



备忘录

Bened数字货币的初步概念



备忘录



注意！注意！

备忘录

BENED 一文不值。
BENED 没有抵押品。
BENED 并不适合所有人。

Bened (BND) 是一个零成本的绿色挖矿虚拟单元。BND 虚拟单元没有任何支持。Bened 作为开源软件分发给社区。根据本备忘录的代币经济学部分，Bened 软件完全透明并按原样分发，不提供任何形式的保证。



二. 内容

序言	1
BENED 概念	3
概述	4
核心技术	5
硬币	7
网络节点	8
积木	9
创建块	10
绿色采矿BENED	14
加密辐射参数	17
挖矿难度	18
钱包 BENED	19
钱包余额属性	21
交易费用	23
BENED 密码学基础	24
BENED 代币经济学	25
路线图	27



现代金融体系是基于信任的关系模型。现代法定货币的历史始于 1347 年的佛罗伦萨，那是黑死病爆发的一年，黑死病在几年内摧毁了欧洲三分之一的人口。大流行标志着经济危机的开始，为了摆脱危机，人们不得不改革货币体系并创造一种新型货币——法定货币。菲亚特这个词从拉丁语翻译为一个公告或许可，这是整个社会的同意，使得创造一种新型货币成为可能，以纸质收据的形式表达，这在当时是不寻常的，来自存放珠宝的珠宝商并在武装警卫下将宝石和金属保存在保险箱中。正是在可怕的流行病期间，社会同意宣布纸币作为支付手段的地位，纸质收据的生产本身变成了一项名为铸币税的业务。铸币税是货币发行人在 所有权。在法币时代初期，铸币税业务是从客户的材料中铸造硬币，作为工作的报酬，铸币者保留了一部分用于生产一批新硬币的材料.正是因为任何有自尊心的领主都从事铸币税业务，我们观察到中世纪欧洲流通着如此多不同的硬币，这是去中心化金融的黄金时代。随着时间的推移，后流行病的欧洲加强了其国家垂直，建立并加强了其军队，建立了一支舰队，开始发现新的土地和全球扩张，但工程师或铁匠并不是成功的关键，菲亚特货币成为真正的引擎进步的信念，它允许创建一个在市场经济原则下发展的新社会。而现在，几个世纪后，历史的螺旋出现了新的转折，世界再次面临一场导致全球信任危机的流行病。到几个世纪以来建立的权力机构和金融机构。

十多年来，去中心化加密货币在世界范围内一直在发展，而且每年都在增加。

有人会说——“呸，加密货币？这里有什么新东西？十年了，大家都知道加密货币，但什么都没有改变！”，但在历史的尺度上，十年是一瞬间，一瞬间，未来的教科书对它的描述只取决于行动者并创造这个故事。乍一看，加密货币没有任何实物资产支持，但这种说法只是部分正确，因为没有比数百万人相信基于区块链技术的去中心化信息存储系统更有价值的了。在数字技术时代，虚拟金融资产获得了法币的力量，其品质满足了公众对公平、平等、透明、财产保护和行动自由的主要诉求。加密货币只是关于存储在分布式区块链注册表中的用户钱包余额变化的信息，可以访问对任何人开放的更改，没有限制和控制，这就是加密货币价值。

Bened数字货币的初步概念



一个在虚拟空间中复兴相当于黄金固体的项目，它已成为现代储备货币的原型，在世界范围内用作法定货币价值的标准。Bened 是金色 Solidus 的继承人，它在君士坦丁皇帝时期传遍了整个欧洲。索尔多是一个讨价还价的筹码，你可以用它来支付食物、住宿、毛皮、武器、马匹的费用，还可以支付雇佣军保护他们财产和任何其他服务的费用。

Bened 是一种去中心化的加密货币，为每个持有者提供绿色采矿方法。通过 Soldo Constant LTD 的先进开发实现去中心化网络的共识和区块链的完整性.

