
Roburst Network 白皮书

由 Roburst Network 团队为您呈现



2018

Roburst Network

版本 1.0b

声明	3
前言	Error! Bookmark not defined.
简介	Error! Bookmark not defined.
1. 为什么区块链、加密货币是机遇	8
2. Roburst Network 和 Roburst Coin.....	10
3. Roburst 交易机器人.....	12
4. 数字银行和未来支付	13
5. ICO 概述	16
6. 如果你没有关注下一部分，你应该阅读的内容	20
Roburst Network	21
1. Roburst 加密货币 (Roburst Coin).....	22
1.1. Roburst Coin	22
1.2. 安全	23
1.3. 交易	23
1.4. 区块	24
1.5. iDPOS	27
1.6. 网络奖励	30
1.7. 通货膨胀	31
1.8. 交易池	32
2. Roburst 主网络 (Roburst Network)	33
2.1. RoburstBridge™	33
2.2. Roburst 卡和无现金支付.....	35
2.3. Roburst 交易机器人	35
2.4. Roburst Network 团队	36
2.5. 路线图	40
ICO	42
1. Roburst 奖励代币 (ROC 奖励).....	42
2. 早鸟投资者	42
3. 预售阶段	43
4. ICO 阶段.....	44

5. 推荐	45
附录	46
参考	Error! Bookmark not defined.

声明

通过参加 Roburst Network 预售活动和/或 ICO（代币公开发售）阶段或使用本白皮书/ Roburst Network 网站（不包括第三方使用 Roburst Coin 作为综合支付网关的网站）中的任何信息，您须同意以下内容：

一般警告

通过使用 Roburst Network 提供的服务，作为 ICO（以下称为 - 预售和/或 ICO 或代币公开发售）的参与者或 Roburst Network 产品和/或服务的客户，您（用户）完全理解并同意以下内容声明：

1. 用户必须理解并承认 Roburst Coin 将在 Roburst Network 创世区块中产生。不会由任何第三方提供。
2. 用户必须明白，Roburst Network 对于超出 Roburst Network 控制范围之外的原因（包括但不限于预售和/或 ICO）参与预售和/或 ICO 阶段持续时间延长，交易延误和其他相关问题不承担任何责任。
3. 用户必须明白，Roburst Network 团队将专注于完成我们的路线图中列出的里程碑任务并实现。然而 Roburst Network 团队没有义务在预售和/或 ICO 阶段之后必须为用户的利益行事。
4. 用户必须明白，通过将现金和/或其他资产转移到 Roburst Network，用户可以作出关于存入现金和/或其他资产的最终决定，但无权退款。有两种情况我们会允许用户从 Roburst Network 提取现金和/或其他资产。
 - 未达到最低软顶，这意味着所有存入的现金和/或其他资产将被退回到您指定的钱包。
 - 在 ICO 阶段之前和之后，我们将允许用户从 Roburst Network 撤出用户资产。但是用户帐户必须经过验证才能提取价值超过 25,000 美元的资产。

用户必须明白，预售和/或 ICO 阶段的持续时间可能会根据 Roburst Network 在每个阶段提供的剩余代币而有所不同。预售和/或 ICO 阶段可能会比我们的计划更快结束。用户会收到一封电子邮件，通知 ICO 阶段已经结束。

用户应该知晓，用户帐户所做的任何可疑活动都可能导致帐户被永久禁止。如有必要，Roburst Network 将提供证据证明用户的账户存在可疑活动。用户必须在 7 天内索要证据。之后，Roburst Network 对用户账户证据遗失不承担任何责任。

税务警告

用户必须明白 Roburst Network 不作为用户的税务代理;用户和 Roburst Network 仅根据其所在国家和地区的适用法律承担其纳税义务。Roburst Network 不是税务代理,因此不应向任何第三方提供用户的财务信息。这些信息在任何情况下都不会被披露。

无担保

本白皮书中的所有信息均按“原样”提供,不提供任何担保。对于本网站或平台上的信息或对信息的任何使用,不做任何明示或暗示的任何类型的担保,包括对适用性或针对特定用途的适用性的暗示担保。Roburst Network 对本白皮书或此平台中的任何信息或内容的准确性或完整性不做任何声明,也不作任何类型的担保。

免责声明

Roburst Network 明确声明不承担任何偶然或间接损失的责任,并且不承担任何人因使用或误用本白皮书或 Roburst Network 网站上的信息或内容而遭受的任何损失或损害的责任或义务。Roburst Network 对由于使用,误用或依赖本白皮书或 Roburst Network 网站上的信息或内容而导致的任何损失或损害不承担任何责任。

在任何情况下,Roburst Network 均不对任何特殊的,间接的,附带的,后果性的,惩戒性的或惩罚性的损害(包括丢失或预期的收入或利润以及未能实现以及 Roburst Network 提供的服务相关的任何索赔)不论索赔是否基于担保、合同、侵权(包括疏忽或严格赔偿责任)或其他方面不承担责任。

自担风险

通过使用 ROC、Roburst Network 平台或 Roburst Network 网站的预售和/或 ICO 阶段(包括但不限于将资产转让给 Roburst Network),用户必须确认用户承诺并理解直接或间接的所有可能风险来自与用户参与预售和/或 ICO 阶段相关的活动和/或使用 Roburst 网络服务和产品。

不可抗力

用户理解 Roburst Network 对于任何违反本协议的行为不承担任何责任,包括由于 Roburst Network 无法控制的原因导致服务未能交付或延期交付,包括但不限于材料无法使用,罢工,劳动力下降停工,劳工短缺,停工,火灾,洪水,地震,风暴,干旱,恶劣天气,暴动,盗窃,事故,禁运,战争(不论是否宣布)或其他爆发敌对行为,内乱,政府行为,上帝行为,政府行为或法规,命令或禁令或其他原因,无论是否与上述相似或不相似(均为“不可抗力事件”)。

最后的警告

预售和/或 ICO 参与可以被视为高风险交易;通过预售和/或 ICO 购买金融资产或利用网站上提供的服务可能导致重大损失,甚至导致所有投入资金的全部损失。

在 Roburst Network 平台或网站上提供的信息不应被解释为投资建议。它并不构成 Roburst Network 向任何用户购买或出售代币或进行任何投资的要约或邀请。

用户保证用户是具有法定年龄的成年人,并符合用户所在司法管辖区的法律规定和适用法律。

通过参与预售和/或 ICO 用户确认用户已阅读,理解并同意遵守上述所有限制。

前言

互联网的发展开启了数字生活的时代，诞生了许多新术语。我们可能听说过电子邮件，也就是 Email，电子商务或 e-commerce。当然，您可能听说过一个术语，它的发展会让您感到惊讶：加密货币。早在 2000 年，电子货币（数字货币）就成了一种趋势，几乎每个公司当时都希望拥有自己的货币。但出现了一个问题，越来越多的货币被黑客攻击，因为它们为中心化的，不具备最高的安全性。2008 年，比特币通过成为第一个分布式的数字货币来重塑“数字货币游戏”，直到现在，它一直在增长。在过去的 5 年里，比特币的增长率已经超过了 10 万倍，这是有史以来第一次虚拟货币可以达到近一万亿美元的市值。借助 Roburst Network 和 Roburst Coin，我们希望能够更快更好的创造像比特币一样同样的奇迹。

