred yet (3 month remaining)"
        Payment-start-end   start=04-01-2017 end=19-04-2017 added-on=08-12-2016
        Please-vote-within  days=19
        Final-voting-deadline in-month=1
        Will-be-funded No // This proposal needs additional 232 Yes votes to become funded.

        Proposal-description {

            Description "BOS Across the World -- Weekly Show Interviewing Businesses and People"

            Overview "This is a 3-month pilot proposal to seek out real business owners, both
                conventional and unconventional, and conduct face-to-face interviews with them
                regarding the use of BOS and how it could be used."

            Scope "The scope of this project is not only to communicate the value of BOS to real
                people in real businesses, but it allows BOS developers and community to follow
                along and watch first-hand, how average people interact with BOS. Real-world
                interviews will be an invaluable feedback-loop to help eliminate or lessen the
                barriers to entry, while promoting BOS in creative and fun ways."

            Deliverables {
                "1. One show per week for 12 weeks. Tuesdays, delivered to various social media
                    channels like Youtube, and shared on Twitter."
                "2. Weekly frequent updates on the BOS.org proposal forum."
            }

            Schedule {
                "Each week, filming Wednesday to Friday (A+B footage)"
                "Each week, Saturday to Monday (Post, editing)"
                "Each week, Tuesday (Upload to social media channels)"
                "12 episodes in total"
            }

            Note "All audio-video, lighting and editing equipment is owned by me, and provided at
                no charge."
        }
    }
    Operator name="proposal" addr="http://blockchainos.org/tal-repo/proposal-v1.tal"
}

```

Fig 4. Trust Contract 案例

Timed Automata Language 的概念基于 Andrychowicz的论文 '基于Timed Automata的Bitcoin Contracts模型化'[10]。TAL用于在 Trust Contract中使用的程序逻辑模型化。OWL及TAL的关系与 HTML与Javascript的关系类似。OWL提供数据结构，TAL则作为演算法运行。程序语言的演算法是一个类似与加减法的执行特定功能的语句。OWL提供信息，TAL提供电脑数据处理方法。TAL由于有global time factor，与其它程序语言稍微不同。执行协议所需的时间可以预先进行测试。通过对所有结果事先进行自动化测试，可以提供数据区块链中无漏洞的协议平台。

[10] Andrychowicz, Dziembowski, Malinowski and Mazurek, *Modeling Bitcoin Contracts by Timed Automata*, Lecture Notes in Computer Science Formal Modeling and Analysis of Timed Systems, 7-22, 2014, https://arxiv.org/pdf/1405.1861v2.pdf

关于上述概念的详细内容将在技术报告中进行说明。

2. 协议算法

a. 概要

共识算法是基于数据区块链的货币或系统的核心。算法将致力于回答“如何证明所有分布式数据库存有相同信息的集合？”

针对这个问题，BOScoin采用了以Stellar合约协议（FBA）[11]为基础的修正的FBA（mFBA）协议算法。

Consensus Algorithm	Proof of Work	Tendermint	Byzantine Agreement	FBA[1]	mFBA[2] (BOScoin protocol)
Decentralized Control	O	O		O	O
Low Latency		O	O	O	O
Flexible Trust			O	O	O
Asymptotic Security		O	O	O	O
Governance Features					O
[1] Federated Byzantine Agreement [2] Modified Federated Byzantine Agreement					

Fig 5. 协议算法比较

Mazieres将 FBA协议的核心功能做了如下定义[12].

- 去中心化的控制：即使没有中央管理者的许可，任何人都可以参加讨论并达成协议。
- 更少的等待时间：节点可以设置人们通过网页或支付交易所需的等待时间（如：多少秒）。
- 灵活的信任：用户可以自由组合自己认为合适的项目。例如，较小的非营利机构也可令更大规模的机构保持对其的信任。
- 渐进的安全防护：安全依托于电子签名与Hash Family。这些变数可以通过现实化调整另庞大的计算能量免受敌对势力的攻击。
- 决策功能：投票及议会运营相关的投票功能作为协议的附加功能得到添加。

b. Federate Byzantine Agreement 协议算法[13]

[11] David Mazieres, *Stellar Consensus Protocol*, https://www.stellar.org/papers/stellar-consensus-protocol.pdf
[12] Ibid.
