FTS 硬币：点对点电子私人交易系统

FTS 项目

白皮书@ ftscoin.xyz

www.ftscoin.xyz

简要：尽管电子对等现金系统已经成为一种。
在过去的 10 年中，不断发展的经济范式日益增长，随着我们拥抱新技术时代的到来，仍然有很多这个新软件还有改进的空间。 FTS 币希望解决其中一些需要改进的地方，包括但不限于至；隐私，POW 集中化，交易时间慢，高交易费用，混乱的交易系统以及种子损失词组。 通过解决这些问题并提供解决方案，以及使用 FTS 币帮助通过我们的 POB 推广大规模采用分布，我们希望有助于推动加密货币走向大众化采用！

一、白皮书简介

在过去的十年中，加密货币巩固了它在全球社会中的地位，因为一种跨境轻松地存储价值和进行交易的方法。虽然比特币，原始的加密货币为该技术的变化奠定了基础，
在过去十年的社会使用中，显而易见的缺点。 FTS 硬币希望在解决这些问题的同时，还利用了一部分小型硬币总供应量为 25,000,000，有助于激励人们学习新业务关于加密货币。比特币存在的最明显的问题是隐私。一旦交易完成是用比特币钱包制作的，其他人知道他们可以追踪的钱包地址该钱包的所有财务交易。如果该钱包可以连接到个人该个人的所有交易都刚刚成为公共信息。以来隐私硬币已经很好地解决了这个问题，FTS 已经成为 Cryptonote 技术。Cryptonote 使用一种不可链接的付款方式来确保隐私;有关 Cryptonote 技术的信息可以在 Cryptonote 中找到白皮书。我们发现困扰比特币的另一个问题是一个人的能力或实体通过创建大型 ASIC 挖矿来集中硬币的 POW 挖矿能力农场，或通过哈希租借服务购买哈希算力。加密货币网络如果分布范围尽可能广泛，并且
人们被投入零和战俘竞赛以获得块奖励。 POW 散列功能的过度集中阻止了这种自然而有益的网络增长，以及吸引新人们使用加密货币的能力。比特币也受制于缓慢的交易时间，尽管大多数“障碍物”比特币发生在比特币内存池中，另一个问题是阻塞时间本身。我们大大减少了标准块时间，使平均时间接近 2 分钟块。加快交易速度，降低交易费用，有助于交易及时移动，使系统易于交换使用产品。
令人困惑的软件系统在加密货币世界中也很普遍。由于大多数人最初都吸引了加密货币，因此互联网，是普通计算机用户，这是为此软件量身定制的人群远。这不利于人们在全球范围内采用加密货币。全球与其他技术相比，易用性在一定程度上推动了任何新技术的采用系统。随着 FTS Coin 朝着未来的发展前进，这一目标将保持下去始终处于前沿和中心位置，我们将与所有努力保持联系，希望他们会总有一天会被大家使用。
围绕加密货币的困惑的一部分是管理，以及资金的原始种子通常会损失很多倍。虽然
如果人们小心自己的钱包种子并加以治疗，这个问题就不会存在。他们喜欢现金，我们相信我们已经提出了一个解决方案，可以让人们随时随地携带钱包种子，而不会造成安全风险。通过允许用户选择的生物识别数据组合，以替换代表标准的钱包种子，我们希望通过没有银行柜员来弥补差距。用资金始终只是从区块链之外产生而已。
FTS 币将在不久的将来提供 POW 和 POS 选项，但将推出带有区块奖励的 POW，以一个额外的 POB 赚钱系统。POB 赚钱系统是与此硬币相关的独特设计，涉及给人们鼓励传播加密货币大规模采用的动机。该 POB 系统将通过 FTSMothership.info 网站进行管理，并从部分 FTS 投币式游戏。
为了增长和发展，一小部分 FTS 在硬币发射期间进行。 FTS 硬币的总硬币供应量为 25,000,000 硬币将在一个 100 年内缓慢分发，其中 200 万枚已被铸造。那意味着 8％的 FTS 代币供应是预先开采的，其中 92％（即 23,000,000）留给了在未来 100 年内可用。概述了这种防去老化的用途。