简介

关于加密货币和 *Roburst Network* 的简要总结

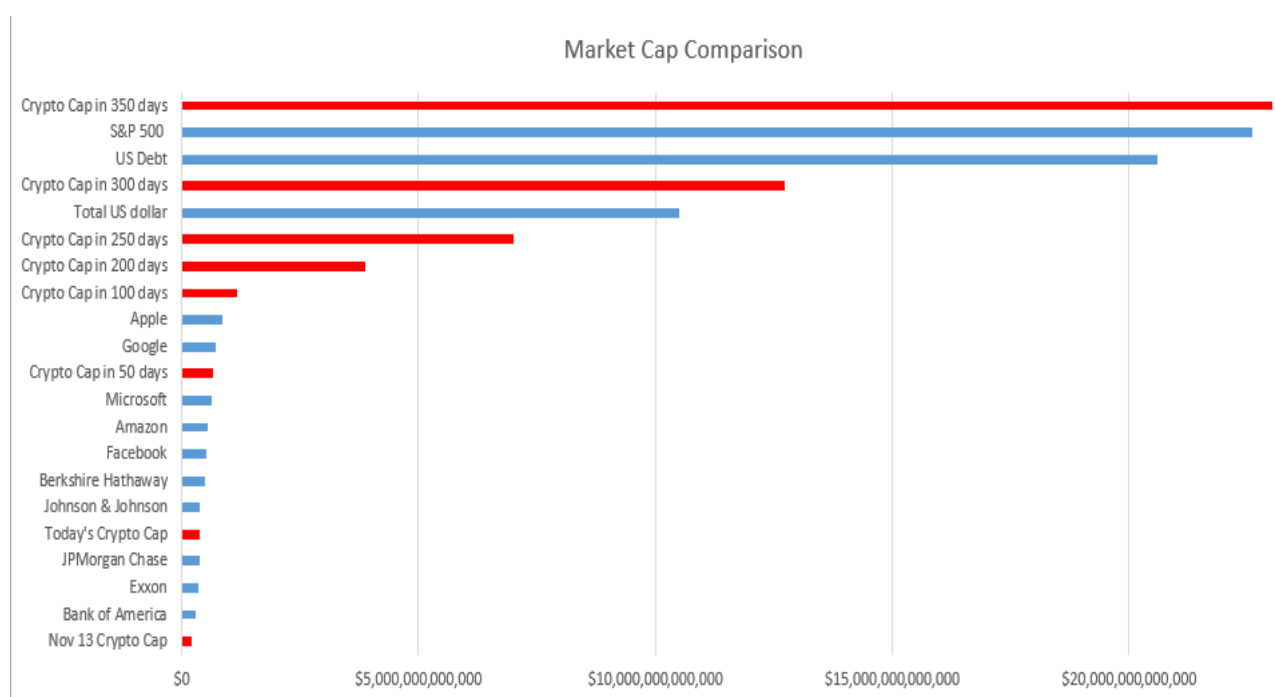
1. 为什么区块链、加密货币是机遇

现在几乎每个人都很熟悉“区块链”和“加密货币”这个术语，对于那些以前没有听说过这些术语的人来说，区块链总的来说是一种技术，它可以让财产远离中心化。与发布在互联网上的传统货币不同，使用区块链的货币很难被黑客攻击，没有人可以从表面上控制货币。有关区块链工作原理的技术细节，请参阅（1）。

加密货币是采用区块链技术的所有货币的简称。我们可能会将比特币作为流行和成功的杰出范例。如今的比特币不仅是一种付款方式，而且还是一种价值数千美元的虚拟财产。使用区块链技术使得比特币交易透明，但仍然匿名。与传统的国际间转账和支付方式相比，它无视距离远近。但是由于价格的波动，我们可能会觉得很难替代传统的支付方式。我们没有办法稳定地保持价格，如果价格稳定，没有人会投资这些货币。这就是为什么我们正在制定新的支付方案，既是传统的付款方式，也是人人都想拥有的一种财产。

一年来，人们试图基于几乎所有东西都想出新型的加密货币。例如，早期代币报价也被称为 ICO，并不是单指货币本身，也是创业公司募集资金的一种方式。

为了便于查看，下面的图表将显示加密货币之间市场资本化以及传统货币市场资本化之间的比较。



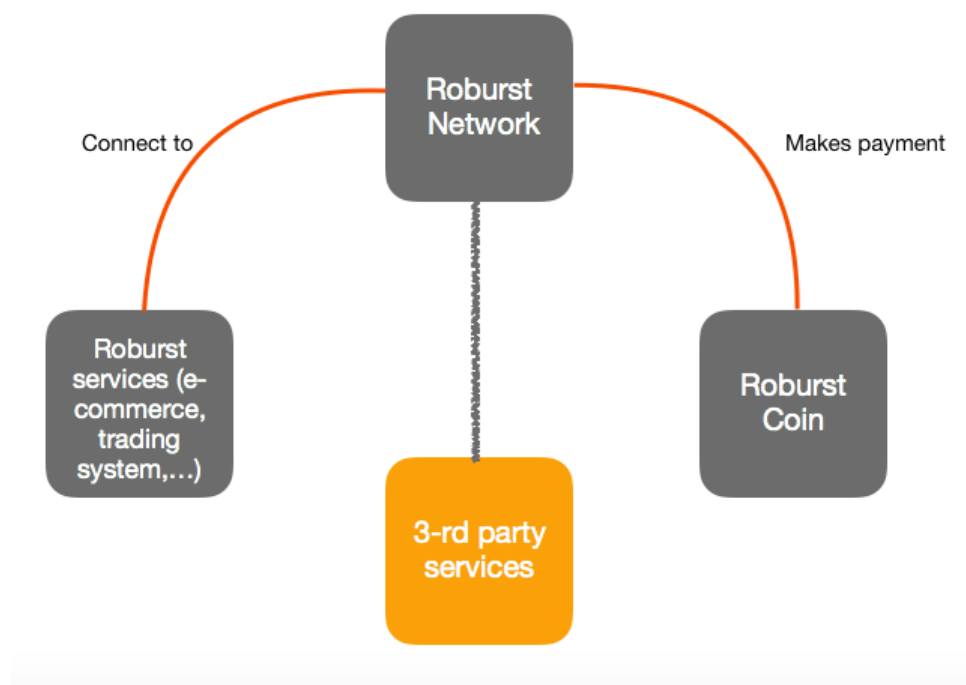
图表 I. 1. 1: 各种加密货币和传统货币的市值

与其他货币相比，该图表显示加密货币的市值大幅增加。问题是，我们参与这个游戏太迟了吗？答案是不。在技术世界中，一切变化都会如此之快，以至于当你没有接触新技术时，世界就会立即将你抛诸脑后。这就是为什么当你介绍 Roburst Network 和 Roburst Coin 时，我们相信这是你不想错过的有前景的投资。

2. Roburst Network 和 Roburst Coin

总之，Roburst Coin 就像传统的加密货币一样，您可以随时随地转账或接收 Roburst Coin。Roburst Coin 作为 Roburst Network 一系列服务所使用的代币。在我们介绍 Roburst Coin 和 Roburst Network 时，第一个服务是 Roburst 交易机器人，它可以帮助您监控，预测加密货币市场并且自己赚钱，这是一个数字钱包，可帮助用户更容易和更快的交易数字货币。我们的愿景是将网络扩展到其他领域，如医疗、教育、电子商务等。网络中的所有交易将由 Roburst Coin 提供支持，并且免费，这意味着当您使用我们网络的服务时，不收取任何交易费用。

第三方开发者还可以使用 Roburst Network 提供的 API 将 Roburst 支付网关应用到他们的应用程序和网站中。Roburst 支付网关将在本白皮书的后面进行



介绍。现在，我们可以快速了解简单视图下的系统如何工作。

Figure I.2.1: 系统中 Roburst Network 如何工作的简单视图

3. Roburst 交易机器人

多年来，我们在机器学习和深度学习方面取得了显着进步。 我们将它用于我们的项目 Roburst Trading Bot (RTB) 中。 RTB 由 Google 运营的开源深度学习技术 TensorFlow 提供支持。 目前，RTB 能够预测和交易多种加密货币，包括最流行的加密货币：比特币 (BTC) 和以太坊 (ETH)。 RTB 还可以预测货币的下跌趋势，因此它可以为您提供多种情况的策略，包括最佳策略和最差策略。 或者您可以让 RTB 选择最优化的方案，并且您所承担的风险将会降低近 50%。

以下是您在 2017 年 1 月 1 日至 2017 年 8 月 16 日期间购买这些加密货币的回报价值表，大概为 9 个月。 可以达到的最高回报价值是 31,620%，表明如果您购买 1 美元元的 NEO，您将获得 31,620 美元的回报。