[13] Ibid.

比特币的协议机制与传统的拜占庭基础协议需要所有网络参与者达成一致。然而FBA不要求所有参与者都达成一致，各个节点可以根据自主判断进行选择。这可以让金融网络既能保持完整性，又可以实现有机的成长，达成更快捷的交易。
FBA由各个节点组成了小组（ 称作法定人数Quorum）群组。因此，即使无法达成一致，也可以建立协议机制。达成交易后，将向群组内的所有人传送信息。无需整个网络认可数据状态，当节点从可以信赖的节点获取足够数量的相同的信息，该节点将被视为信息正确。如果发生节点重复或者节点组松散，将创建同意同一个交易的归属不同小组的不同的节点。这样的机制，能够让各个交易数据区块，即使无法的到统一决策意见，也能够在整个系统中达成一致。

c. mFBA算法有什么不同?

除了FBA，BOScoin的合约协议为了进行管控系统的维护，适用了类似于股份证书的特性。即，用户在一个节点内可以预存10000个单位的BOScoin。作为遏制灵活性的作用的补偿，用户还可以获得与预存于节点的货币数相对应的新发行的BOScoin（类似于预存金的利息）。

预存于节点的货币，除了可以获得运行节点所需的经济奖励外，还将起到存储于节点数据区块链的信息安全与完整性的担保作用。根据实现设定的规则，如果发现节点伪造了数据区块链，预存的货币都将被没收至Commons Budget账户。

3. 议会网络

a. 概要

议会网络作为BOScoin的民主决策机构，由各个Full Nod的运营者组成。虽然，人们常说加密货币是一个去中心化的自动化货币，但大多数情况，事实并非如此。存储于代码与数据区块链的信息很容易受到上述二者的影响。为了克服这些问题，BOScoin建立了旨在完全去中心化，并实现自动化的称作 ‘议会网络’的决策机构。源代码开发、数据叉及营销资源可以从系统中获取。

b. 议会网络的作用

i. 议会成员

满足如下条件即可以成为议会成员

- 以稳定的网络速度，运行完全同步化的节点（Full Nod）
- 4个单位以上的货币预存（一个预存单位为10000BOS）
- 参加投票

任何人都可以成为议会成员。节点可以是议会成员使用的服务器或个人用电脑。只要网络速度稳定，节点可以设置于家用或远程服务器。

议会成员为了提高他们的政治影响力，可以运行更多的节点或通过扩大BOScoin预存，从而增加经济收入。

ii. Users

用户是BOScoin系统的受益人。他们将通过进行交易，提交提案，获得BOScoins利息等三种方式与BOScoins网络进行相互作用。相互作用如下图所示。

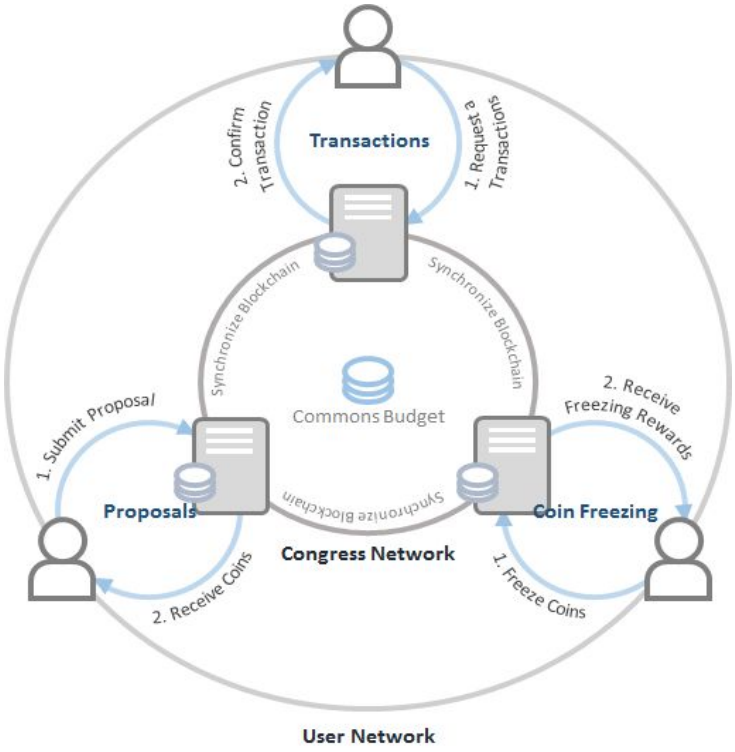

Fig 6. Congress Network与用户 Network 间的相互作用

c. 网络的相互作用

i. 交易

当用户请求进行交易，该请求将传输至议会网络。我们可以对BOScoin做个简单描述。即，当节点（约每5秒）确定数据区块，用户的交易被认可，BOScoin将转到其它账户。如果是较为复杂的Trust Contracts，将根据事先定义的逻辑与步骤运行。BOScoin的初期手续费将固定为0.01BOScoin，但该费率可通过议会网络投票进行调整。交易手续费，可以成为节点运营者的经济性奖励，也可用于建立针对DOS攻击的防御机制。

ii. 提案

提案是指提交到议会网络的公共预算使用计划。为了制定提案，并获得通过，必须让同意或拒绝的投票超过10%以上的差距。提案通过后，相关货币将汇入提案人的账户。在某种情况下，比如提案的规模较大时，可以要求提交系统货币的使用记录报告。

iii. 货币预存(Freezing)

货币预存是类似于POS的概念，当用户预存了货币，那么将根据它的数额和预存时间获得利息。该利息称作补偿金。用户可以预存以10000BOS为一个单位的货币。预存货币，可以作为数据区块链伪造保证金来使用。如果节点意图伪造数据区块链，那么预存的货币将被没收，并汇入公共预算账户。为了建立保持货币价格的稳定机制，取消货币预存至少要提前2周进行通报。

