罗伯特·安德鲁斯

2018.4.12

V 1.1

(简体中文版)

BIBLEPAY 圣经支付

基督教慈善加密货币

全球化影响力　　通缩投资

革命性区块链解决方案

传播福音，帮助那些需要帮助的人们

通过分散的自治慈善机构实现通货紧缩的投资方式

https://www.biblepay.org


“永远祈祷你可以被认为是值得的…
站在人子面前。”
卢克 21:36, 圣经

目录

简介

BiblePay (BBP)-圣经支付，既是一个分散的自治慈善机构，又是一种投资方式。它将 Dash 和 Bitcoin 等其他加密货币的许多功能与独特的社区建设功能相结合，并采用了一种新颖的方法来避免与典型的加密货币挖矿而带来的资源浪费。 BBP 致力于创造一个更美好的世界，并通过革命性的技术向世人展示上帝的爱。

现状分析

常见的加密货币在对核心区块链技术应用有很多种共识机制，每种形式都有其自身的缺点。 工作证明（POW）系统的电力效率极差，而证明证明（POS）系统具有调节不良行为者的固有缺陷。

此外，很多以区块链为基础的硬币或代币，产出及记账形式是利用挖矿的方式。而这样衍生出了很多的芯片级专用矿机加入到挖矿行业，这是大多数人所无法触及的。 消耗了大量的资金及电力资源。 再加上缺乏问责制的低信任环境，混乱的 ICO 发行，项目团队的预挖掘，并且不难看出为什么这么多人在寻找替代品。

圣经支付解决方案

圣经支付利用基于国王詹姆斯圣经的新证明算法算法，称为圣经证明（POBH）。 它的独特之处在于每个矿工都集成了整个 KJV（圣经），使其几乎不可能移植到 GPU 或 ASIC 挖掘中。挖掘的另一个关键方面是分布式验证计算（PODC），它是传统的更绿色的替代方案 POW，是主要的共识算法。

圣经支付具有内置的功能，使其成为自筹资金和自我管理，基于 Dash 主节点战略，并且没有 ICO 和预挖。

钱包本身内置了全面的问责制 - 每个区块的 10%可以看作是由社区支持的高效慈善机构。

市场及机遇

前瞻性

我们的目标是提供对恶性通货膨胀的对冲机制，同时帮助孤儿及更多需要帮助的人们。我们也希望通过使用圣经散列算法代替工作量验证来减少能耗产生，并通过在分布式计算证明中的社区贡献抑制我们的能耗产生，能够有效在共识机制及能耗产出中找到平衡点。并使每个人都可以公平的参与进来。

问题

有很多因素的出现，这些因素对圣经付款的机会产生重大影响，现在正是引入圣经付款的正确时机。

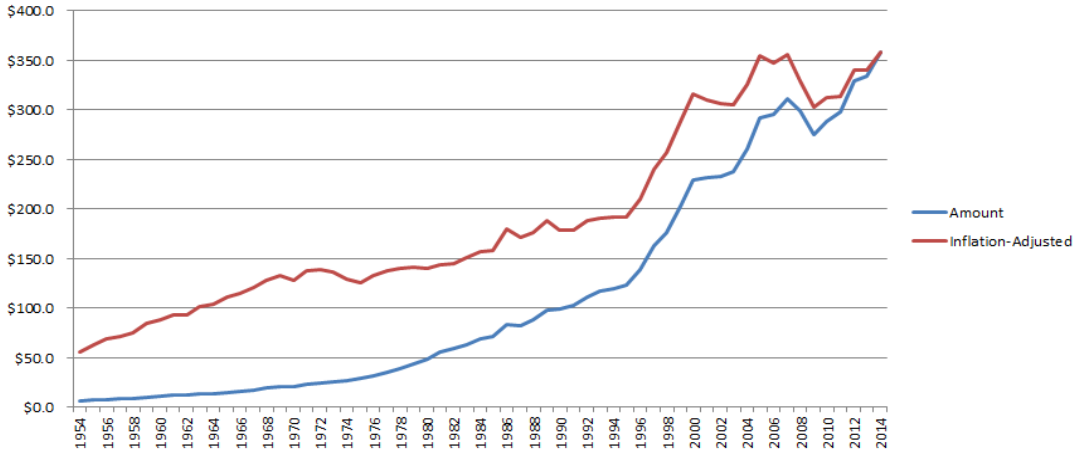
从慈善机构的角度来看，过去几十年来平均支出（GivingUSA）在持续增长，但最近慈善机构的效率却有所下降（True and Fair Foundation）。 事实上，在英国，2016 年发现超过五分之一的慈善机构将其捐款总额的不到 50%用于慈善事业，而在美国，许多大型慈善机构的宣称用途（Mercola）的开支不到 20%。

