A. 介绍

在其存在的很长一段时间里，每个国家都在各个领域积累了丰富的经验科学、技术、文化和日常生活领域。世界上有很多聪明而有才华的人，他们一代一代地把知识传给另一代，但很多人失去了或得不到

因为各种各样的原因。有许多人不仅想传给他们的孩子，而且想让全世界知道一些事情。就像珍稀动物在世界和世界上消失一样下一代甚至不会记得它们，也看不到它们的样子（例如，猛犸象和恐龙）。历史上，我们一直在试图恢复信息，但让我们考虑保存信息。

我想你们每个人都在思考未来会发生什么，也许你们至少想把自己的一部分转移到未来。这就像给后代传递一个信息，传递你的思想，你的创造力，以及你自己。（例如，音乐家、艺术家、思想家和发明家）。我们只知道它们是因为我们小心地保存了它们。

在任何时候，都有不同的民族和国家。这些国家之间一直有边界和控制。随着互联网的出现，界限和控制正在慢慢被抹去。现在，几乎每个人都使用因特网从世界各地获取新的信息和知识。每个人都越来越容易获得信息。

无论身在何处，人们总是互相交流。用邮件、电报和电子邮件与亲人交流和商务交流。交付的重要性和保密问题一直是而且仍然是每个人的一个重要问题。Infinium 项目就是为了解决这些问题而创建的。

B. 目的

主要目标是使用先进的加密技术和区块链技术来存储信息和传输消息。我们的项目将能够在一个加密的数据库中存储信息，这将控制存储数据的完整性。保存信息时，将固定块高度以跟踪信息到达的时间。用户之间信息的安全传输。使用现代技术（节点）“Infinium”将在世界的每个角落提供。

C. 问题- 无限硬币和数据库大小

这不是问题，而是优势。更确切地说，无限就是我们的生命。只要有人活着，人类的生命就无穷无尽。

黄金一直被开采，并一直被开采到今天，以换取其他价值。黄金也可以被认为是无限的，但它变得更加难以获得。开采黄金的工人越多，需要支付的工资就越多。我们的项目使用公式 (log2(难度）*2^40)/2 奖励工人（矿工）。员工越多，奖金越高。

硬币的数量将无休止地增长，但增长缓慢。由于保管费的原因，硬币的总量将不断减少。例如，我是一个音乐家，我想保留我的音乐和歌词，所以我不得不花一些硬币的存储。这些硬币不进入总的硬币供应，但被删除从可用的硬币。这将减少流通中的硬币数量。同时，非物质价值被添加到数据库中。

现在，磁盘的体积是巨大的，在未来，大小将增加，所以你不必担心硬币是无穷无尽的。容量的增长速度将慢于技术发展的速度（硬盘大小）。

由于硬币是无限的，未来的人们将永远有机会将信息添加到存储中。

D. 要保存的信息类型

我们的技术提供给人类的主要信息类型是文本、照片和音乐。因此，它们将保存在数据库中。

1.文本
2.照片
3.音乐

此外，将在块中分配空间用于记录文本信息。这些信息的具体内容将在下面讨论。

E. 范围

数据库中的信息

1. 文本 - 艺术作品，技术描述，诗歌，你自己的作品文本，智者的格言，给后代的信息，以

及一切可以用文本形式描述的东西。
2. 照片 - 公司标志，名人和普通人的照片，艺术家的画，以及一切可以拍摄的东西
3. 音乐-你最喜欢的作曲家的作品，你自己创作的音乐，DJ/音乐家的作品，以及所有可以在音频上录制的东西。

加载数据时，日期（块高度）将是固定的。这是必要的，以便能够看到录制的时间。例如，一位音乐家写过音乐，想维护自己作为原始音乐来源的权利。

区块链中的信息

1. 计算硬币的数量
2. 控制向另一个人转移硬币或支付储存信息的费用
3. 数据的加密和解密
4. 为想要记录任何数据的人提供额外的专用空间。例如，我想

控制数据库或任何其他信息的完整性。我可以保存数据的哈希函数
直接到区块链进一步验证我个人数据的完整性。

信息

发送消息-与每个人相关

F. 获取信息的选项

1.每个人都可以不受限制地获得信息。
2.每个人都可以不受限制地获取信息，但必须在特定日期（街区高度）之后。例如，我写下了文本，我希望每个人都能看到文本后，才块 5000000.
3. 信息可供拥有钱包的一个人或一群人使用。钱包就像一把钥匙，可以打开隐藏在每个人面前的信息。（使用钱包的私钥加密）例如，一个人/一群人可以将其用作机密信息的存储库。如果某人/团体想向所有人打开钱包，他们可以向所有人发布钱包或为所有人创建新消息。第 1 点。（要阅读敏感信息，即使余额为 0，钱包/钥匙也足够了）
4.区块链中记录的信息是开放的，每个人都可以使用。只有这个记录的创造者才知道真正的目的。
5.消息只能由消息的目标用户读取。使用用户的密钥进行加密和解密。