Soldo Constant LTD 是开发节能区块链技术的先驱，该技术可有效存储和传输有关用户在相互独立运行的点对点网络中进行的交易的信息。Bened 加密货币的主要特点是基于专利混合算法的低成本新币挖矿技术，用于确认币的余额和存储时间，挖矿难度随着总排放量的增加而增加。

PoTS



CURVE25519

SHA256



Bened是一种开源的点对点 **Proof-of-Time-Stake (PoTS)** 加密货币。先进的 **Bened PoTS** 算法是“硬币时代”概念的完美实现，可以抵抗所有可能对区块链进行的攻击，以伪造交易并生成新硬币。可用硬币的总量作为反硬币的负余额分配在创世账户中。使用带有 **SHA256** 散列算法的 **Curve25519** 混合密码系统。平均出块速度为 **60** 秒。交易在 **10** 次确认后被认为是安全的。

POTS

PROOF OF TIMESTAKE

在 Bened 使用的 [Proof of TimeStake] 模型中，网络安全由在网络中拥有硬币份额的节点管理。该算法虽然不像 [Proof of Work] 算法那样不利于中心化，但 Bened 网络自成立以来一直保持去中心化，并且随着用户数量的增长，它变得越来越去中心化。

BENED 中的 POTS 混合挖掘模型

Bened 使用绿色挖矿系统，其中每个“币”都是一个虚拟矿场，根据账户是否在区块链中生成新区块，生成率不同。由于创建一个区块而收到的总“奖励”是位于该区块内的交易费用的总和。Bened 网络节点不会因为创建区块而发行硬币，而只是确定维护去中心化网络所涉及的账户的新硬币生成率，并从他们创建的区块中记录的交易中收取佣金。区块是根据来自前一个区块的可验证、唯一且几乎不可预测的信息生成的。区块通过这些链接链接起来，创建了一个可以追溯到第一个区块的区块链（和交易）。平均块生成时间可以从 **30 到 120 秒不等**。

基本原理适用于 **BENED POTS** 算法

- 累积难度值作为参数存储在每个块中，每个后续块都从前一个块的值中获得新的“难度”。在模棱两可的情况下，网络通过选择具有最高累积复杂度的块或链的片段来达成共识。
- 为了防止账户持有人将他们的资金从一个账户转移到另一个账户以作为一种操纵手段，以便能够生成区块，硬币必须在 1440 个区块中得到确认。满足此标准的硬币具有有效的账户余额，该余额用于确定生成新区块的概率。
- 为了防止攻击者创建新链，网络允许从位于当前块后面的 720 个块重新计算该链。任何低于此阈值高度的块都会被拒绝。这个位移阈值可以被认为是最稳定的 Bened 参考点。
- 由于任何账户通过创建自己的区块链来接管区块链的可能性极低，如果交易被编码到比当前区块晚 10 个区块的区块中，则交易被认为是安全的。



硬币

初始排放

150亿

最后一期

1500亿

首期发行150亿贝内德，最终发行1500亿贝内德。硬币随着创世区块（区块链中的第一个区块）的创建而发行。公司将 10% 的初始发行量留给自己支配，以确保区块链在开发的初始阶段可运行，并且 90% 的初始发行量在交易所以市场价格出售，无需初步封闭销售程序。整个问题要归功于环保挖矿的算法[Proof of TimeStake]，产生一个负余额账户，可随时监控和收集分析信息。



Bened 网络节点是向网络贡献交易或块数据的任何设备。任何带有 Bened 软件的设备都被视为一个节点。Bened 网络中的每个节点都具有处理和传输交易和区块信息的能力。区块在从其他节点收到时会被验证，并且在区块不符合网络当前标准的情况下，节点可以暂时被“列入黑名单”，以防止传播无效的区块数据。

