Bitcoin Private

白皮书

一场隐私的革命

在 2018 年及未来实现中本聪的愿景

2018 年 2 月

第一版

已通过同行评审

作者:

Bitcoin Private 社区

Jacob Brutman, Ph.D.

Jon Layton

Christopher Sulmone

Giuseppe Stuto

Geoff Hopkins

Rhett Creighton

WWW.BTCPRIVATE.ORG

摘要

互联网创造了信息共享历史上最大的拐点。尽管便利的信息存储方式具有无数优势，但人们通常需要牺牲自己的隐私作为代价。很多时候，在用户没有任何漏错的情况下，由于第三方信息储存的安全性薄弱被破坏，从而导致用户的敏感信息被损害或盗取。因此，需要有一个更好的系统来移除第三方中间人并让任何两个人可以进行自由安全的交易。一个新的加密货币，Bitcoin Private，因此被推出。Bitcoin Private 具有低费用、快速和隐秘交易的网络特征 - 真正实现了比特币创造者中本聪的意图。 Bitcoin Private 是比特币与 Zclassic 合并分叉的产物。由此产生的 Bitcoin Private 交易费用较比特币大大降低，并且将交易速度提高了四到六倍。更重要的是，zk-SNARKs，一个由 Zcash 基金会研发执行并经过同行评审的隐私技术，也被应用到了其中。 zk-SNARKs 允许匿名和隐秘交易 - 这是一项其他私密技术无法实现的优势。Zclassic 和 Bitcoin 的 UTXO 数据将会被包含在这个新账本的初始货币中。这意味着总量 2100 万个币中的大约 2040 万个币在分叉时就会产生，这将确保 Bitcoin Private 在加密货币领域中拥有着最低的通胀率。总之，本白皮书讨论了 Bitcoin Private 的技术优势、商业适用性、该区块链的未来发展潜力以及其主要由社区主导的属性。

内容表

1. 介绍

在大部分有记录的历史中，交易都是隐秘并且匿名的。交易信息只会对支付方和收取方披露。但是近来，由于绝大部分金融交易都需要通过信息技术完成，因此维护金融财务信息的隐私变得越来越困难。最常见的付款方式（例如信用卡/借记卡，ApplePay，支付宝等）导致交易的所有信息都以数字形式存储。虽然这些交易方法带来了巨大的好处，但它不应妨碍普通消费者拥有自己的金融财务隐私。鉴于时常发生的大型金融机构内部因违规行为而导致个人和金融信息严重泄漏，一个更具保护金融隐私的需求已经变得更加迫切。[1,2] 此外，各种金融机构也被发现售卖客户的数据，[3] 以及在没有任何合法的依据下阻碍用户的合法交易。

2008 年 10 月，中本聪发布了名为“比特币：对等电子现金系统”的学术文章，其中详细描述了世界上第一个加密货币的基础。[5] 中本聪的愿景是创造一种货币，在无需第三方机构管控下进行交易、限量通货膨胀以及通过匿名性实现公民的货币自由。自从 2009 年推出比特币以来，已经有超过 1000 种不同的加密货币被创建并取得了巨大进步。[6] 的确，许多新的加密货币在交易速度和费用方面远远超过比特币。但无论如何，由于其先发优势和大量的交易配对，比特币仍然是最流行的加密货币。

随着比特币区块链逐年发展，开始出现了一些值得注意的问题。这包括固定的小块区块（导致不实用的过高收费）、缓慢的区块时间（平均 10 分钟）、长难度调整期（每 2 周）、以及先进的专用集成电路（ASIC）采矿设备（用于快速计算 SHA-256：该算法是关键共识参数）的开发和批量生产而导致的进一步的中心化。为了让比特币处理这些问题，超过 50%的矿工必须同意更改他们正在运行的代码；迄今为止，还没有发生过这样的事件。这推动了比特币分叉的出现（如比特币现金和比特币黄金），以实现这些技术改进中的一些。例如，比特币现金改造为允许更大的区块（≥8MB vs 1MB）从而降低费用并提高交易容量。然而，这并非没有权衡 - 它的价