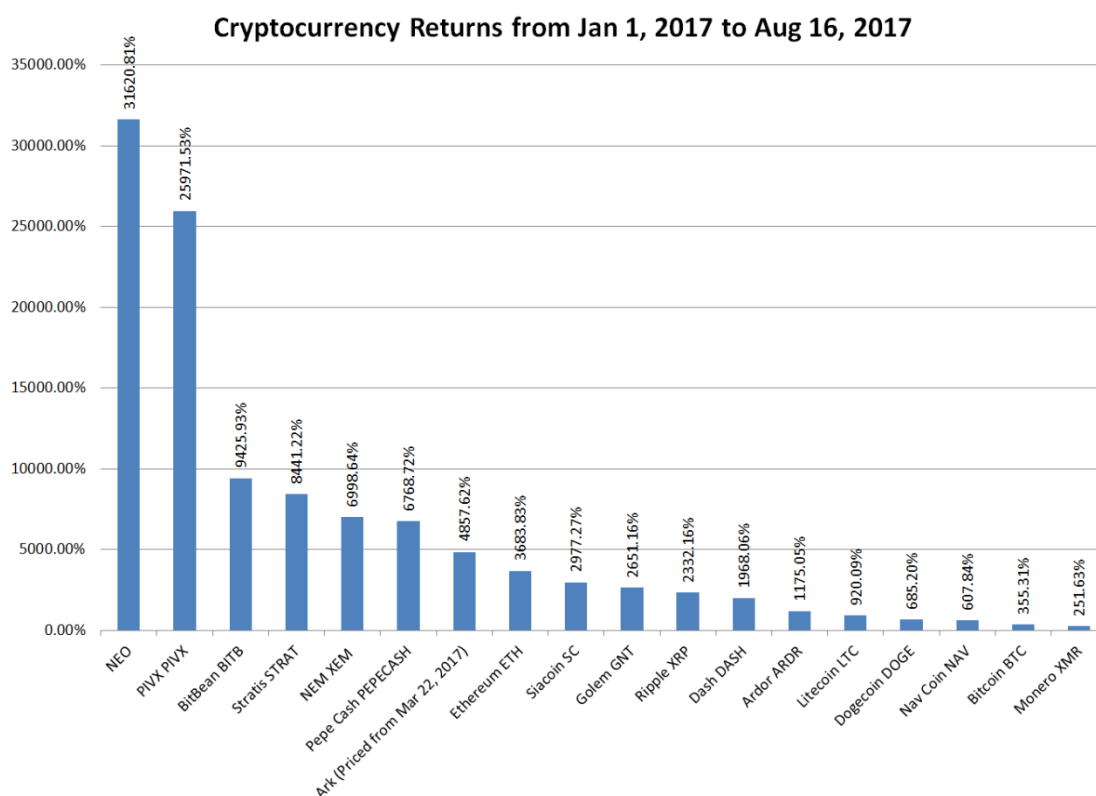


Figure I.3.1: 2017 年 1 月 1 日至 2017 年 8 月 16 日加密货币投资回报率

(分类, 来源 CoinMarketCap)

4. 数字银行和未来支付

正如我们在过去几年看到的一样，无现金支付已成为每个人生活的一部分。互联网人数的激增迫使企业开发新的网上购物方式。其中之一是数字银行的出现，现金变得毫无用处。没有人希望拿着一袋满满的钱成为抢劫目标。他们手中只有一张卡，他们可以轻松支付几乎所有的东西。下图 I.4.1 显示，从 2010 年到 2014 年，超过 4 年的时间里，人们使用无现金方式支付的金额（根据 RBR 的一项研究），令人难以置信的从 311 亿美元增长到 4170 亿美元。

随着许多新技术的应用，无现金支付变得越来越流行。例如，Samsung Pay 和 Apple Pay 不需要卡，只需要一部手机即可付款。使用近场通信（NFC）技术，付款变得毫无障碍。预计这种支付方式的年复合增长率将达到 80%，到 2020 年移动支付量预计达到 4 万亿美元。2017 年，每月至少使用一次非现金支付方式的全球用户总数已达 1.5 亿。

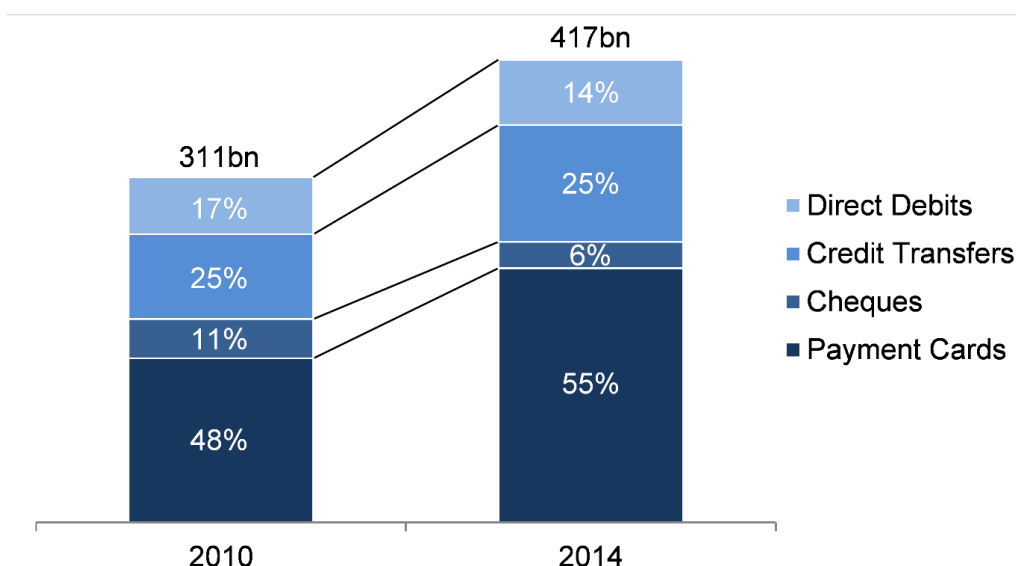


图 I. 4. 1: 2010 年至 2014 年全球无现金支付方式增长量

Number of Apple Pay, Samsung Pay, & Android Pay Contactless Users 2017

	2015	2016	2017
Apple Pay	15	45	86
Samsung Pay	3	18	34
Android Pay	2	12	24

Figure I. 4. 2: 使用近场通信付款用户数量（以百万为单位，来源 NFCWorld）

Roburst Network 通过发行第一张智能加密货币卡（RSC），帮助您在任何 Roburst 自动取款机（RATM）上以小额费用提取现金或免费使用 Roburst 销售点（RPOS）机器直接付款。所有这些条款将在后面的部分进行描述。

5. ICO 概述

为了使系统正常运行并使交易过程顺利，我们决定为早期投资者提供合理价格的加密货币。该流程将于 2018 年第一季度开始，Roburst Network 将发行 420,000,000 ROC，然后将按照我们的计划以 1 个 ROC= 0.00001 比特币（BTC）的初始价格进行发售。

开始时间	10:00 AM PST, 2 月 24 日, 2018
结束时间	08:00 PM PST, 4 月 24 日, 2018
期限	60 天
代币出售量 ⁽¹⁾	315,000,000 ROC
初始代币价格 ⁽²⁾	0.00001 BTC
代币技术限制数量 ⁽³⁾	Unlimited
硬顶 ⁽⁴⁾	\$5000 万 USD
软顶 ⁽⁵⁾	\$1000 万 USD
代币发放日期 ⁽⁶⁾	5 月 1 日, 2018(最差情况) 4 月 25 日, 2018(最好情况)
最小购买量	1 ROC

购买限制 (7)

100,000 ROC/账户/天

要了解 ICO 阶段的概况，请参阅下表。

在 ICO 阶段的前 30 天（2018 年 2 月 24 日 - 2018 年 3 月 25 日）申请预售奖金）

津贴	+50% 代币	+38%代币	+27%代币	+20%代币
最小购买	1,200,000 ROC	500,000 ROC	200,000 ROC	50,000 ROC

如果您的购买金额低于 50,000 ROC，您将获得相当于购买额的 10% 的早鸟奖励。

从 1 ROC 起的投资，我们会给这些账户额外推荐奖金 (8)。有关我们的推荐系统如何工作的详细信息，请参阅第 III 部分 - ICO。

- (1)：出售代币的数量包括赏金猎人代币，奖金代币，预售代币。
- (2)：比特币的价格可能会有所不同，但初始价格不会随 BTC 价值变化。请注意，售价可能会随初始价格的最低价格而变化。
- (3)：这是 Roburst Network 可以提供给市场的最大数量。
- (4)：当销售达到硬顶时，ICO 将停止，所有未售出和未分配的硬币将被销毁。
- (5)：如果 ICO 未达到最低限额，则所有资金都将退还给您的钱包。
- (6)：如果 ICO 在结束日期之前达到硬顶，我们将通过电子邮件通知所有投资者最新的代币分发日期。
- (7)：购买限额是系统在一天内单个账户可以购买代币的数量，这个数字不适用于 ICO 预售阶段。
- (8)：每个从您的推荐链接注册的账户购买 1 个 ROC 代币，您的钱包将计入并将增加 0.1 ROC，更多政策请参阅推荐部分
- (9)：在 ICO 阶段，所有奖金代币都不能提取或转移到其他账户。结束日期后，奖励代币将自动转换为普通代币。

(10): 激活的推荐账户是指一个账户，在推荐链接下注册，并在 ICO 阶段购买了至少 0.1 个 ROC 代币的账户。

更多信息请查阅第三部分 III - ICO.