随着通货膨胀的急剧变化，这些捐款的持续性正在下降，也就是说人们得到的帮助资源在减少。 随着时间的推移，传统货币的影响力越来越小。

加密货币在解决通货膨胀问题上是一个潜在解决方案，具有从信任到更具可塑性，但加密货币普遍存在缺乏隐私和效率低等问题。 由于在开采过程中的高能耗导致过度的电力资源浪费，诸如比特币之类的采用工作证明的加密货币是最差的，因为近年来总能量消耗呈指数级增长，目前占全球能源消费总量的 0.14%以上（参考 CoinTelegraph）。

时间轴

在过去的 60 年中，慈善捐赠猛增，从每年大约 1 亿美元增至超过 350 亿美元。 同时，效率却在不断下降。



1. 社区和目的

许多加密货币的目的只是为其持有者提供一种创造财富的新方式，而加密货币自身的价值仅仅达到目的的一种手段。 这些加密货币不太可能直接对相关行业乃至整个世界产生更为广泛和积极的影响，因为它们被创造出来仅是财富驱动下的虚拟形式，而并不能改变什么。

2. 可及性

对于大量潜在的用户来说，在参与到加密货币中很难获取到更多的利益，因为加密货币的开采门槛越来越高，专用芯片级矿机及大型矿池的加入对大众来说成本过高，这是一个不幸的现实。对于那些不能从这样的技术中获益最多的人来说，更是无法触及的。

3. 治理

在缺乏统一明确的治理结构的加密货币体系中，高度分散的次级社群、持有者群体之间的利益关系会减缓加密货币的发展。 用户需要足够大的能力来创建改变，而网络需要足够快，来批准提案并实施预算。 此外，必须有可能确定一个“真实”的共识以避免分叉问题。

4. 环保

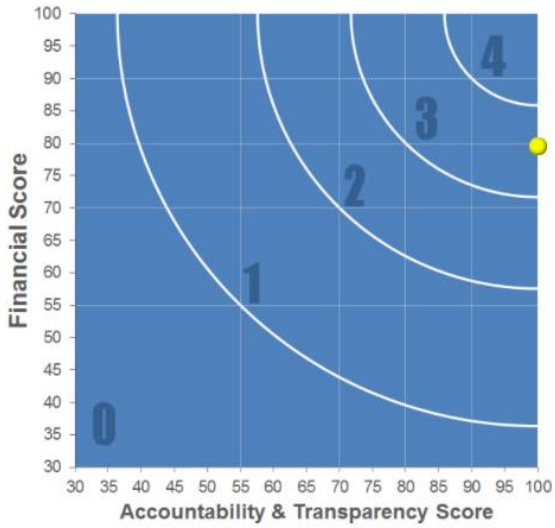
Pow 算法本身就需要大量的能量; 然而，这种计算能力本质上通常是浪费的，除了控制难度和引入安全性之外，其他用途很少。 随着此类系统规模的扩大，环境影响也在不断上升。

5. 隐私

区块链技术架构具有较高的安全性和隐私性，而安全性和隐私性又毫无关系。 许多人不希望他们的个人信息和完整的交易记录公开。 慈善捐赠尤其如此，在马太福音 6:4 中特别鼓励慈善的隐私。