格潜力由于缺乏固定的区块大小和“费用市场”而受到损害。比特币 mempool 的"费用市场”促使各笔大大小小的交易与彼此的机会成本竞争；这使得它的持有价值更加迫切，造成了更高的需求。比特币黄金选择了另一条路线，它不缩短区块时间（2.5 分钟），而将 PoW 算法转换为 Equihash（ASIC 抗性），并引入增强的难度调整算法，在每个区块调整。它在很大程度上实现了作为一个与 GPU 兼容的比特币分叉的目标，但它缺乏比特币的广泛采用，并且其开发人员未公开地预挖获得大量币，让许多人认为是不道德的行为。[7] 尽管处于各种好意，截至 2017 年第四季度，比特币分叉币在加密货币市场上地位居仅次于比特币。

在中本聪的核心理念中，许多人被这种技术带来的以匿名方式使用一种通缩价值单位的能力所吸引。“隐私权”象征着自由世界中的最高自由，[8] 也是中本聪和加密货币社区所提出的核心价值。金融隐私是中本聪对新数字货币世界愿景中的一个重要理念。然而，许多人仍然迷失于在区块链上使用伪匿名交易的十字路口。此外，还有政府和私营部门组织利用大量数据集和机器学习来识别与此类交易相关的个人身份。事实上，截至 2018 年 1 月，BitFury 能够对 15%的比特币交易中进行反匿名处理，这一数字每天都在增加，并将在未来几年显著改变加密货币世界。[9] 比特币缺乏隐私性 - 这在其创造者的初衷看来如此具有讽刺意味。不过，这里有一个解决方案。

各种加密货币都试图解决这个隐私问题。不幸的是，许多通过混淆或 TOR 节点实现匿名的链上交易系统仍然能够通过各种技术被攻陷。2014 年，麻省理工大学的研究人员在一项突破性研究论文中讨论了“zero-knowledge non-interactive arguments of knowledge”或 zk-SNARKs。[10] 值得注意的是，实施 zk-SNARKs 的加密货币允许进行隐秘式交易 - 资金完全匿名且无交易或地址余额出现在分类帐上。2016 年，这项研究的作者开发并推出了第一个采用 zk-SNARKs 的加密货币 Zcash。“创始人税”也被纳入 Zcash 的代码中，允许开发团队和早期投资者获得社区开采的 20％的币。在仔细听取采矿界的意见后，Rhett

Creighton 决定在 8 天后分叉 Zcash，取消了创始人的税收并创建了 Zclassic - 一个由社区开发的透明 Zcash 平台。不幸的是，这个伟大的想法同时也让 Zclassic 陷入了困境：缺少创始人税导致缺乏资金对项目进行活跃开发。然而，有各种治理方法可以防止这种滞怠的发展。

Bitcoin Private，一个比特币和 Zclassic 的“分叉合并”，旨在增加比特币区块链的隐私性和可用性，同时对先前比特币分支面临的挑战、选择和失败保持充分认识。为了实现这一点，Bitcoin Private 将使用更大的区块（2 MB），更短的区块时间（2.5 分钟）以及具有 ASIC 抗性（更亲好 GPU）的工作证明（PoW）算法 - Equihash 用于挖矿。此外，由于这种分叉合并的双重性质，会有更多的加密社区参与其中。在快照之后，ZCL（t &z）和 BTC（segwit&normal）地址将在同一地址收到 BTCP（两者均按 1：1 的比例）。这是此类分叉的第一次，开源的区块链社区终于开始了全面探索 UTXO 集合的可塑性。

表 1: *Bitcoin Private 与比特币, 比特币现金, 以及比特币黄金的比较.*

	Bitcoin Private	比特币	比特币现金	比特币黄金
总量	2100 万	2100 万	2100 万	2100 万
隐私性	zk-SNARKs	**x**	**x**	**x**
区块时间	2.5 分钟	10 分钟	10 分钟	2.5 分钟
区块大小	2 MB	1 MB	8 MB	1 MB
PoW 算法	Equihash	SHA256	SHA256	Equihash
难度调整	每个区块	2 星期	2 星期	每个区块
私募预挖	**x**	**x**	**x**	Yes
社区主导	Yes	**x**	**x**	**x**
治理机制	Yes	**x**	**x**	**x**