d. 补偿系统

议会网络有独特的奖励机制。议会成员可以在一个节点预存 BOScoin，以最大限度谋求经济补偿或通过运行多个节点（1节点如图1所示），最大限度增加投票权。

这样的划分类似于经济与政治权利分离的概念，要么奖励希望参与决策的动机，要么奖励希望获得经济补偿的动机。

由于比特币依托于PoW协议，导致Hash Power过于集中。导致少数的巨型采掘者可以轻松购买比特币采掘机。这将会导致代码变更，或者影响数据区块链的完整性。我们区分了寻求获得经济利益的人群，使得参与决策的门槛低于决策权限与金钱补偿相挂钩的系统。

议会成员获得BOScoin的方法有如下三种：

- **预存补偿金(Freezing Reward) :** 议会成员如果冻结了其货币，将获得与一般账户用户相同的利息。第一年起，总共11,500个BOScoins将被均分至各个预存的单位，该预存补偿金将在每720数据区块（约一个小时）发行一次。分配的总金额将在50年内，每年减少11.16%。

- **数据区块补偿金(Confirmation Reward) :** 确定数据区块后，数据区块生成补偿金将被提供至该节点。该补偿金是提供给节点运营者的核心奖励。该补偿金将与预存于节点的单位数挂钩。同比特币的数据区块补偿一样，参与的节点数增加，获得数据区块生成补偿金的概率减少。预存补偿金与存到节点的金额等比。补偿金将按每个数据区块平均补偿21的BOScoin开始。

$$confirmation\ reward\ = 21 \times \frac{Number\ of\ Frozen\ Units}{Average\ of\ Total\ System\ Frozen\ Units}$$

  第一个数据区块补偿金将从每个数据区块21BOS开始，在100年内，每年同比减少7.36%。

- **Transaction Fee:** 交易手续费固定为0.01BOScoin。议会节点将获得每个数据区块交易手续费的70%，30%将汇入公共预算账户。交易手续费可以通过议会进行调整。

e. 决策结构

关于BOScoin内嵌的决策流程的创意来自Dash Coin[14]使用的方式，即Master Nod[15]通过投票进行决策的方式。BOScoin的决策是在提交提案后，如提案投票表决通过，提案所需的资金将会汇入公共预算账户。任何人都可以提交提案，提交截止日期是每个月第三个星期一的GMT24点。然后，针对该提案，议会成员将会在第四个星期一的GMT24点前进行投票表决。同意或否决之间的百分比差超过10%，提案会

[14] Evan Duffield, Daniel Diaz, *Dash: A PrivacyCentric CryptoCurrency*, https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

[15] *Using Decentralized Governance: Proposals, Voting, and Budgets*, https://dashpay.atlassian.net/wiki/display/DOC/Using+Decentralized+Governance%3A+Proposals%2C+Voting%2C+and+Budgets

被通过。议会成员即使参加投票也有权保持中立，且在截止日期前随时可以更改意愿。

为了提高提案获得通过的概率，可以对提案进行担保。需要1,000,000 BOS以上货币的提案，被划分为上级提案。议会成员如果不对上级提案进行投票，他们将受到节点在两周内不能使用预存功能的处罚。货币预存功能停用，则节点将无法获得预存货币而获得的任何优惠，且在两周内无法预存货币。