6. 如果你没有关注下一部分，你应该阅读的内容

如果您要阅读下一部分，您可以在最后阅读本章，因为这是来自 Roburst Network 首席执行官 Samantha Wilson 的感谢信。

亲爱的投资者

首先，我想对你们所有人阅读本白皮书表示真诚的感谢。我认为你已经阅读了第 1 部分，可能会对这本白皮书感到无聊。由于这只是我们计划的第一步，所以我们可能会在计划中犯错误，或者本文中的术语要么太模糊，要么您难以理解，要么太简单，您几乎在阅读时就睡着了。我们内心致以真诚的歉意。

我必须说，我不是一个能够比我的团队中的任何人更好地向大家传达这个信息的人，但深深地在我的心中，我真的希望你继续阅读这篇文章，无论你是否想投资，因为当我们越来越接近未来支付时，你不应该忽略它，加密货币和无现金支付是其中最有力的因素。在接下来的几个月甚至几年时间里，当互联网上的每个人的隐私成为最大的问题时，你会看到互联网上越来越多的支持性行动。对于一些人来说，这可能听起来有点奇怪，但它有可能成为人们未来可以做出的最大投资。

最后，如果您认为这是您自比特币繁荣以来的第二次机会，但您仍然害怕投资 Roburst Network 和 Roburst Coin，请通过我的电子邮件联系我：samantha@roburst.network。我会尽快回复您关于 Roburst Network 的问题或疑虑。

Regards,

Roburst Network 首席执行官

Samantha Wilson

II.

Roburst Network

Roburst Network 是什么，怎么样和为什么

1. Roburst 加密货币 (Roburst Coin)

Roburst Coin 是 Roburst 团队开发的一种在互联网以及 Roburst Network 中交易和支付的安全加密货币。与比特币不同，Roburst Coin 使用 BitShares 采用的代表权益证明 (DPoS) 共识算法。对 Roburst 对 DPoS 算法进行了更多改进，主要集中在投票系统、隐私和交易速度上。我们把我们的一致性算法称为智能代表权益证明 (简称 iDPoS)。

iDPoS 主要集中在解决原始 DPoS 方法尚未解决的问题，例如权力下放较少，或者大股东掌握投票权。我们将在后面的章节中详细讨论 iDPoS。

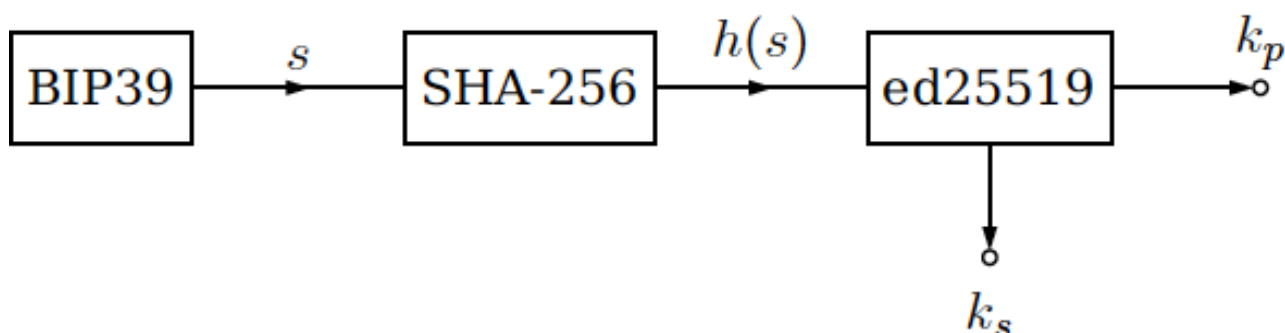
1.1. Roburst Coin

Roburst Network 的基本代币叫做 Roburst Coin，简称 ROC。它可分割为 10^6 次方个子单位。

1.2. 安全

Roburst Coin 就像市场上其他加密货币一样，使用加密哈希算法，但我们不使用比特币和其他许多其他加密货币中的 ECDSA，而是使用更快更安全的 EdDSA。

1.2.1. 密钥对



一个密钥对意思是两个密钥，一个是公开的一个是秘密的。公钥是从私钥导出的，不能转换为私钥。私钥是只有拥有者才能知道的信息。生成密钥对的过程如下所述：

图 1.2.1.1: 生成新密钥对的过程

当用户创建密钥对时，会生成一个 BIP39 助记词，然后将其散列为 256 位字符串。然后这个散列被用作为 ed25519 种子来生成私钥 k_s 然后导出公钥 k_p 。

使用密钥对，用户可以使用私钥对交易进行签名并将其广播到网络。节点然后使用公钥来验证签名的有效性。

1.2.2. 多重签名

对于需要高级安全性的用户，Roburst Coin 提供多重签名帐户，这意味着用户必须有多個签名才能提交交易。想要使用此功能的用户必须提交一组 $n k_s$ 并指定要确认交易最小有效数量的 k_s ，任何源自多重签名账户的交易必须在交易处理之前符合最小签名验证。

1.2.3. 钱包地址

从公钥中生成地址。公钥将被散列成 256 位的字符串，然后取出散列的前 8 个字节。钱包地址是那些 8 字节的数字，Roburst 地址用字母 R 开头表示。

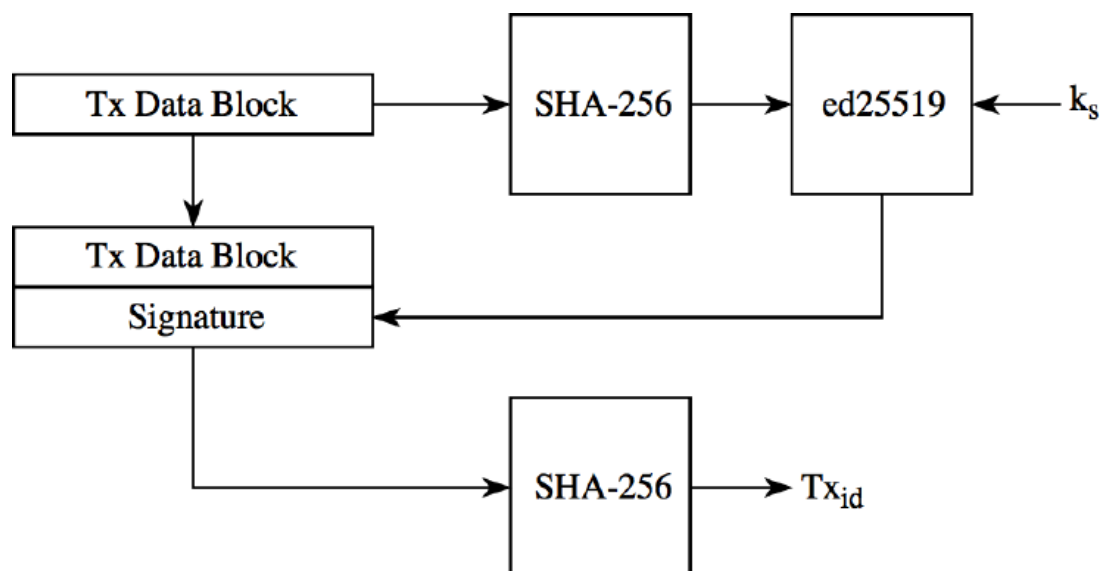
1.3. 交易

Roburst Coin 内的交易分为 5 种类型，即在下表中：

类型 0	将资金转到 Roburst 钱包地址
类型 1	注册第二密钥
类型 2	注册一个授权
类型 3	为代表提交投票
类型 4	注册多重签名

图 1.3.1: Roburst Network 交易类型

所有类型的交易，无论何种类型，都需要在网络处理之前进行签名。签署交



易的过程如下图所示：

Figure 1.3.2: 单一签名交易流程图

表示交易的数据区块必须与标准化信息一起生成。根据交易类型的不同，其他信息将有所不同，但以下字段是每笔交易的必备信息：

- 标记交易类型的 8 位整数
- 标记创建交易时间的 32 位时间戳
- 交易发行人的 256 位公钥
- 表示正在传输的 ROC 数量的 64 位整数

1.4. 区块

区块由区块头部和交易确认列表组成。授权是指分配了一个插槽并且正在运行节点的代理生成下一个区块，并确认来自矿池的多达 25 个交易。这些交易将被添加到该区块的有效负载中，然后在区块中签名。

0	16	32	48	64
Version		Timestamp		
Previous Block ID				
Number of transactions		Length of payload		
Amount of ROC transferred				
Amount of fee				
Reward of the delegate				
Payload hash				
Delegate's public key				