2. 分叉方法

Bitcoin Private 提出了“分叉合并”的倡议，即将两个加密货币的 UTXOs 合并到一个区块链。这将会在 Zclassic 区块链上发生，因为 zk-SNARKs 和 JoinSplit 交易会是新区块链的基础。人们可以将区块链运算比作链增长聚合机制：当下一个区块被运算出时，区块链就会增长，就像聚合物随着聚合反应添加单体到链端而生长一样。然而不同的是，聚合物链通常希望变得更长来增加它们所产生塑料的韧性，而增加区块链尺寸却会导致存储消耗的增加以及节点同步时间显著更长。幸运的是，这个快照只需要从比特币和 Zclassic 中检索一个时间点的地址状态，并引入到新区块链中。这种方法有效并显著减少新的区块链所需的存储空间，从 157 GB 减少到 10 GB（启动时）。此外，Bitcoin Private 客户端将支持区块链修剪和像 Electrum 这样的 SPV 技术，以减轻用户设备上区块链的负担。

任何分叉必须处理的一个重要问题是“重放攻击 – reply attack”，它会让分叉后在旧区块链上的交易也会在新区块链上生效。所有分叉币都必须有重放保护（reply protection），以确保新旧区块链之间的合法性和独立性。为了防止来自比特币和 Zclassic 的重放攻击，Bitcoin Private 将提供双向重放保护。这是一个被研究过的问题，我们将使用行业标准方法，即如上所述采用双向方式，并已经实施到了新的区块链中。我们使用行业标准方法（SIGHASH_FORKID），该方法经过充分研究，并已成功应用到了比特币黄金分叉中。[11]

比特币和 Zclassic 的快照定为 UTC 时间 2018 年 2 月 28 日下午 5 点之后第一个区块，分叉/主网上线约在之后的 2 天发布。发布后，将有大约 70 万个可开采的 Bitcoin Private。初始的区块奖励将定为 1.5625 个 Bitcoin Private，并且将在每 21 万个区块后（约 1 年）减半。如果届时这个实验证明不成功，有一个替代计划可以实施，这将在第 7 节中描述。

3. 工作量证明 POW: Equihash

正如介绍中所讨论的，比特币的挖掘主要由 ASIC 来完成，ASIC 是专门用于显著超越 GPU 的设备。与 GPU 不同，ASIC 非常难以获得，这导致比特币挖矿的显著中心化。事实上，Igor Homakov 认为超过 60%的比特币网络哈希运算率位于中国。[12] 相比之下，由于 GPU 在世界各地更容易获得，抗 ASIC 的算法更可能实现去中心化。网络哈希运算力的去中心化使得区块链的民主化程度更高，51%攻击的可能性降低，并能确保通过挖矿产生的加密币以及获得的相关费用能尽可能地均匀地分布在整个社区。这进一步避免了少数矿工通过挖掘大量的加密币来操纵市场以及影响区块链开发的能力。

Bitcoin Private 将利用备受推崇的 Equihash PoW 算法作为不对称工作证明（PoW）机制，该算法由位于卢森堡大学的 Alex Biryukov 和 Dmitry Khovratovich 开发。[13] 与其他抗 ASIC PoW 算法不同，Equihash 基于“生日问题”和用于解决它的增强型 Wagner 算法。此外，Equihash 具有“内存硬度”特性，使内存使用率和速度的降低与高额的计算力惩罚进行关联。这一特性增加了 Equihash 的 ASIC 抗性，因为 ASIC 需要增加内存成本才能使其与 GPU 或甚至 CPU 具有竞争力。原论文的作者讨论到，虽然“内存硬度”无法抵御基于僵尸网络的 CPU 挖掘，但大量的内存消耗会非常严重，这样被感染 PC 的用户群会发现性能存在显着差异，并采取必要措施消除感染。

4. 透明 vs. 隐秘交易

Bitcoin Private 是两个交易系统的融合 - 透明和隐秘交易。透明交易的运作原理与比特币相同 - 输入、输出、金额和签名。所有资金、目的地和金额的来源都透明地存储在区块链中。相反，隐秘交易将这些细节加密

到称为 JoinSplit 的区块的特殊部分中。这些交易是可验证的，但对第三方观察员来说却难以解读。在支付隐秘票据时，区块链的完整性通过专门的零知识证明算法 zk-SNARKs[6] 来保持。该算法执行一系列计算，以显示输入值与每个隐秘传输的输出值之和。然后，发送者证明他们拥有输入票据的私人支出密钥，赋予他们支付的权力。最后，输入票据的私人支出密钥与整个交易的签名密码相关联，这样交易就不会被不知道这些私钥的任何一方修改。[14] 整个方法依赖于 Zcash 的信任设置：在 Zcash 启动时，零知识证明和私密交易产生并随后销毁所需的密钥；这被称为“仪式”。[6] 通过这样做，系统可以确保“对被选消息攻击的一次性强不可伪造性”。[10]