社会影响力

圣经支付具有强大的社会影响力，它已经被特许只与高效的慈善机构合作。 首次推出的慈善机构是 Compassion International，这是一家公认的高效慈善机构，为世界各地的贫困儿童提供护理服务。 随后的慈善机构被选中，预算允许并由社区投票。 为确保我们的慈善承诺服务的连续性，缓冲基金被预留作为对冲 BBP 或其主要贸易伙伴 BTC 和 USD 的价格下跌风险的对冲。

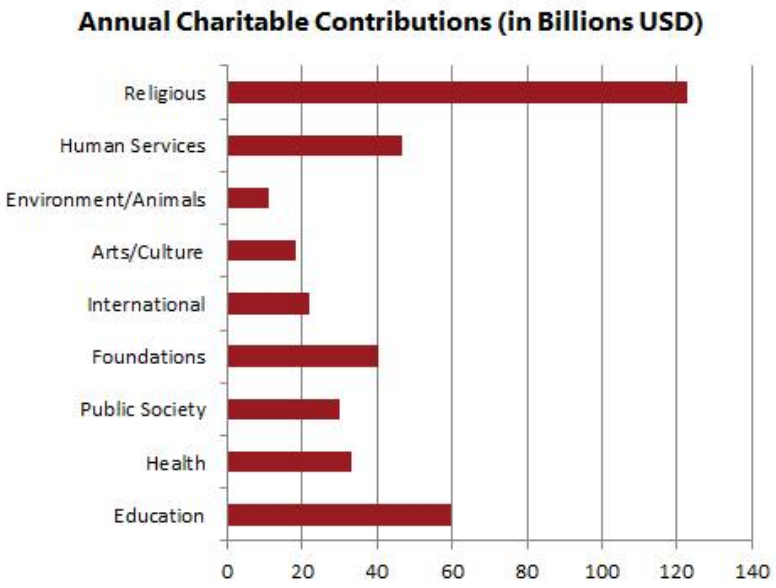


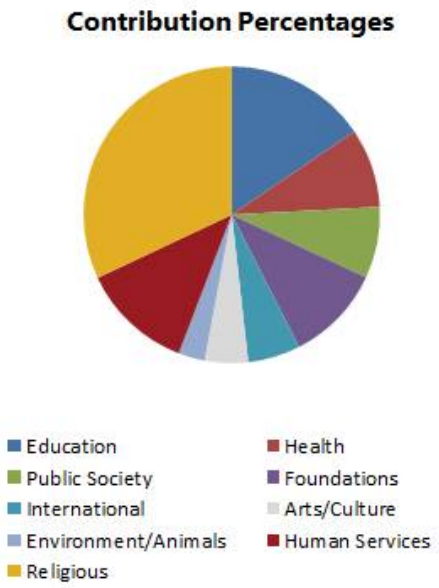
圣经支付（BBP）只与Compassion International 等高效慈善机构合作

核心价值观：诚实、高效、关爱、乐于助人，致力于提供优质服务同时不损害诚信

基于我们的核心价值观，以及对高效率的要求，我们相信我们有能力在社区中产生重大影响。 此外，宗教慈善捐款存在庞大市场，如下图（Giving USA）所示 2016 年全球慈善捐款中超过 32%，超过 120 亿美元的捐款用于宗教慈善事业。 人类服务也排在前三位，并获得非常高的 46.8 亿美元。 这样很容易能够看清圣经支付的作用。

最初的慈善机构尽管是由开发团队选择的，但随后的所有合作伙伴都是基于提案。这意味着成员必须投入股份才能提交提案并投票，如果成功，则将其添加到预算中。 通过这种方式，任何社区成员认可的优秀组织都有可能获得圣经支付的支持。





快速引导

圣经支付不是一个 TOKEN（代币），而是一个明确的加密数字货币。 虽然本身有许多与其他加密货币相同的属性，并且计划用于支付和交换，但圣经支付系统还有其他功能值得更详细地讨论。 以下部分提供了圣经支付的一些基本统计数据和概览信息。

基础特性

上线时间	2017 年 6 月 30 日
简称（币名）	BBP
计量单位	1 mBBP=0.001 BBP
最小单位	0.00000001 BBP
挖矿策略	仅限 CPU（规避 ASIC/GPU）
基础架构	Dash
核心算法	Proof-Of-Bible-Hash Proof-Of-Distributed-Computing