G. 与其他类型区块链/硬币的区别

例如比特币 — 21000000 枚。数量有限的硬币。很多比特币由于各种原因丢失。这意味着真正的总数将少得多。将来价格还会上涨。如果每个人都只使用比特币作为标准，那么有人（bang/一群人/国家）最终将能够获得大部分硬币并控制整个世界。此外，每一笔交易都会被追踪，并且可以计算出持有硬币的人。比特币只存储交易数据，并不为每个人提供任何好处。

其他硬币的数量很多，但普通人很难使用。使用只有该领域的专家才能拥有的合同和其他技术。
不像这样的物种。我们的变种是更安全的跟踪和提供更多的隐私。易于使用的人，即使没有特殊教育。无限的数字使后代能够像今天一样使用技术。我们不限制我们的子女，孙子，曾孙.数量硬币或一个狭窄的专业。 .. 我们传递我们的知识和经验 ..
我们的硬币的价值在于一个人可以写入数据库和区块链的信息本身。拥有硬币可以让一个人为今世后代的每个人传递一个“不朽”的信息

如今，拥有任何信息/技术都要花费 1000 比特币。有时候，一个人知道非常重要的信息，想与全世界分享，却不知道该告诉谁，这样每个人都会知道或保存多年。我们的“Infinium”项目将有助于做到这一点。写作和阅读的方式将便于每个人使用。随着时间的推移，这样的信息会越来越多。每个人都想在我们的数据库和区块链中写或读一些东西。信息的价值和记下来的能力只会随着时间的推移而增加

H. 与后代的沟通

对自己和周围的人要公平，这样你才能保护自己不说谎。你很快就能分辨真假。0-假 1-真-生活中不要为零。即使是一个单位也能改变一切。寻求和分享知识。313

I. 关于网络和源代码

1. 基本解释

Infinium 是一种以隐私为中心的加密货币，具有存储数据的能力。它基于 cryptonote 协议。Cryptonote 是构建具有绝对匿名性的去中心化区块链网络的协议，没有人能够看到交易细节，只有发送者和接收者。这种匿名性通过环签名，环签名是一个复杂的方案，需要更多的公钥进行验证。在环签名的情况下，我们有一组个人，每个人都有自己的秘密和公钥。环签名证明的声明是给定消息的签名者是组的成员。与普通数字签名方案的主要区别在于签名者需要一个单独的密钥，而验证者不能确定签名者的确切身份。因此，如果您遇到一个具有爱丽丝，鲍勃和卡罗尔公钥的环签名，您只能声明这些人是签名者，但你将无法确定他或她。这个概念可以用来使发送到网络上的数字事务不可追踪，通过使用环签名中其他成员的公钥，一个将应用于该事务。这种方法证明了事务的创建者有资格花费事务中指定的金额，但是他的身份将与他在环签名中使用公钥的用户无法区分。需要注意的是，对外交易并不限制你自己花钱。您的公钥可能会出现在许多其他人的环签名中，但这只是一个混淆因素（即使您已经使用了相应的密钥对自己的事务进行签名）。此外，如果两个用户使用同一组公钥创建环签名，则签名将不同（除非他们使用相同的私钥）。

2. 双重支出证明

很多人可能会认为，当你完全匿名支付时，可能会出现一个问题，用户将能够多次使用相同的硬币，当然，这与任何支付系统的原则是不兼容的。但是加密笔记协议已经准备好了。环签名实际上是一类具有不同特征的密码算法。Cryptonote 使用了“可追踪环签名”的修改版本，并将可追踪性转换为可链接性。此属性将签名者的匿名性限制如下：如果他使用同一私钥创建多个环签名（这组外部公钥不相关），则这些签名将链接在一起，这表示双重开销尝试。它曾经在 cryptonote 协议中被利用过，所以用户可以进行双倍消费，因为 cryptonote 中的密钥图像使用的是椭圆曲线 ed25519，并且它可以被复制 以一种特殊的方式修改，允许双倍的花费。此错误在 Infinium v2.0.0 版中修复。

3. 网络

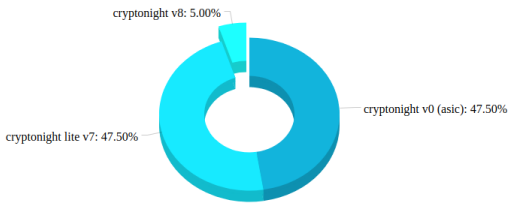
Infinium 使用 P2P 网络来同步节点之间的块。区块是存储交易和数据的区块链的一部分。所有区块都包含铸币库交易，即向 PoW 验证器排放新硬币（在现代主要是采矿池）以及其他非铸币库事务，可以是硬币传输或数据存储事务。Infinium 网络的目标是在大约 90 秒内解锁块，因此如果更多的 PoW 验证器加入网络，解锁块的难度将增加。该网络正在计算 720 块解锁时间的平均难度。每个节点保存 p2p 状态，其中写入节点在其生存期内与其他节点的所有连接。当节点启动时，它将尝试从 p2p 状态连接到节点。但是当您是一个全新的节点时，您将使用硬编码的种子节点。这些节点是由 Infinium 开发团队运行的，是与 Infinium 网络的初始连接。