f. 公共预算(Commons Budget)

公共预算(Commons Budget)是存放BOScoin的账户，只有通过了议会投票的提案方能汇款。公共预算的主要作用是在初期增加货币用户的数量。公共预算主要通过两个渠道进行积累。第一个是每个区块直接发行50BOS，（约6年）内，第二个是积累30%的交易手续费。发行的所有货币中，公共预算占据最多的部分。它可以保障大幅提高BOScoin使用率所需的资金。

任何通过了议会表决的提案都可以获得公共预算。比如说，可能有这样的一些提案。即，为了增加BOScoin的用户数，免费向用户发派Airdrop。或者为了进行BOScoin生态圈开发资金划拨，开展营销活动，亦或召开BOScoin相关会议等。

5. 事先开发的应用生态圈

许多加密货币在他们的平台上使用应用程序，并提供搭建方法相关案例。却很少有以该货币运行的应用程序。加密货币的价值很难通过交易价值以及投机价值组成水平来获得充分的了解，然而BOScoin的目标是通过与竞争单位进行比较，来提升交易的价值。长期来看，货币的核心价值在于该货币的使用价值。

与货币同步公开的如Stardaq及Delicracy这样的应用程序，能够让用户在BOScoin生态圈立即得到成熟、实用的服务。

a. Stardaq

Stardaq是知名人士人气预测市场。它将以知名人士指数来体现。用户可以根据知名人士的人气上升或下降与否进行投注，投注只能使用BOScoin。

b. Delicracy

Delicracy是任何组织都可以适用的集体决策系统。它与(Augur)的预测市场[16]相似，用户可以针对相关提案进行投注，并参与决策。投注最多的提案最终将被选定。这样的方式的系统将有助于在各类组织中增强决策的透明性与参与的积极性。

这些服务可以成为免费发行货币的渠道作用，还可以成为使用BOScoin市场的作用。这些工具使用得当将有利于发展用户，促进生态圈的成长。

这样的应用程序可以成为使用BOScoin的使用场所，还可以成为免费发行货币的渠道。 这些工具使用得当将有利于发展用户，促进生态圈的成长。

[16] Decentralized Prediction Market, https://www.augur.net/

6. 技术蓝图

下表是讲述主要日程的技术蓝图

Milestone → ↓ Module	**M1**		**M2**		**M3**		**M4**
P2P	Protocol specification & Implementation		Unit & Acceptance Test				
mFBA Consensus	Key design Implementation		Test App				
Remittance	Address design UTXO Pattern Send & Receive coin				Multisig Tx Specs		Multisig Tx Implementation
Data Store	Store specs & SQLite Store implementation		MessagePack History				Blockchain backup & restore using ISP(AWS, Azure and google)
CLI & Web Interface	Web design & implementation	**ALPHA**	Web UX design	**GENESIS**		**NEBULA**	
Trust Contract Proposal & Vote			Trust Contract design		Proposal & Vote implementation		
Simple payment verification wallets (Mobile)	Wallet Formal specification		UX design Application PoC Test				Android & iOS Wallet