发行特性

硬顶	2050 年 5,200,000,000 BBP
发行类型	Deflationary
发行速度	每月减少 1.5%

可在我们的网站或维基上查看公布的发行时间表。

难度 7 分钟/块。

公平性

建立圣经支付的基本原则之一就是公平。 为此，绝对没有对 BBP 进行预挖，也没有初始代币。 没有保留的供应和特殊奖励 。每个参与者都有相同的权利获得 BBP。

钱包特点

圣经支付在钱包中融入了大量令人兴奋的特色功能。例如 InstantSend 和 PrivateSend，源自 Dash，诸如本地化电子商务支持，祷告请求和什一奉献对于圣经支付来说都是独一无二的。

经济特性

BBP 的区块奖励经过精心的设计，既服务于圣经支付任务，也适当地奖励努力。 为此，基本的区块经济分析是：

- 10%通过投票捐赠给慈善机构
- 5% 作为 IT 的支持奖励
- 2.5% 用于 PR, 2.5%用于 Peer-to-Peer features
- 3% 用户挖矿奖励
- 38.5% 捐赠给庇护所
- 38.5% 用于 Proof-Of-Distributed-Computing

避难所及分配原则

圣经支付网络由一系列被称为圣所的主节点自我管理。 这些主节点启用 PrivateSend 和 InstantSend 功能，并且可以作为分散式自治组织（DAO）共同使用。 他们对提案和发布请求进行投票，并且以高利益要求进行投票，有助于确保整个网络的安全。

财务部门完成了 DAO——这仅仅是根据保护区投票预算花费的部分资金。财务分配要求最低限度的 10%的保护区投票，并且所有的 IT、公关和对等预算均由财务部门奖励资助。

Proof-Of-Bible-Hash 介绍

钱包使用 X11 blockhash 来维护 blockindex 映射的引用指针。 然而，它使用 BibleHash 来调节难度，并证明一个完整节点生成圣经（通过要求 txindex 查找，块散列或接收地址存在于 hash 的后缀中）。

请参阅以下信息，了解 Proof-Of-Bible-Hash:

1. BibleHash 函数在某个时间点提供当前块模板的输入 X11hash。 这始于 uint256。 它也被引用到最后一个块索引（以及之前的高度和之前的块时间）

2. BibleHash 函数使用 AES512 将 x11 hash uint256 加密为密文向量。 这个密文向量然后被转换为 base64。 （这些功能被选择来提高标准，以降低将 hasher 移植到 GPU 的可能性，因为 AES512 需要 OpenSSL 库）

3. 通过 MD5 散列过后的 base64

4. md5 hash 长度为 32 个字节。 BibleHash 函数将 md5 哈希分为 8 个八位字节，每个字节为 4 个字节。

对于每个 4 字节的八位字节，十六进制数乘以 IVerseFactor（.4745708）。 这 IVerse 因素指向 0-31101 之间相应的 KJV 圣经经文。 这个结果链接到输出，这个过程重复八位字节 # 2-8，同时将诗句附加到链接的诗节输出。.

5.当 BibleHash 函数达到第 8 节时，它将源四字节八位字节分解为四个元素：一个十六进制 2 字节源，导致回溯块从 0-255 偏移，十六进制一字节源导致事务偏移量为 0- 15，一个十六进制的一个字节源，导致事务输出偏移量为 0-15，一个字节源导致数据类型指针为 1-3（乘以 0-15 * .1875）（用于确定这个圣经诗句 将需要引用块冲突，事务 ID 或接收地址）。