我们可以如下图所示说明区块头部：

图 1.4.1：区块头部说明

签署区块头部的过程与签署交易相似。区块头部将使用 SHA-256 算法并使用委托的密钥进行签名。之后区块 id 将使用与交易相同的逻辑生成。下图描述了对区块头部进行签名的过程：

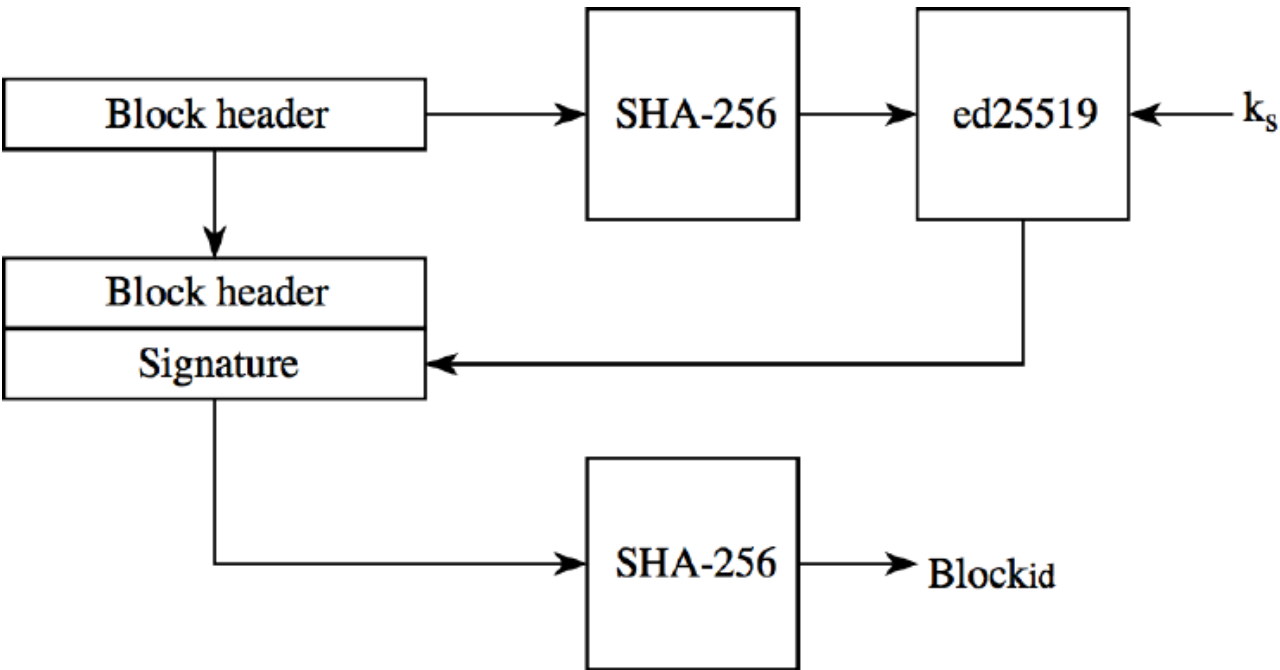


图 1.4.2：区块头部签名过程

如果每种交易类型的体积不超过有效负载允许的最大体积，则有效负载可以保持的最大未确认交易数为 25。 下表显示了每种交易的最大尺寸：

交易类型	最大体积 (bytes)
类型 0	220
类型 1	149
类型 2	201
类型 3	2326
类型 4	1223

图 1.4.3：每种交易类型最大体积

每隔 10 秒使用 iDPoS 共识机制生成一个区块。 代表过程将选择一个帐户，委托生成下一个区块，称为授权。 同等的 51％需要维持广泛的共识。 生成过程将在广泛共识建立时执行。

1.5. iDPOS

智能代表权益证明（iDPOS）是来自 Bitshares 原始 DPOS 的改进方案。iDPOS 旨在解决当前 DPOS 共识中存在的问题，并改进网络中的安全性和处理速度。代表生成网络中的所有区块，需要通过股东操作的竞争性选举系统进行选择。Roburst Coin 网络中有 101 名活跃的锻造代表。一个股东可以投票给多达 101 名代表。投票权重取决于股东拥有的 Roburst Coin 的数量。如果股东希望为代表投票（交易类型 3），则必须进行代表交易。

1.5.1. 特征

1. 股东达到控制

每个股东都可以为签署该区块的代表投票。任何人获得 1% 或更多的选票就可以加入董事会。那些将成为董事会将对区块签名。如果有人错过了，股东将会从他们身上撤销投票。最终这些代表将被清退出董事会，其他人将加入填补空缺的地方。董事会成员将获得少量代币报酬，以确保网络的正常运行。iDPOS 还为每个董事会成员设置了隐藏分数，这意味着如果他们的分数低于特定数字，他们将自动从董事会中删除。这个分数是根据正常运行时间，代表的可信度和多种其他因素来评分的。

随着股东的控制，网络进行分散化。由于投票可能存在缺陷，当涉及到公司的共同所有权时，这是唯一可行的方法。

2. 环保

Roburst 网络中的采矿过程与旧的方式即工作证明相比较几乎不需要耗电。随着越来越多的人使用 PoW 共识挖掘加密货币，能量被大量浪费。当没有电力驱动时，iDPOS 仍然是可以运作的。

3. 混合采矿是委托工作证明吗？

这个问题已经被多次提及。当谈到挖掘比特币时，用户必须选择一个矿池，每个矿池可以拥有 10% 或更多的算力。这个过程就像用户对其代表投票一样。随着矿池数量的减少，只有 5 个主要采矿池控制整个网络，可能会将比特币变成一个中心化的加密货币。告诉用户不断切换矿池，这总是令人不愉快的。随着一个矿池停机，整个网络变得缓慢，必须等待矿恢复到原来的速度。这从历史经验来看会比较危险。

4. 不利于攻击

如果一个代表决定不生产一个区块，这个代表有可能被排除在董事会之外，将来也不会有任何收益。委托人无法签署无效区块，因为该区块需要其他委托人确认。

1.5.2. 可扩展性

假设确认成本和每笔交易费用都是固定的，可以进行权力下放的数量是有限的。如果确认成本等于费用，那么系统是中心化的，并且只能服务一个确认者。那么如果费用是验证费用的 100 倍，则网络可以服务多达 100 个验证者。

像 Nxt 这样的原始股权证明共识系统就出现了问题。如果系统允许每个人都成为验证者，那么收费过高。换句话说，如果人们没有 1% 或更多的股份，那么除非收费增加，否则他们不能成为验证者。如果该链假定 100 个验证者过于集中，则他们必须将该数量提升至 1,000 个验证者，这将比 iDPOS 高 10 倍。随着验证规模的扩大，例如 100 亿美元，那些拥有 100 万美元代币的企业就可以加入董事会。如果他们希望最低的股份低至 1000 美元，那么他们的收费将比 iDPOS 高 10,000 倍。

总之，任何运行传统权益证明系统，如果不改变系统的运作方式，很快就会集中。在规模上，这些成本将不支持集中式授权系统的运作。

1.5.3. 投票算法

该系统的设计目的只是提高投票率，这意味着系统中不存在 anti-vote 的情况，这种投票效率更高，复杂性更低。系统中的人员向其他代表投票，在维护间隔期间，投票将被计算并且结果生效。iDPOS 还提倡代理投票，这表示处理某人投票权给其他人的过程。这个过程可以恢复。代理投票有助于减少忽视投票的情况，并帮助积极的股东更快速地应对业务和安全问题。这样那些不守规矩的代表就会被更快地解雇。代理投票可能引发一个问题，即它太集中。这个过程就像是在比特币矿池中进行挖矿一样，但是每个股东都可以参与并且只有投票权，这个过程也是可以恢复的。如果股东不喜欢系统运行的方式，他们可以停止给予投票权。

1.5.4. 代表轮

代表轮的长度恰好为 N 个区块（ N 当前为 101，总锻造活动委托人）。在每轮开始时，每个代表将被分配到一个插槽，该插槽将表示其在区块生成过程中的位置。在一轮中，每个代表将锻造一个区块。如果代表未能锻造其区块，则另一个代表将锻造此区块，而失败的代表将从股东那里得到反对票。如果完成锻造区块，与代表相关联的节点将对其进行签名并广播到网络。一旦完成，下一个代表将在他们预先分配的位置进行锻造。

1.6. 网络奖励

Roburst Network 中的一个节点可能会获得许多激励措施来保持其运行。第一个就是区块生成奖励，还有活跃代表为确保网络安全进行锻造的其他奖励。

Roburst Coin 网络中具有固定的生成区块奖励，网络中的每一个活跃代表将获得区块奖励。随着越来越多的区块产生，奖励将会减少。这是维持代表在网络中保持活跃状态的激励。在网络中区块奖励将线性下降，每轮从 5 个 ROC 起，初始奖励区块后每 300 万个区块开始下降。