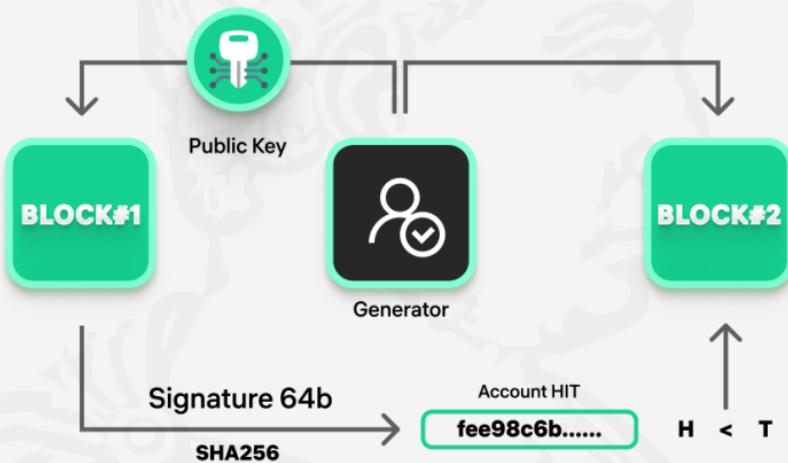
BLOCKCHAIN

与其他加密货币一样，Bened 数据库建立并存储在称为区块链的一组连接块上。该分类帐提供已发生交易的永久记录，并确定进行交易的顺序。区块链的副本存储在 Bened 网络中的每个节点上，并且每个帐户都具有生成块的能力，前提是该帐户中至少有一笔传入交易已被确认 1440 次。任何满足这些条件的帐户都称为活动帐户。在 Bened 中，每个区块最多包含 100 个事务，平均大小为 400Bytes，所有事务前面都有一个包含标识参数的 Header。一个块中的每个事务最多由 1536 个字节表示，最大块大小为 40 KB。

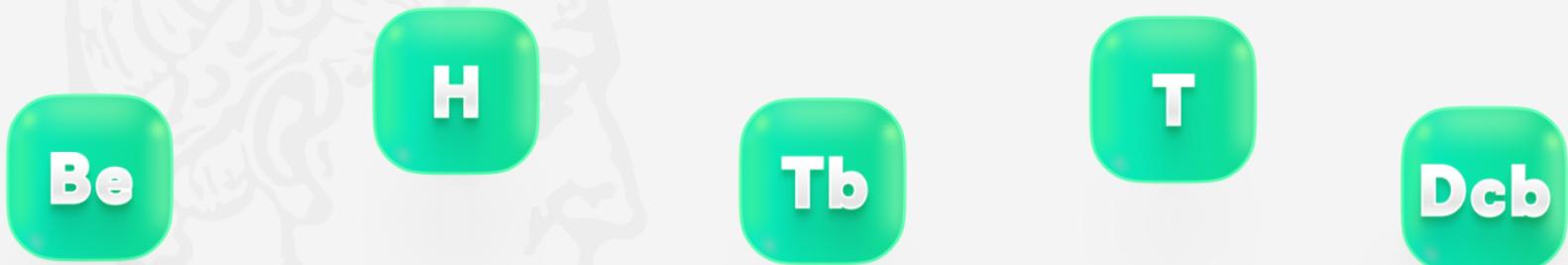
所有块都包含以下参数：

- 区块版本、区块高度值和区块ID
- 区块时间戳，以从创世区块开始的秒数表示
- 创建区块的账户的ID，以及账户的公钥。
- 前一个区块的标识符和哈希
- 存储在一个区块中的交易数量
- 一个区块中的交易和费用所代表的 Bened 总量
- 区块中包含的所有交易的交易数据，包括其交易 ID
- 块有效载荷长度和块有效载荷散列值
- 区块的基础目标值和累积难度

块生成算法



链中的每个块都有一个签名生成选项。为了参与区块生成过程，活跃账户使用自己的公钥对先前生成的区块进行加密签名。这会创建一个 64 字节的签名，然后使用 SHA256 对其进行哈希处理。接收到的哈希的前 8 个字节给出了一个称为帐户 HIT 的数字。将 HIT 与当前目标值进行比较。如果计算的 HIT 低于目标，则可以生成下一个块。如目标值公式中所述，目标值每秒都在增加。即使网络上只有几个活跃账户，其中一个最终也会产生一个块，因为目标值会变得非常大。