然后，BibleHash 通过读取磁盘，检索结果，并将结果附加到最终的链式经文（第 8 节），从链中调用结果 DataType 的完整节点。

6. 然后生成的链式经文文本内容经过 MD5hash 处理，为 X11 散列器提供输入。

7. DM5 hash 到 X11 的过程。

8. X11 哈希通过业务逻辑过滤器发送，需要最新强制版本圣经支付的完整节点业务逻辑（IE 中的一些业务逻辑根据块编号调整结果散列）。

9. 接下来，如果该块比滞后块阈值早，则 X11 散列被修改为更容易解决。

10. 如果该块是 TITHE_MODULUS 块，则该块更容易解决。

11. 得到的 X11 散列作为散列结果从函数中发出

Proof-Of-Distributed-Computing 介绍

Proof-Of-Bible-Hash（作为前面描述的 POW 变体）由我们的分布式计算机制进行补充，这对于那些使用 POS 算法的人来说是熟悉的。 PODC 通过将圣经支付矿工与一个或多个圣经支付的任务相一致的分布式计算项目进行协调。 创建交叉项目标识符（CPID）后，矿工将 CPID 添加到其控制器钱包中，然后与运行 BOINC 软件包的一个或多个设备相关联。

把每个批准的项目与圣经支付团队联系起来，可以将 BOINC 最近的平均信用（RAC）作为股权要求的基础。 当矿工提供 BBP 的足够股权余额以满足 BOINC RAC 的要求时，它们将被添加到每日超级块中，根据它们的规模或他们在团队总数中的份额分配给每个成功的矿工。 RAC 计算为 14 天内的平均运行时间，因此，只要用户保持准确的股权余额，用户在停止计算后也将获得历史工作报酬。

为了在 PODC 共识系统中实现最大的完整性，PODC 更新事务是基于任务完成而定期执行的（并且也可以手动触发，特别是当没有当前分布式计算任务正在运行时）。这些更新事务确保了利益平衡，通过验证控制器钱包报告的任务开始时间与分布式计算源系统（例如 Rosetta @ Home 或 World Community Grid）中的时间对比，验证数据日志的完整性和准确性，阻止任何 SQL 信用篡改并确保任务所有者的签名与记者的 CPID /钱包组合匹配，防止任何接管攻击。 在配置的网络时间（当前 24 小时）内没有完成任务的矿工被认为拥有 0 的量级并且不符合超级块奖励。

有些项目可以调整个别项目的权重以反映替代难度/信用计算 - 这在每个项目中都普遍适用于每个圣经支付团队的成员。 此外，可以随时调整的股权要求并非全部或全无 - 部分股权允许甚至新用户从每日超级块中获得部分奖励。 我们鼓励用户将自己的计算能力贡献与其可用的股权余额进行平衡，以确保获得准确的奖励。