除了积分奖励之外，积极的代表还会收取每轮费用，作为所有董事会成员的奖励。本轮交易结束后，所有交易费用将分摊给所有活跃的代表。可能会给参与者一笔超过区块生成奖励的费用。如果董事会成员没有做好这项工作，那么接受这项工作的成员将会得到两倍的费用支付。但是这个成员不会被指定这项工作除非是原代表未完成此项工作。 N 轮（ N 为董事会成员的数量）后，该成员将有资格再次从事其他工作。下表是网络中的交易费用。

类型	费用
类型 0	0.1 ROC
类型 1	1 ROC
类型 2	20 ROC
类型 3	1 ROC
类型 4	1 ROC/sign

图 1.6.1: Roburst Network 不同类型交易费用

请注意，Roburst Network 中类型 0 的交易费用将被赞助，并且不会在 Tx 帐户中收取费用，但董事会成员仍然可以收到类型 0 的交易费用。

1.7. 通货膨胀

随着锻造奖励的推出，通货膨胀率也成为网络中的一个问题，除了交易费用奖励之外，代表们还会得到一定数量的代表轮，称为锻造奖励。为了确保通货膨胀率保持在一个较低的水平，锻造奖励将每隔 300 万块减少一次，大约每 1 年减少 1 次。经过 4 年的锻造后，锻造奖励将在 1 ROC 停止。通胀率预期如下图所示：

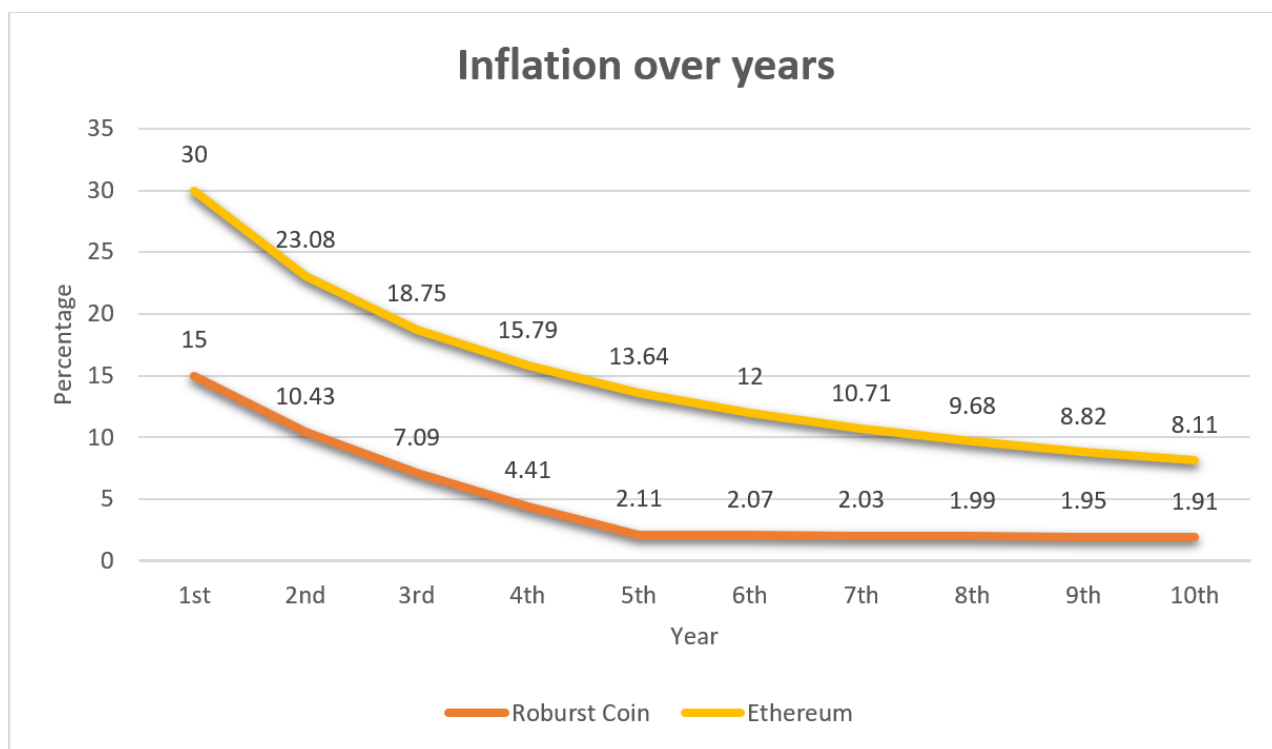


图 1.7.1:与 Ethereum 相比多年后的通货膨胀率

1.8. 交易池

随着网络的增长，25 个交易的区块容量可能无法同时处理大量交易。这就是为什么我们引入 Roburst 交易池的原因，它将保留未确认的交易溢出到下一个区块。该池将作为待签名交易的房子。这样具有未完成多重签名的交易可以等待足够的签名然后进行处理，并且不会影响区块的生成过程。为了保持交易池的整洁，所有待处理的交易都以特定的时间存在交易池中，在这种情况下，我们将其设置为 3 小时或 10800 秒。这意味着如果挂起的交易无法在 1080 个区块内处理，它将被标记为失败的交易并被移除。

交易池的其他作用是它将作为广播交易的机制。节点准备获取交易池中未决的 25 个交易并对该区块执行验证。然后，该区块将广播到网络中的其他节点。

2. Roburst 主网络(Roburst Network)

Roburst 主网络 或 Roburst Network 采用 Roburst Coin 作为货币的服务之间的链接。Roburst Network 提供了许多实用程序，不仅可以帮助用户从中受益，而且开发人员还可以更轻松地将 Roburst Coin 集成到他们的应用程序中。

2.1. RoburstBridge™

由于 Roburst Coin 不支持直接的侧链或 DApp 数据库，所以开发 RoburstBridge™用于所有区块链能够通过 Roburst 网络接收和发送任何信息或触发功能。

RoburstBridge™将在区块链之间架起一座桥梁，帮助 Roburst Network 与其他区块链进行沟通。例如，创建贷款服务，Roburst Network 的人员可以要求申请小额贷款并将其通知给其他区块链，例如以太坊网络，并等待其他人与我们网络中的人员联系。这种方法由一个编码监听器处理，最初由 ARK 引入，由 Roburst Network 进行改进。

任何现有的区块链都可以通过 Roburst Network 提供的几个简单步骤将此方法应用到他们的网络中。 RoburstBridge™的工作流程可以通过下图来说明：

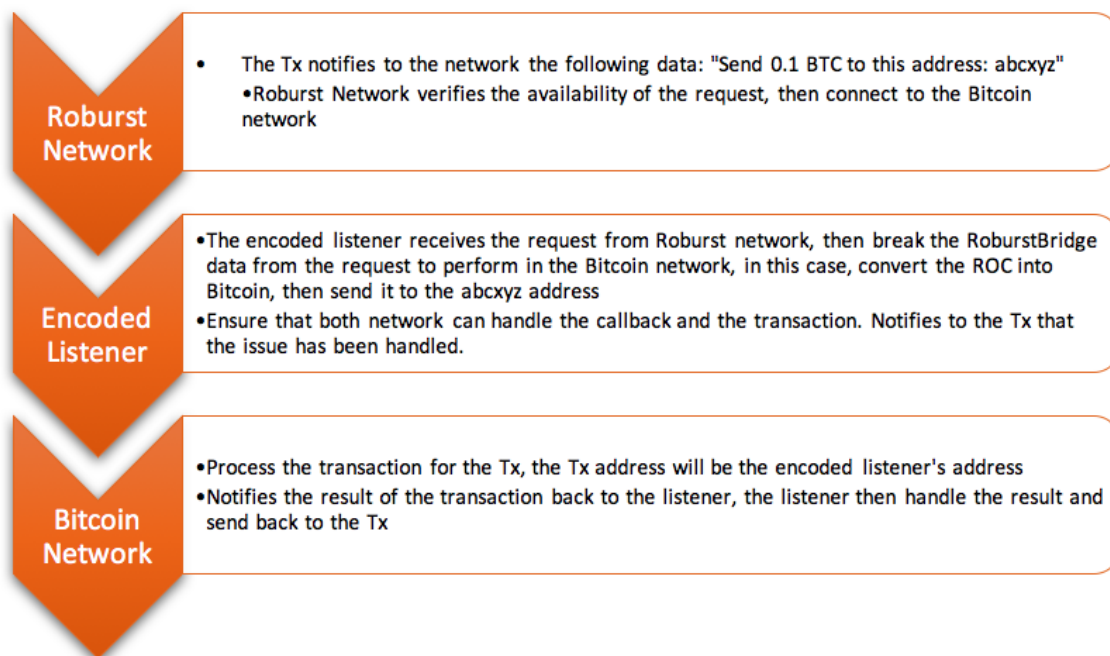


图 2.1.1: RoburstBridge™在特定情况下的工作流程

所有使用 RoburstBridge™进行的交易均根据开发人员设置的类型进行标记。例如，如果您想使用 Roburst Coin 将 1 BTC 发送到其他账户，您必须支付 0 类费用（将 ROC 转移到其他账户），并且将收取 BTC 和 ROC 之间的转换费用。使用 Roburst Trading Bot 不会收取您类型 0 的费用，因为它是 Roburst Main Network 服务之一，并且由网络本身提供赞助。