Inference Engine			Formal spec. and key design elements available		Reasoner integration with Blockchain		Constructing Basic Ontology
Trust Contract Modeler					Formal spec. and key design elements		App Deployment & Demo Site

					available		
RPC & REST API			Blockchain Explorer				

Fig 7. 框架图

7. 货币发行

新的货币将以四种方式发行。早期开发预算（0.5bil，10%），区块生成补偿（1.8bil, 36 %），预存金补偿（0.9bil，18%）及 公共预算（1.8bil，36%）。我们将在100年内发行5.0亿个货币。这个数额也可能发生变化。

	Initial Development Budget	**Confirmation Rewards**	**Freezing Rewards**	**Commons Budget**
BOScoins	500,000,000	1,800,000,000	900,000,000	1,800,000,000
Share	10%	36%	18%	36%
Decrease Rate	-	7.36% per 6,311,520 blocks	11.16% per 6,311,520 blocks	-
End of Issuance	Genesis Block	Year 2117	Year 2067	Year 2023

Fig 8. 发行摘要

- **Initial Development Budget:** 早期开发的货币是在Genesis区块以前发行的货币，主要用于完成软件的开发。该货币由ICO销售及补偿（Bounty）组成。5亿个BOScoin将与Genesis数据区块一同发行。

- **Confirmation Rewards:** Confirmation rewards是针对所发行的数据区块（每5秒）的，随机支付给节点的金钱性补偿。由于补偿是随机进行的，随着节点数增加，单个节点获得补偿的概率将减少。该补偿将与预存于节点的单位数挂钩（参考4d图）。1.8亿BOScoin将作为区块生成的补偿发行。初期，每个区块将发行21个BOScoin。补偿将以每年631万区块的速度分100年，每年减少7.36%。

- **Freezing Rewards:** 是指针对预存金的补偿，将根据预存于节点的 BOScoin单位数进行分配，每720区块（约1小时）发行。初期的总金额为11500。补偿金为631万区块（大约1年），50年内，每年减少11.16%。针对预存金的补偿，可促使议会成员增加预存于单个节点的货币数，并减少决策中央集权化的动因。

- **Commons Budget:** Commons Budget是支付给已通过Congress Network的提案的存

有BOScoin的账户。为了编制充足的预算，第一次将发行3500万个数据区块（约5年半），每个区块50 Commons Coins。第一个5年半以后Commons Budget将通过交易手续费30%的Commons手续费来维持。

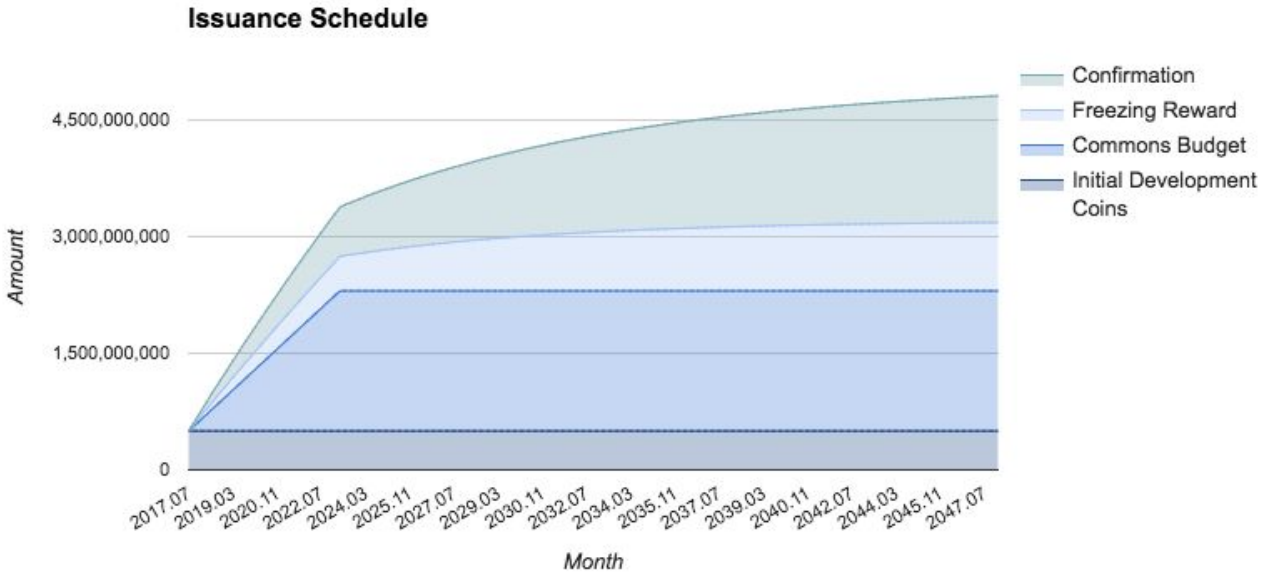

Fig 9. 货币发行计划

8. 结论

BOScoin小组以克服各类加密货币技术与运营方面存在的问题为目标。奖励制度及发行计划以遏制权利的中央集权化及创造货币价值为目标。 mFBA算法可以提高能量的效率，并实现快速的交易。议会系统是为了实现民主化、建设性决策流程而搭建的。Trust Contract将提供在数据区块链生成并运行协议的过程中，具有可决策性，可处理性的框架。BOScoin小组将运用通过数据区块链技术获取的安全性与完整性，实现上述目标。