在网络异常的情况下，已经实施了分层次的灾难恢复方法，确保超级块中的矿工奖励得到精确计算，并以尽可能精准的信息进行分配。

安全性介绍

对主要加密货币有几个众所周知的攻击，这些攻击已经被思考、评估并在圣经支付系统中设置防御。

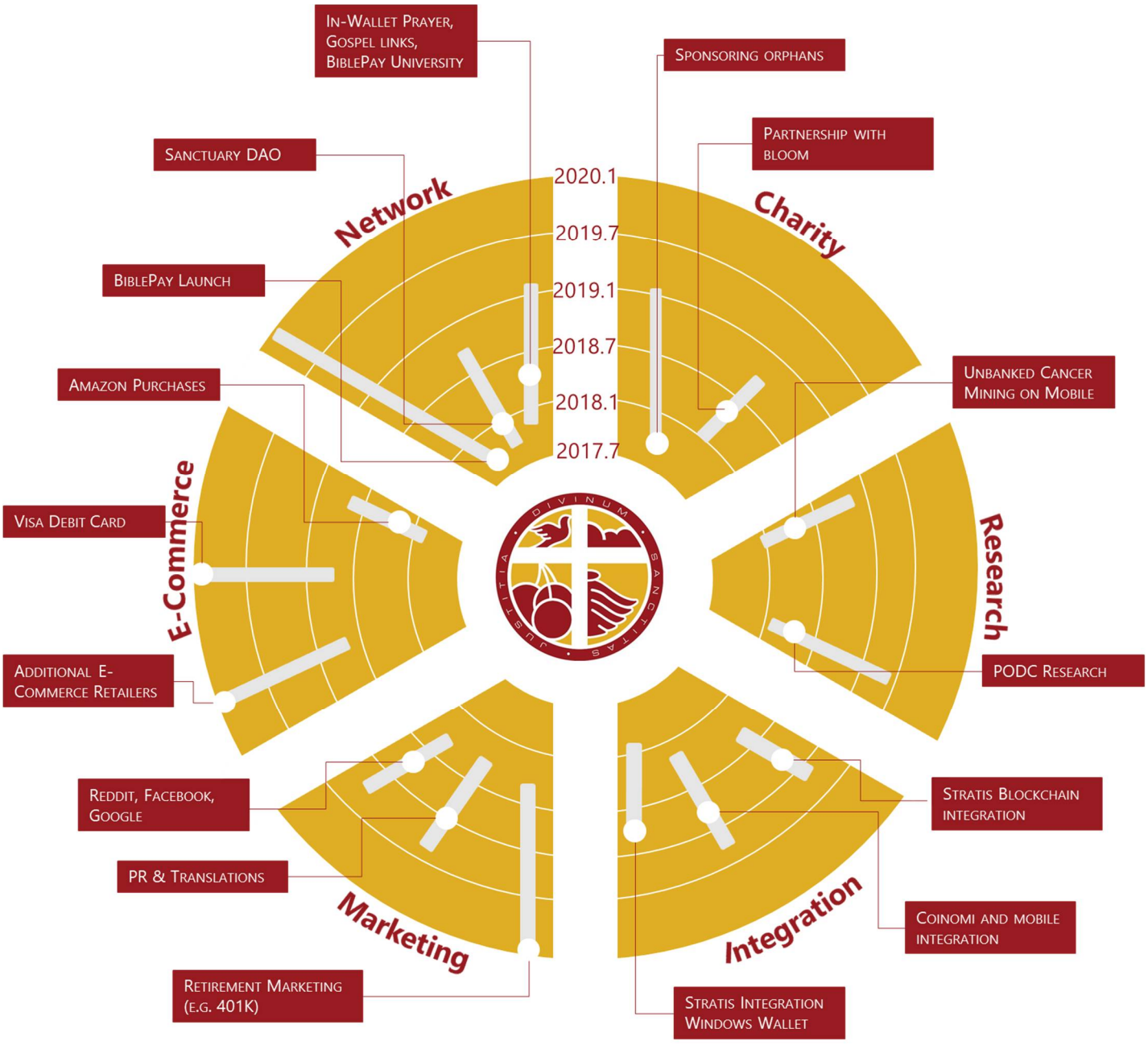
一种常见的技术是众所周知的“51％攻击”（实际上现在认为实践中操作成本低至 30％，成功概率较低），其中矿工或一小组矿工充分控制计算能力以影响不适当的变化这通常也是用僵尸网络执行的，所以有时也被称为“僵尸网络”攻击。在圣经支付中，由于一些因素，这种攻击被认为比其他许多加密货币困难得多，尽管分布式计算证明是该防御的基础方面。

首先，我们需要一个不同的 CPID 来挖掘每个块，并限制给定块范围内给定 CPID 可以解决的块的数量，因此攻击者不仅需要哈希功率的 51％，而且需要 51％的哈希功率为了影响这种攻击，也有不同的 CPID。这不仅成本高昂，而且还有时间限制，因为每个 CPID 需要有足够的 RAC 随着时间的推移而建立起来，而在概率较低的版本中，每次这种失败的攻击仍会导致难度增加为每个后续块，并因此为其他合法的 CPID 打开大量机会来解决一个块并擦除攻击。

关于目前用于人为地扼制阻碍难度的“时间窗口”攻击，使得矿工可以快速解决多个街区，从而为双重花费或其他非法活动创造机会，圣经支付通过减少这种风险来减轻风险，解决方案的平均时间戳窗口（15 分钟，大致为 2 个块的解决时间），并且不允许时钟时间超过 5 分钟。