这意味着您可以通过将该帐户的命中值与目标值进行比较来估计生成块所需的时间。最后一点非常重要。由于任何节点都可以为任何活跃账户请求有效余额，因此可以通过所有活跃账户来确定它们各自的命中值。这意味着可以以合理的准确度预测下一个有资格生成区块的帐户。通过将质押转移到将生成下一个区块的账户可以触发洗牌攻击，这也是 Bened 的余额需要在 1440 个区块确认的另一个原因。无法预测下一个区块的新基础目标值，因此几乎不可能确定谁将生成下一个区块。在生成多个相同块的情况下，节点将选择累积值最高的块 复杂性作为权限块。

四个值是决定哪个账户有权生成区块、哪个账户获得区块创建权以及在冲突期间哪个区块被认为具有权威性的关键：**有效余额 (Be)**、**HIT (H)**、**基准目标值 (Tb)**、**目标值 (T)** 和**累积复杂度 (Dcb)**。

基本目标值

为了赢得生成块的权利,所有活动Bened帐户都"竞争"尝试创建低于给定目标值的散列值。此目标值从块更改为块。计算方法是将创建前一个块的时间添加到前一个块的部分值和前一个块的基本目标值,乘以有效平衡。

目标值（目标值）

每个账户根据其有效余额计算自己的目标值。

此值为：

$$T = S + H / (Tb \times Be);$$

其中：

T - 新的目标值

S - 自最后一个块以来的时间,以秒为单位

H - HIT

Tb - 基线目标

Be - 有效账户余额



初始目标值由10248191的成因平衡计算，最小值和最大值分别为有限和

(目标值根据目前的GENESIS余额计算) *9/10

(目标值从当前创世纪余额计算) * (占当前创世纪余额的1%)。

背景资料 {

初始=1024819,

初始min=9223371,

初始max=1537228650000000,

最终=1024819,

最终min=922337,

最终max=1537228500000000。

}

对于试图在特定块顶部生成的所有帐户,此目标值和基本目标值是相同的。唯一确定的账户参数是有效的平衡参数。



累积复杂性

总复杂性由基本目标值通过公式获得：

$$\mathbf{Dcb} = \mathbf{Dpb} + (2^{64}) / \mathbf{Tb}$$

其中：

Dcb是当前块的复杂性

Dpb是前一块的复杂性

Tb是当前块的基本目标值



绿色采矿BENED



Green Bened是在两个州生产的：
[SoftMining] 和 **[HardMining]**。

SOFTMINING

SoftMining是一种软件方法,可以通过使用私人访问密钥为每个硬币持有者提供账户余额来生成新硬币。

HARDMINING

HardMining是一种使用专门设备获取硬币的软件和硬件方法,该设备存储阻塞链的最新副本,并与公共网络同步以参与生成新的阻塞。

硬币产量的比率



每个钱包的硬币数量



附属钱包上硬币的数量



块生成

硬币生产速度由三个主要参数决定：每个钱包的硬币数量、附属钱包结构中可达十代的硬币数量以及参与区块的生成。根据平衡度量、关联钱包结构中的连接以及网络维护状态，潜伏的绿色挖掘算法从成因中生成新硬币。所有计算都是由网络节点的网络核心根据当前度量在实时模式下执行的。

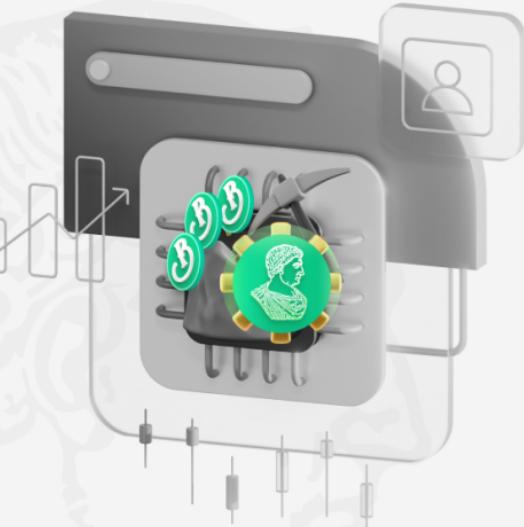
Green Mining Bened是一种先进的专利保护推广和推广工具,它将区块链固定与多层次营销联系起来,它基于在网络和其他加密技术基础上开发的企业中经过时间验证的技术。绿色开采Bened的主要优点是能够有效地防止对开采机制的干扰和绝对透明，所有用户都可以实时跟踪硬币的生产数量。Green Bened Minering在任何钱包上工作,当它达到10万硬币的余额时就停止工作.