Works Cited

Andrychowicz, Dziembowski, Malinowski and Mazurek, *Modeling Bitcoin Contracts by Timed Automata*, Lecture Notes in Computer Science Formal Modeling and Analysis of Timed Systems, 7-22, 2014, https://arxiv.org/pdf/1405.1861v2.pdf

David Mazieres, *Stellar Consensus Protocol*, https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Decentralized Prediction Market, https://www.augur.net/

Evan Duffield, Daniel Diaz, *Dash: A PrivacyCentric CryptoCurrency*, https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

Golem, https://golem.network

Hodges, Andrew*, Alan Turing: the enigma,* London: Burnett Books

Ian Grigg, *The Ricardian Contract*, First IEEE International Workshop on Electronic Contracting (WEC) 6th July 2004, http://iang.org/papers/ricardian_contract.html

Leading the Pack in Blockchain Banking: Trailblazers Set the Pace, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN&

N. Atzei, M. Bartoletti, T. Cimoli, *A survey of attacks on Ethereum smart contracts*, https://eprint.iacr.org/2016/1007.pdf

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

Simple Declarative Language, https://sdlang.org/

The DAO, https://slock.it/dao.html

Using Decentralized Governance: Proposals, Voting, and Budgets, https://dashpay.atlassian.net/wiki/display/DOC/Using+Decentralized+Governance%3A+Proposals%2C+Voting%2C+and+Budgets

OWL Web Ontology Language, https://www.w3.org/TR/owl-features/

OWL Web Ontology Language Reference, https://www.w3.org/TR/owl-ref

Vitalik Buterin, *Ethereum Whitepaper*, https://github.com/ethereum/wiki/wiki/White-Paper