通过这些方式，由 PODC 和 POBH 组合授予的圣经支付的安全性确保了连锁店的完整性保持不变，确保安全让用户放心，因为知道最广为人知并且被充分利用的攻击在这里不适用。随着其他攻击手段的曝光，圣经支付团队致力于快速评估和缓解系统中的任何弱点。

发展路线图


In-Wallet Prayer, Gospel links, BiblePay University
Sponsoring orphans
Partnership with bloom
Sanctuary DAO
Network
Charity
2020.1
2019.7
2019.1
2018.7
2018.1
2017.7
BiblePay Launch
Amazon Purchases
Unbanked Cancer Mining on Mobile
E-Commerce
Research
Visa Debit Card
Additional E-Commerce Retailers
PODC Research
Reddit, Facebook, Google
Stratis Blockchain integration
PR & Translations
Coinomi and mobile integration
Marketing
Integration
Retirement Marketing (e.g. 401K)
Stratis Integration Windows Wallet
Probable Manifestation Range
Estimation of Maturation

免责声明

本白皮书的目的是介绍圣经付款加密货币。 本文提供的信息可能并非详尽无遗，并不意味着合同关系的任何要素。 其唯一目的是向潜在投资者和参与者提供相关合理的信息，以便他们决定是否对提供进行更彻底的分析。

本白皮书中的任何内容都不应被视为构成任何形式的招股说明书或招揽投资的招股说明书，也不以任何方式涉及在任何司法管辖区提供或招揽购买任何证券的要约。 本文件仅在性质上属于资讯性质 - 它不是根据（也不受制于）可能旨在保护投资者的任何司法管辖区的法律或法规组成的.

圣经付款团队明确表示不承担任何直接或间接因下列原因导致的任何直接或间接损失或损害的责任：

1. 依赖本文档中包含的任何信息
2. 任何此类信息中的任何错误，遗漏或不准确性
3. 由此产生的任何行动

本白皮书可能包含对第三方数据和行业出版物的参考。就圣经支付所知，本白皮书中转载的信息是准确的，其估计和假设是合理的。但是，不保证这些信息的准确性或完整性。尽管本白皮书中转载的信息和数据被认为是从可靠来源获得的，但我们并未独立验证本白皮书中提及的第三方来源的信息或数据，或确定了此类来源所依赖的任何潜在假设。

本白皮书包含前瞻性陈述或与圣经当前期望和未来事件观点有关的信息。 圣经支付将这些前瞻性声明基于其当前对其未来事件和财务趋势的预期和预测，它认为这可能会影响其财务状况、经营业绩、业务战略、财务需求或圣宝的价值或价格稳定性。不应该过度依赖这些前瞻性陈述。

加密货币是一种高风险投资，可能不适合所有类型的投资者。在购买任何加密货币之前，必须确保明了加密货币交易中固有的特性，复杂性和波动性等，并请做好风险评估。在不了解潜在损失程度的情况下，不应购买加密货币。

加密货币汇率迄今表现出强烈的波动性，潜在损失的风险程度可能扩展到整个加密货币投资。圣经支付以外的许多因素会影响加密货币的市场价格，包括但不限于国家和国际经济、金融、监管、政治、恐怖主义、军事和其他事件、不利或正面的新闻事件和宣传、以及不确定的极端因素所导致的市场波动状况，价格和买卖、交易能力的极端变化可能随时发生。

参考文献

PAGE 5 & PAGE 7, GIVINGUSA
https://givingusa.org/

PAGE 5, TRUE AND FAIR FOUNDATION
http://www.trueandfairfoundation.com/content/file/feature/review-hornets-nest-report-into-charitable-spending-UK-charities-12-dec-15.pdf

PAGE 5, MERCOLA
https://articles.mercola.com/sites/articles/archive/2013/08/07/worst-us-charities.aspx

PAGE 5, COINTELEGRAPH
https://cointelegraph.com/news/bitcoin-mining-uses-more-power-than-most-african-countries

PAGE 5, CHANNEL4
https://www.channel4.com/news/factcheck/how-much-charities-spend-good-causes

PAGE 6, CHARITY NAVIGATOR
https://www.charitynavigator.org/index.cfm?bay=content.view&cpid=42