Bened使用专利系统在钱包之间建立连接,并将其固定在块链数据库中而无需任何参考。为了提高贝奈德的生产速度,不仅要确认钱包中的钱包,而且还要确认与你有关联的十代钱包中的钱包。

要获得新的Bened,就足以创建您的私钥,并从任何活动的钱包中获得一个传入的事务。为了提高回收率,第一笔交易需要激活一个或多个钱包,然后十代关联钱包的合并资产负债表将影响参考提取率的乘数系数。Green Bened Mining允许您将能耗降至最低,并在您的钱包中发行新硬币。一届会议可获得的最大硬币数量不超过**[10000 BND]**,在达到**[100000BND]**之后,钱包将停止生产,直到其余额减少。



HARDMINING BENED 硬件

Bened cryptocurrency实现了提高矿工生产硬币的基本速率的功能，以支持对等网络的效率。对于资产负债表用来确认网络交易的钱包，无论其资产负债表如何，硬币生产的基本费率为每天1%。从接收网络的验证块生成时起，这些提取参数就被应用并运行于30,000个块。同时，从附属钱包加速生产的系数也应用于这种钱包。

加密辐射参数

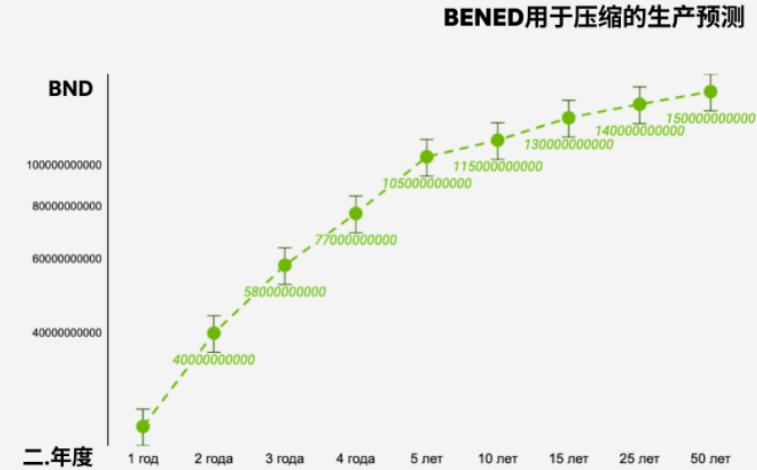
绿色软开采的基本速度--无复杂性

在没有复杂性的情况下24小时内 生产新硬币的百分比	钱包中硬币的数量
1%	不到1枚硬币
0.25%	1 - 10000
0.5%	10000 - 100000

10代中从属钱包加速生产的系数.

加速度因子	十代连接钱包结构硬币的尺寸
1,2	100000 - 1000000
1,5	1000000 - 10000000
1,8	10000000 - 100000000
2	超过100000000

BND排放总量	提取压缩系数
高达300000000000	1
高达450000000000	0.85
高达600000000000	0.7
高达750000000000	0.55
高达900000000000	0.4
高达1000000000000	0.25
超过1000000000000	0.15



*Bened的绿色采矿算法包含一个压缩系统（类似于比特币中的半数），增加了生产新硬币的难度，这有利于加密的经济吸引力。Bened的排放率与已经开采的硬币总数成正比。在提取的时候，有1000亿。硬币的有效性将比基值减少15倍，这一因素保证了内部通货膨胀的平稳减少，并增加了硬币的流动性。采矿压缩由七个系数组成，这些系数降低了萃取效率，同时增加了总排放量。