4. 硬叉

Infinium 2.0.0+ 硬叉。这是一个从 2020 年 11 月 4 日开始的硬叉，它改变了英菲尼乌姆历史上的一切。所有旧的交易都保留了下来，旧用户可以使用旧密钥导出器还原他们的钱包，旧密钥导出器可以从旧钱包导出密钥，并与新版本的 Infinium 一起使用。您需要这个导出器，因为新版 Infinium 使用 ChaCha8 算法对钱包中的私钥和公钥进行加密。硬叉的另一个变化是将块奖励减半，因为 Infinium 块奖励由网络哈希率控制，可以在 C 下找到公式。但如今，Infinium 的功能比 2014 年推出时强大得多。那时候可以用 CPU 来挖掘 Infinium，例如当时最顶尖的 CPU — Intel Core i7 5820k 在挖掘 Infinium 方面的计算能力约为 190 H/s。但随着时代的发展，现在我们使用的是 ASIC 矿工，这是一种带有芯片的设备，专门用来挖掘一种特定的算法，而且速度非常快。例如，antminer X3 的速度约为 240000 H/s，因此需要这样做。下一步的改进是关于同步速度和计算 Infinium 总供应量，因为旧的代码基写得不好，并

且随着总供应量的变化而溢出。此外，支持 BIP39 种子被添加到新的 Infinium，使容易记住的种子到您的钱包。新的硬叉基于 Bytecoin v3.4.2 的 cryptonote 协议，所以感谢 Bytecoin 团队。

5. **Infinium 3.0.0+ 硬叉**



这个硬叉偷走了矿工之间的平等，并有助于确保未来的网络安全。

1) 多个 PoW 从那时起，infinium 网络上的挖掘算法就非常活跃。 我们希望填充所有矿工组（CPU, GPU, FPGA, ASIC），以最大限度地分散 infinium 网络。本文档右侧的图表中列出了每个算法的百分位数。

1.1) 我们是如何选择这些算法的？

正如我之前所写的，我们希望所有矿工组之间相等，所以我们保留了原来的 cryptonight v0 作为 ASIC 挖掘的算法。 这个算法经过时间的检验，知道它没有任何不必要的错误。 作为第二种算法，我们选择了 cryptonight V8 作为 FPGA 挖掘算法，该算法也经过了时间的检验，并且在最大的 cryptonote 项目（Monero）上实现，安全性得到了保证。 你可能会说为什么我们用这个算法只能开采 5%的区块。很好的问题是，大多数情况下，在其他硬币上，少数能够编写比特流的 FPGA 农场接管了采矿 hashrate，因为这并不是什么有趣的事情，因为只有少数实体获得了新产生的硬币，其他矿商也没有任何盈利的机会。因此，我们只将其设为 5%，因为我们不想错过从 FPGA 农场获得的高额利润，但又不想破坏其他矿商的盈利能力。 昨晚的 CryptoLite V7，我们用这个算法来挖掘 CPU 和 GPU，这个算法在过去从来没有在 FPGA 上被挖掘过，所以它的比特流存在的可能性很小。通过这个算法，我们把采矿 Infinium 带给国内的小矿工，让他们能够赚取新创造的硬币，并确保网络的安全。

1.2) 我们如何为每个算法设置百分位数？

我们已经提出了一个简单的方法，如何设置百分位数的开采区块的具体算法。在正常的 PoW 硬币开采难度已自动重定目标，以尝试在特定的时间块开采。INF（90 秒），BTC（600 秒）。 大部分时间是通过平均花费多少时间来挖掘一个区块，然后难度上升或下降以命中目标来计算的。 我们在 infinium 上为每个 algo 标记了 3 个独立的开采困难，从最后 720 个区块中每个 algo 的特定区块的百分位数计算，然后我们针对每个 algo 特定时间设定目标，以接近百分位数。cn v0–189 秒，cn v8–1878 秒，cn lite v7–189 秒。

1.3) 这一变化后，积木奖励是如何计算的

方块奖励是根据所有难度的平均难度来计算的。

2) 合并开采 允许从这个硬叉。infinium 在合并开采中起着母币的作用。 它是在这里吸引其他矿工从其他硬币相同的算法来挖掘他们最喜欢的硬币 +infinium 和安全的两个网络。它有助于稳定 infinium 的命中率，因为有更多的矿工，所以前面提到的不同算法的困难将在长期内更稳定。

原始链接：

网站: https://infinium.space
Discord:https://discord.gg/jRQZMr9u84
Telegram: https://t.me/Infinium8
Github: https://github.com/Infinium-dev

感谢：CryptoNote 开发者、字节币开发者维护 CryptoNote 协议
在英菲纽姆团队到来之前。

白皮书是雅各布和 313 写的
灵感来源于最初的 cryptonote 白皮书：
https://infinium.space/cryptonote_v2/cryptonote_v2_whitepaper.pdf