二、本白皮书具体内容

注：交易隐私****第 2 节是从 Cryptonote 白皮书中逐字借来的。

我们提出一种（隐私）解决方案，允许用户发布单个地址，并且收到无条件的不可关联的付款。每个 CryptoNote 输出的目的地（默认情况下）是一个公共密钥，源于收件人的地址和发件人的随机数据。反对比特币的主要优点是默认情况下每个目标密钥都是唯一的（除非发件人针对与同一收件人的每笔交易都使用相同的数据）。因此，不存在设计中的“地址重用”这样的问题，观察者也无法确定是否有任何交易发送到特定地址或链接两个地址一起。
首先，发件人执行 Diffie-Hellman 交换以从中获取共享机密他的数据和收件人地址的一半。然后他计算了一次目的地密钥，使用共享密钥和地址的后半部分。两种不同的电子琴键是
这两个步骤都需要收件人提供，因此标准的 CryptoNote 地址是几乎是比特币钱包地址的两倍。接收方还执行 Diffie-Hellman 交换以恢复相应的密钥。
标准交易顺序如下：
1.爱丽丝想向鲍勃（Bob）付款，鲍勃已经发布了他的标准地址。Sheunpack 地址并获取 Bob 的公钥（A，B）。
2.爱丽丝产生一个随机数[1，l-1]并计算一次公共∈keyP = Hs（rA）G + B。
3.爱丽丝使用 Pas 作为输出的目标键，并打包 valueR = rG（作为一部分 Diffie-Hellman 交易所）进行交易。请注意，她可以创建其他具有唯一公钥的输出：不同收件人的密钥（Ai，Bi）表示不同 Pi 与 r 相同。
4.爱丽丝发送交易。
5. Bob 用他的私钥（a，b）检查每笔通过的交易，并计算
P ＝ Hs（aR）G + B。如果爱丽丝（Alice）与鲍勃（Bob）作为接收人的交易属于
他们，thenaR = arG = rAandP’= P。
6. Bob 可以恢复相应的一次性私钥：x = Hs（aR）+ b，因此 P = xG。他
可以随时通过与 x 签署交易来花费此输出。
结果，鲍勃获得了与一次性公钥相关的入账款，对于观众是不可链接的。一些附加说明：
•当鲍勃“确认”交易时（请参阅第 5 步），他实际上只使用一半的交易额私人信息：（a，B）。这对也称为跟踪密钥，可以传递给第三方（卡罗尔）。鲍勃可以委托她处理新交易。鲍勃
不需要明确信任 Carol，因为她无法恢复一次性密钥 p，而没有 Bob 的完整私钥（a，b）。当鲍勃缺乏乐队时，这种方法很有用宽度或计算能力（智能手机，硬件钱包等）。
•如果爱丽丝想证明她已将交易发送到鲍勃的地址，则可以披露 ror 使用任何一种零知识协议来证明她知道 r（例如通过与 r 签署交易）。
•如果鲍勃想拥有一个与审计兼容的地址，其中所有入账交易都在可链接，他可以发布自己的跟踪密钥，也可以使用截断的地址。那个地址仅代表一个公共 ec-keyB，协议要求的其余部分为从中得出如下：a = Hs（B）和 A = Hs（B）G。在这两种情况下，每个人都可以“识别”鲍勃的所有入账交易，但是，当然没有人可以花掉这笔资金封闭在其中而没有密钥 b。

三、 预先挖掘
FTS 从区块 0 释放了 8％的预挖，这是 2,000,000 个硬币被用于进一步制造硬币并支持 POB 系统。这 2,000,000 个硬币的分配将在本节中详细介绍尽可能。其中的 50 万将用于技术赏金发展。随着代币的发展，使用代币的社区也在增长，FTS 代币团队的共同点，是为编码人员和可以完成某些任务的开发人员。这些赏金将根据需要寻求工作的困难。其中的 50 万将用于营销和促销。这将包括促销空投，IRL 促销活动的奖励，社交媒体促销以及任何其

他广告或促销的奖励 FTS 团队认为这将有助于推动代币向前发展。其中的 500,000 枚预兆将用于 POB 系统。 POB 系统将向个人提供 FTS 代币，用于向企业教授加密货币，以及让他们开始接受当前市场上的任何加密货币。更多细节将在本白皮书后面的 POB 系统上提供。其中有 50,000 种以任何形式用于生态系统发展可能会包括仅 FTS 加密货币商店，由 FTS 代币资助的服务专营店或任何其他有助于支持 FTS 代币价值的其他活动。剩余的 450,000 FTS 代币用于初始开发费用。