所有Bened钱包都存储在一个网络上,其中包含每个可能的帐户地址的个人密钥,这些密钥直接来自使用**SHA256**和**Curve25519**操作组合的每个帐户的代码短语。每个帐户由64位数字表示,该数字使用所罗门代码错误更正记录以帐户地址表示,该记录允许检测帐户地址中最多四个错误或修复最多两个错误。之所以采用这种格式,是因为有人担心,错误的账户地址可能导致硬币不可逆地转入错误钱包。帐户地址总是以"**BENED-**"为前缀,这使得Bened帐户地址易于识别,并且不同于其他加密地址使用的地址格式。



由**Code-Solomon**编码的与秘密代码短语关联的帐户地址生成如下所示：

1. 一个秘密代码短语使用hash来获取个人帐户密钥。
2. 私钥使用Curve25519加密以获取公共帐户密钥。
3. 公钥用hash来获取帐户标识符。
4. 帐户ID的前64位是可见的帐号。
5. Code-Solomon的编码,带有前缀"BENED-"的可见账号生成帐户地址。

首次生成私钥时,不受公钥保护。当第一个传出事务从钱包到块链时,从私钥获取的256位公钥将被保存。公钥地址空间大于帐户号的地址空间,因此不存在代码词与帐户号和可能冲突的一位数匹配。这些冲突的定义和预防方法如下：一旦使用私钥访问钱包,并且钱包受到公共256位密钥的保护,则任何其他公钥对都无法访问该钱包。



每个钱包有几个不同的平衡级别 [BENED]。每一种平衡类型都有不同的用途，其中许多值都作为检查和处理事务的一部分加以验证。

有效的平衡

有效账户余额被用作计算区块生成的基础。钱包的有效余额包括所有在区块链中有1440个确认值的硬币。

基本资产负债表

钱包的基本余额包括至少有一个确认的所有交易。

产生平衡

帐户余额生成器显示成功生成块所生成的Bened总量。



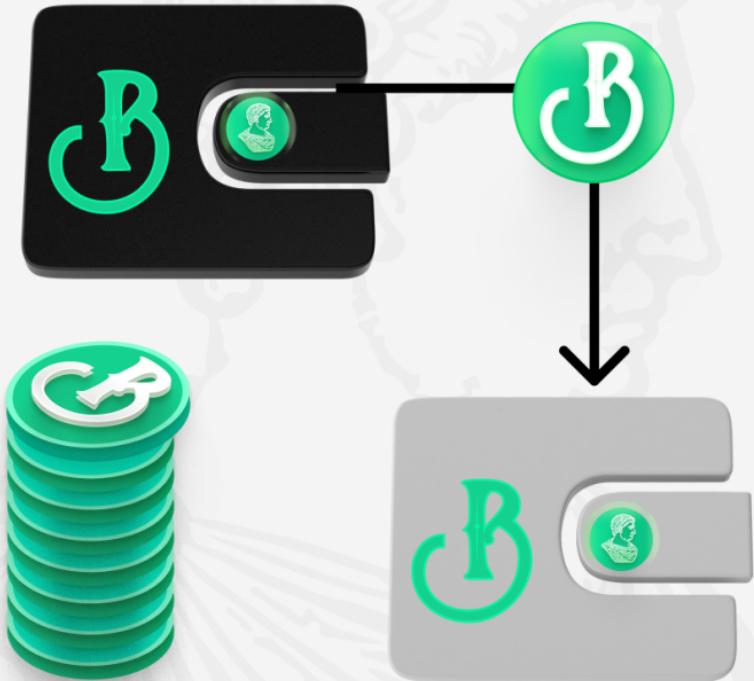
交易确认

所有Bened交易都被认为是没有证据的，直到它们被包括在块链中。创建的新块由创建这些块的节点分布在网络中。由于后续的块被添加到现有的块链中（块链），因此每个附加块都会添加另一个对事务确认数量的确认。如果某个事务在24小时内未包含在该块中，则该事务将被刻录并从事务池中删除。



交易时间安排

每个事务都包含一个以事务发送到网络后的分钟数设置的最后期限（最后期限）参数。默认截止时间为1,440分钟（24小时）。已传输到网络但未包含在块中的事务称为未经证实的事务。如果事务在事务最后期限到期前未包含在块中，则该事务将从网络中删除。Blockchain不接受具有损坏特征码或与当前网络条件不匹配的参数的事务。