RoburstBridge 是我们下一个系统的核心，加密货币之间的交易变得更容易，费用更低。开发人员可以构建在 RoburstBridge 上运行的应用程序，发布他们自己的加密货币，这些货币可以轻松地与以太坊智能合约等主要网络进行交互，而且效率更高，仅需几乎零能耗来运行整个系统。有关 RoburstBridge 的更多的开发进程，请参阅路线图。

2.2. Roburst 卡和无现金支付

任何使用 Roburst 代币移动应用程序的人都可以创建特定的卡片在现实世界中进行付款。这是一张可在任何支持 NFC 销售网点进行支付的虚拟卡。该机制使用 RoburstBridge™通过 Paypal 或类似服务将 ROC 转换为当地货币。如果商店支持 ROC 作为他们的付款，则客户只需扫描 QR 码即可付款，并且不会收取任何费用。

2.3. Roburst 交易机器人

它是 Roburst Network 提供的许多服务之一。RTB 为那些工作繁忙并想要被动收入的人提供自动交易服务。通过深入学习，RTB 提供了一个安全的选择，在没有交易知识的情况下投资到加密货币市场。RTB 提供两种模式，全自动交易或手动交易。通过全自动交易，我们将其作为出借系统，但有很多选项供您选择，包括每天深入观察。你可以看到你有多少利润和你目前的风险衡量百分比。使用手动模式，您可以在咨询系统的情况下独立使用。机器人每小时将根据新闻、社交网络、之前的预测以及加密货币的价值变化，为未来 24 小时价格提供新的预测。我们支持通过 Telegram 和 Whatsapp 发送预测，以便您始终获得每小时的更新，而无需查看我们的网站。请注意，所有的交易都将在 Roburst 交易网站进行，我们的交易机器人不支持其他交易网站。此功能需要钱包中具有固定数量的 Roburst 代币，如果您的 ROC 低于特定数量，则此功能将被禁用。奖励代币不计算在此服务中。



Figure 2.3.1: Roburst Trading Bot forecasts Ethereum in next 24 hour

2.4. Roburst Network 团队

我们很自豪能够将自己打造成一支可以挑战一切的团队，冲破我们在前往最终道路中遇到的任何障碍，如您所见。



Samantha Wilson

CEO，联合创始人

经济学博士，加利福尼亚大学

Samantha 是一个非常有抱负的人，在金融和经济领域拥有非常丰富的知识。她对加密货币和区块链技术很感兴趣，她希望向公众推广这些技术。



Daniel Lee

技术总监，联合创始人

麻省理工学院计算机设计与优化硕士

Daniel 是我们见过的最杰出的人之一。他在这个领域努力学习更多关于加密货币世界的相关知识。他对当前 Roburst 协议的研究有着惊人的成果。



Justin Wilkerson

运营总监

芝加哥大学工商管理学士学位

Justin 在运营大型战略营销计划方面有着非凡的才华。感谢他，我们的计划比以往任何时候都更加成功。



Ronald Raji

财务总监

明尼苏达大学金融硕士学位

罗纳德作为金融分析师，有在 F.N.B 工作的经历。他在加密货币方面的知识与他的金融经验相结合令人惊讶，这一事实显然是非常了不起的。

“…没有什么能够阻止非现金支付将成为下一代支付方式…”

– Samantha Wilson

顾问



David Jones

MBA, EAZL 联合创始人
加密货币 Youtuber 始人



Michael Suppo



Marshall Hand

区块链 & 加密货币分析师 & 作家 - 区块链倡导者



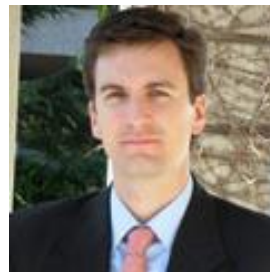
Samy Mkacher

区块链顾问



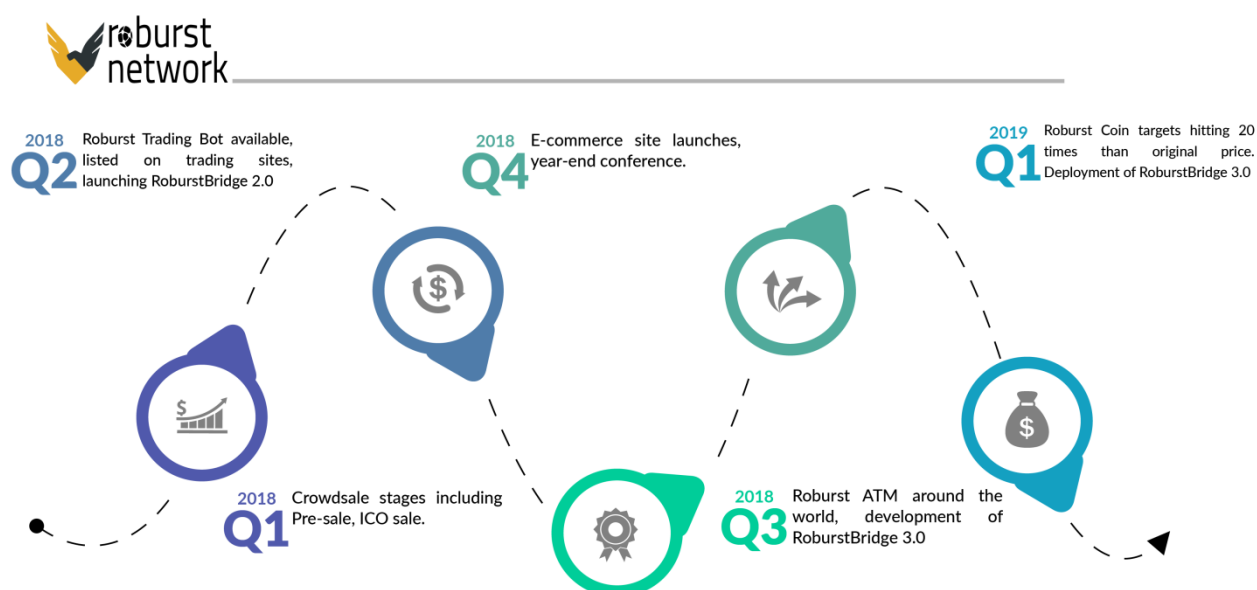
Arvind Narayanan

普林斯顿计算机科学助理教授。



Marc Badia

IESE 学校会计和控制助理教授



2.5. 路线图

这是 Roburst Network 计划的紧凑路线图。这是 Roburst Network 的 1 年计划，可以根据即将到来的销售情况进行更改。下图是我们的详细计划。请注意，日期可能会更改。

预售阶段开始

2018 年 2 月 24 日

售前阶段已开放。要加入预售，投资者需要完成 Roburst Network 白名单注册。

预售结束，ICO 阶段开始

2018 年 3 月 25 日

预售活动总结，进入下一阶段：ICO 阶段。

ICO 阶段结束

2018 年 4 月 24 日

ICO 阶段结束。总结所有阶段已售出和未售出代币。

代币分发日期

2018 年 5 月 1 日

主网络启动以及将代币分配给投资者。

5 月 5 日, 2018

Roburst Coin 在多个交易网站（至少 5 个网站，包括内部交易网站：Roburst Trading Bot）上市。

RoburstBridge 2.0 部署

2018 年 6 月 15 日

首先部署 RoburstBridge 2.0，允许创建侧链，传输交叉链，提高安全性、速度、稳定性等等。

洛杉矶安装第一台 ATM

2018 年 6 月 20 日

在 RoburstBridge 2.0 的帮助下，第一台 Roburst Coin ATM 将在加州洛杉矶上市。

RoburstBridge 3.0 的开发

2018 年 7 月 4 日

开始下一版 RoburstBridge 3.0 的开发，包括实施闪电网络。

全球部署 Roburst 代币 ATM

2018 年 9 月 5 日

我们的目标是在全球部署超过 300 台 ATM 机，首先在全球主要城市部署。

允许创建公共侧链

2018 年 10 月 1 日

现在，每个人都可以基于 Roburst Network 创建自己的加密货币。

Roburst 电子商务网站启动

2018 年 11 月 11 日

Roburst Network 的电子商务网站只接受 Roburst Coin。

全球 Roburst Network 大事件

2018 年 12 月 12 日

由 Roburst Network 举办的第一次世界性活动，总结了与 Roburst Network 合作的一年。.