四、技术路线图

FTS Coin 将以 Cryptonote 分叉式隐私的初始形式发布硬币，总供应量为 25,000,000 枚硬币。 25,000,000 个硬币的分配应该会在 100 年后完成，并且每个区块的奖励会逐渐减少时间。这是我们当前使用该技术的计划的路线图；虽然有可能我们可能会在此议程中添加项目，因此我们不太可能将其中的任何项目都删除，未来的计划如下：

4.1 1-创始阶段

每个区块平均不到 2 分钟，正在处理交易

如上所详述，并使用具有 ASIC 抵抗能力的 POW 进行开采算法。该代币将与 CPU 挖矿选项和终端钱包一起发布，以及适用于 Windows，Linux 和 Mac 的易于使用的 GUI 钱包。

4.2 阶段 2 池采矿和电话钱包

在此阶段，FTS Coin 将添加 Pool Mining 和 android 和/或 IOS 硬币的钱包。这些添加的选项将有助于扩展矿工和用户的基础为硬币。添加电话钱包将成为第 4.5 阶段的关键步骤

4.3 阶段 3-轻松挖掘，消息和交换

FTS 币的第 3 阶段将涉及在 GUI 中添加一个简单的“立即开采”按钮钱包，以及添加从钱包发送私人消息的功能。我们希望实现简单的“立即开采”按钮，这是我们努力的一部分，推广加密货币的大规模采用我们觉得很容易抵制 ASIC 为人们提供参与网络的能力，并为网络做出贡献安全性，不仅提供了更加分散和牢固的网络，还提供了新人通过以下方式投资于加密货币本身的平台参与大块奖励的竞争。

通过为人们提供一种定时发送自己的加密消息的方式通过安全网络上的破坏机制，该机制还允许私人交易；我们希望为在法律领域进行完整的私人业务互动提供一种手段和医疗咨询。这对于希望互动的人非常有用与远程或私下与律师或医疗专业人员进行交流，同时精简两者付款和通过一种软件机制支付的咨询费用。在这一点上，如果没有从加密社区免费获得该代币。

4.4 阶段 4-POS / POW 混合股权证明将在此阶段提出。为了帮助创造动力

人们要持有他们的 FTS 币，我们将进行系统的硬分叉 POS 选项。因此，人们可以通过持有，获得，获得与我们合作的 POW，以帮助网络安全或向 FTS 币引入新业务

www.ftsmothership.info 上的 POB 系统。

4.5 阶段 5-生物识别种子整合

FTS Coin 软件计划的技术路线图的第五个也是最后一个阶段涉及添加用于生成钱包的辅助手段。此时的人们将能够生成带有单词种子的标准传统地址，这在当前很常见加密货币。或者，他们将能够开始使用相机和指纹手机上的扫描仪选择生物特征数据的组合以用于与将信息转换成 SHA 种子的算法的连接 256 个算法。通过这种方法，人们将得到保证，只要他们仍然具有关键的身体部位，他们将拥有自己的种子作为钱包，并且应该能够

使用任何手机下载钱包软件并收回资金。

五、业务证明

来自预备版的 500,000 FTS 将用于业务证明机制或 POB。人们将可以将 10 秒以上的视频企业主说，由于记录器，他们现在接受加密货币，并且发送视频的人将获得 FTS 代币的赔偿。前 2,000 个提交将分别获得 50 个 FTS 硬币信息经过验证后，请访问 www.ftsmothership.info 上的视频。下一个 4,000 个提交将获得 25 FTS 硬币。 FTS 金额每 100,000 个 FTS 代币收到的投稿硬币将继续这样的一半直到 POB 基金中剩下 50,000 FTS Coin。此时，FTS POB 基金钱包仅剩 50,000 FTS 代币的人将为他们提交的每笔业务获得 1 FTS 对于 FTS POB 提交； 企业不必开始接受 FTS 硬币。 唯一重要的是他们开始接受任何形式的加密货币，并愿意拍摄一个视频，感谢您教给他们关于它。 这样做的重点是支持加密货币的大规模采用，而不仅仅是 FTS 采用！

六，结论

我们对当前的加密货币提出了一系列改进系统将增强整个加密货币生态系统，并提供旨在易于被大众广泛采用的加密货币的当前的加密货币系统（包括比特币）为所有现代边界较少的点对点现金系统铺平了道路，但是这十年的 Beta 测试已使密码系统出现了故障。当前的系统非常清楚。我们希望通过结合以下方法解决这些问题：技术和意识形态的转变，将有助于继续采用这种令人难以置信的技术。

开发者团队

SHAHAB 先生

JEREMY 先生