1%
BND

完成交易的佣金为 1%
最低佣金为 **0.150000 BND**
最高佣金为 **100 BND**



Bened的密钥交换是基于Curve25519算法的,该算法使用快速高效的Diffie-Hellman椭圆曲线生成了一个通用的密钥,并具有高度保护。Daniel J. Bernstein于2006年首次证明了该算法。



高级JAVASCRIPT客户端

一个方便的客户端应用程序,一个新一代内置到主Bened软件的分发中,能够通过本地Web浏览器进行控制。

客户端为实现的所有基本Bened功能提供完全支持,从而使专用密钥永远无法传输到网络。

Bened的主要优势是对用户和投资者绝对开放和透明。凭借这些品质，你可以很容易地进行基础分析，并根据客观数据做出决定。

货币制度成功与否的主要标准是，有多少个人用户或社区为了其直接目的，即支付或作为积累和保存价值的一种手段而使用密码。Bened的加密业务发展战略针对的是金融监管之外的日常自愿付款市场，例如餐馆小费、捐赠以及人们每天支付的其他费用，作为对已经缴纳的税款的激励。这种类型的Bened分布将使我们能够尽可能广泛地接触并吸引大量的新的人进入Kryptics。为了实现这一发展方向，开发了一个方便的WEB钱包，可以立即写一张包含BND硬币的虚拟支票，并根据你的要求提供小费或其他奖励。为了以QR代码的形式进行虚拟检查，只要让您将其从智能手机的屏幕上拍摄到预定对象就足够了。这是在现实世界中以有机方式增加用户数量的许多策略之一。其他更有趣和有效的战略将受到商业保密的保护。

根据Bened加密货币的概念，可以得出结论，生态友好采矿**SoftMining**将以分散的方式在所有用户的钱包上进行。因此，问题是，**Soldo Constant LTD**如何为项目的开发获利？

Soldo Constant LTD的利润产生包括在开放市场上实施的相当于**[150亿BND]**的部分预支以及销售支持算法的网络节点的许可证密钥**HardMining**。在用户网络中开采**[100亿BND]**之前，Soldo Constant LTD保留以与客户和合作伙伴请求相匹配的价格为网络节点实施软件的权利。

矿前分配情况
15亿BND

● 150百万

● 30亿



19.12.2021 初始排放量为Bened隐藏度最终发行量的10%，数量为1,500亿枚硬币。

- [150,000,000 BND] **Soldo Constant LTD** 保留维持网络节点生成交易寄存器新块的性能，直到 HardMining 网络节点释放免费访问权限。
- [3,000,000,000 BND] **Soldo Constant LTD** 预留广告活动，以 AirDrop 的形式交换在市场上失去人气的其他项目的代币。
- [850,000,000 BND] **Soldo Constant LTD** 将作为赠款分配给开发生态友好型 POS 采矿技术的项目。
- [11,000,000,000 BND] **Soldo Constant LTD** 通过公开交易市场出售三年，以确保根据计划的流动性：每天不超过 [10,000,000 BND]。

Premine将在第一个区块内开采，并按照托克尼经济学模型分发到四个部分，以便进一步执行Bened备忘录。



1.Bened
blockchain发射



1

3.为Android开发
和发布本机钱包



3

5.与工程公司签署许可证协议,以分发
HardMining软件并构建一个由支持Bened
blockchain操作的节点组成的对等网络。



5

7.开发并发布iOS
的本机钱包。



7

9.在Bened blockchain中开发了元
对象的数字签名系统。



9

2.根据备忘录分发临时发行



2

4.与大使合作,并向全世
界人民分发初始排放物.



4

6.发起了一场大规模运动, 通过世
界各地的大使免费分发BND硬币。



6

8.Bened的密码在交易所上市,
硬币根据备忘录的条款出售。



8

10.利用蓝牙和无线电信号开发
和实现有限互联网事务算法。



10

ROADMAP

备忘录

数字货币BENED的原始概念



Bened.cc

2022

BENED