III.

ICO

初始代币出售(ICO) 以加密货币为中心公开发售的一种募集资金的手段
(Wikipedia)

1. Roburst 奖励代币 (ROC 奖励)

Roburst 奖励代币由 Roburst Network 发行。Roburst 奖励代币等同于 Roburst Coin 但是有以下规则限制：

1. 在预售和 ICO 阶段不能转移到其他账户。
2. 在预售和 ICO 阶段不能交易。
3. 在预售和 ICO 阶段不能提款。

预售和 ICO 阶段结束后，ROBURST 奖金将自动转换为 ROBURST COIN。奖金 ROC 将添加到您的主要 ROC 钱包中，并可以撤销，交易以及转账。

只发行 84,000,000 Roburst 奖励代币，并以 Roburst 社区奖励计划、赏金猎人计划和市场推广活动的形式发行。一旦奖金 ROC 用完，介绍朋友和预售奖励活动将结束。我们将通过电子邮件通知投资者。

2. 早鸟投资者

早期投资者是投资者加入预售阶段并且购买 50,000 ROC 及以上。

以下声明是在预售阶段成为早期投资者的好处：

- 可以使用 Roburst Trading Bot 测试版（在 ICO 阶段结束后立即使用）
- 可以使用 Roburst Trading Bot 生成 24 小时预测方案
- 网络内无转账费用（仅限 Roburst Network 提供的服务）
- 使用 Roburst Trading Bot 没有交易费用
- 特殊电报频道

- 紧急支援（20 分钟内回应）
- Roburst Network 活动的 VIP 门票
- 优先使用我们的最新服务

3. 预售阶段

Roburst Network 以合理的价格提供 Roburst Coin 给早期投资者，包括购买可以获得奖金。投资者将获得 Roburst 奖励代币将根据 Roburst 代币投资者购买的金额而有所不同。预售阶段符合 KYC 标准，这就是为什么禁止 ICO 销售的国家将无法加入我们的预售活动的原因。Roburst Network 要求投资者提交您的国家身份证/驾驶执照/护照或任何其他类似的官方文件，以验证投资者的身份。我们还需要投资者的清晰自拍照以防止身份盗用。

未能提供我们所需信息的投资者将无法加入预售阶段。投资者无法在预售阶段发起退款。如果购买超过 2,000,000 ROC 的投资者将获得 Roburst Network 的额外奖励。您成为早期投资者需要在预售阶段加入并购买超过 50,000 个 ROC。预售阶段售出的代币数量限制为 63,000,000，相当于代币发售量的 20%。一旦代币售完，预售阶段立即结束。

下图是预售活动的摘要：.

开始日期	10:00 AM PST, 2 月 24 日, 2018
结束日期	10:00 PM PST, 3 月 25 日, 2018
持续时间	30 天
代币销售量	63,000,000 ROC

每个代币价格	0.00001 BTC
--------	-------------

代币分配日期	5 月 1 日, 2018(最差情况)
	4 月 25 日, 2018(最好情况)

最小购买	10,000 ROC
------	------------

购买限制	10,000,000 ROC/账户
------	-------------------

4. ICO 阶段

公开拍卖分为 3 个阶段, 每个阶段的起始价格不同, 每个 ROC 起价为 0.00001 BTC。根据代币的需求, Roburst Trading Bot 将为每个阶段提供特定的价格。投资者可以加 ICO, 无需申请白名单。每个阶段持续 10 天。预售阶段的未售出的硬币将转移到此阶段。下一阶段的价格将在下一阶段开始前 3 天通知所有 Roburst Network 会员。Roburst 早期投资者计划并不适用于这一阶段。

下图是 ICO 阶段的总结：

开始日期	11:00 PM PST, 5 月 25 日, 2018
------	------------------------------

结束日期	10:00 PM PST, 4 月 24 日, 2018
------	------------------------------

持续时间	30 天
------	------

代币出售量	252,000,000 ROC + 预售未售出代币
-------	---------------------------

代币价格	>0.00001 BTC
------	--------------

代币发放日期	5 月 1 日, 2018(最坏情况)
	4 月 25 日, 2018(最好情况)
最小投资	1 ROC
购买限制	100,000 ROC/账户/天

5. 推荐

作为我们营销活动的一部分, 我们向推荐朋友参与 Roburst Network 的投资者提供 21,000,000 ROC 代币奖励。但是为了防止活动中的欺诈行为, 奖励将根据推荐购买的 ROC 数量来计算。特别的是, 如果您的被推荐人将 Roburst Network 介绍给其他朋友, 您也将获得奖金。以下是推荐朋友奖金计算公式:

我们认为客户在第 n 级别买入 C 币。系统必须奖励上级转介绍金额 a 的奖金代币。 a 可以通过以下方式确定:

$$0 \leq a \leq C \lim_{n \rightarrow \infty} \sum_{i=0}^n 5\% \left(\frac{1}{2}\right)^i$$

$$0 \leq a \leq C \frac{5\%}{1-\frac{1}{2}}$$

当 $n = 0$ a 最小, 当 n 无穷大时, a 达到最大值。

例如, 如果您的网络有 3 个级别, 这意味着您介绍了朋友 A, 然后朋友 A 介绍了朋友 B, 则网络有 3 个级别。在这种情况下, 如果朋友 A 购买 1,000 ROC, 那么您将获得 1000 的 5%, 相当于 50 ROC。如果朋友 B 购买 1,000 ROC, 那么朋友 A 将获得 1,000 的 5%, 相当于 50 ROC, 您将获得 1,000 的 2.5%, 相当于 25 ROC。同样, 通过将更多人介绍到您的网络, 您可以获得更多奖金。

附录

EdDSA 是什么？

EdDSA 结合了最安全的选择。EdDSA 与 Schnorr 相似，不同于 ECDSA，因为它可以输入算法，增加了对算法冲突的弹性，避免了反转，简化并加速了结果实现。EdDSA 与 Schnorr 不同之处在于使用双倍大小的散列函数，进一步降低了散列函数问题的风险；利用 Edwards 曲线，再次简化和加速实现；并将公钥作为散列函数的进一步输入，从而减轻针对多个密钥的攻击的担忧。EdDSA 还避免了一种较小的压缩机制；压缩机制是公开的，所以它不能提高安全性，而跳过它是 EdDSA 快速批量验证的关键。最后，EdDSA 通过将每条消息与一个长期秘密散列在一起来生成每个消息的秘密随机数，而不是要求每个消息具有新的随机性。

BIP39 mnemonic code

本 BIP 描述了助记符代码或助记句的使用 - 一组易于记忆的单词 - 用于生成确定性钱包。它由两部分组成：生成助记符并将其转换为二进制代码。这种代码可以在以后使用 BIP-0032 或类似方法生成确定性钱包。

参考

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <http://bitcoin.org>.

Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov (2017). *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*. Retrieved from <https://iacr.org>.

Internet Research Task Force (2017). *Edwards-Curve Digital Signature Algorithm (EdDSA)*. Retrieved from <https://scholar.google.com>.

Larry Ren (2014). *Proof of Stake Velocity: Building the Social Currency of The Digital Age*. Retrieved from <https://coss.io>.

Sunny King, Scott Nadal (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. Retrieved from <http://peerco.in>.

Jae Kwon (2012). *Tendermint: Consensus without Mining*. Retrieved from <https://relayto.com>.

Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, Robbert van Renesse (2016). *Bitcoin-NG: A Scalable Blockchain Protocol*. Retrieved from <https://usenix.com>.

The Lisk Protocol. Retrieved from <https://lisk.io>.

Young Bin Kim, Jun Gi Kim, Took Kim, Jae Ho Im, Tae Hyeong Kim, Shin Jin Kang, Chang Hun Kim (2016). *Predicting Fluctuations in Cryptocurrency Transactions based on User Comments and Replies*. Retrieved from <http://plos.org>.