5. 志愿矿工贡献计划

为了建立供 Bitcoin Private 的维护和开发的基金，启动了志愿矿工贡献计划。在这个计划中，6.25 万 Bitcoin Private 通过哈希运算力的方式被拍卖给矿工并筹集到总共 5 万 Zclassic 捐赠到 Bitcoin Private 基金中。项目中给任何一个矿工的支出由以下公式确定：

$$P = Z_m * 62{,}500/Z_p$$

其中 P 是给矿工的支付，Z_m 是矿工通过挖矿开采的 Zclassic，Z_p 是整个矿池开采的所有 Zclassic。6.25 万 Bitcoin Private 在分叉时产生并存入每个矿工提供的相应钱包地址。为此计划而建立的分叉前 ZCL 多签名钱包将拥有高达 5 万 Zclassic，随后将分叉产生 BTCP，以供社区使用于 Bitcoin Private 的开发、赏金、营销以及总体财务开支。这是用于解决最初 Zclassic 发展问题的几种方法之一。

在某些方面，这个计划可以被看作是 Bitcoin Private 贡献团队强烈反对的“预挖矿”。然而不同的是，预挖矿一般由核心团队直接执行并受

益，这个项目的情况显然不是这样。在这个计划中，矿工社区可以自愿选择捐赠资金，以换取早期挖掘 Bitcoin Private 的机会。此外，由于该计划采用拍卖的方式，矿工社区能够选择每个 ZCL 捐赠的价值是多少（参见上面的公式）：这种自由市场方法是中本聪对比特币最初愿景的核心。这些资金将用于交易所上市（50%），开发（25%），市场营销（15%）和一般/行政（10%）。

6. 基金会治理

Bitcoin Private 成立了基金会治理委员会，委员会由三名社区成员和两名来自矿工社区的成员组成，基金会治理委员会已经被注册为 BTCP Developer Community, LLC。在本白皮书出版时，Jacob Brutman 博士（业务负责人）、Giuseppe Stuto（市场主管）和 Peter Hatzipetros（总法律顾问）代表社区，而 Adib Alami 和 Evan Darby 代表矿工社区。该理事会的章程文件也已准备好。[15]

7. Bitcoin Private 的未来

全面提高隐私性是 Bitcoin Private 项目的重要组成部分。目前，zk-SNARKs 在签署交易时需要大量内存和 CPU，并需要几分钟的时间。在分叉之后实施的第一批改进之一是采用 Zcash 核心开发团队正在开发的称为“Jubjub”的新“树苗 - sapling”。[16] 这种新“树苗- sapling”将显著提高采用 zk-SNARKs 加密币的隐秘交易速度和可用性。另一种改善 Bitcoin Private 隐私的方法是利用当前正在开发的“蒲公英 - Dandelion”隐私项目。[17] 这种技术涉及“stem”（交易）和“fluff”（混淆）。虽然任何混淆程序本质上都不如 zk-SNARKs 安全，但蒲公英混淆可以被添加到 Bitcoin Private 的透明和隐秘交易中，从而全面提高隐私性。

允许区块链的改进对于 Bitcoin Private 项目非常重要，为此，BIP9

已被纳入 Bitcoin Private 区块链以允许未来的软分叉以及改进。[18] 当用于改进的代码被完成后，矿工会被要求发出信号表示接受区块链代码更改。当95％的矿工接受这种改变时，更改就会被“锁定”，软分叉也就完成。但是，如果矿工在规定的时间内没有发出准备就绪信号，软分叉就会失败，代码改变不会发生。Bitcoin Private 项目的支持和发展将依赖于基金会来自矿池之外持续获取的资金。但是，Bitcoin Private 贡献团队强烈反对在没有民主投票赞成的情况下对其社区征收的任何形式的税收。因此，通过 BIP9 提出的早期改变之一将涉及基金会募款的条款。通过这种方式，矿工可以集体选择合适的金额作为捐赠，以确保项目未来的成功。

如第 2 部分所述，在分叉之后剩余可开采的 Bitcoin Private 数量较低可能导致一些问题，其中就包括极低的网络哈希率。一个可供选择的解决方案是通过 BIP9 的方式从该在网络上某些地方销毁未认领的硬币。如果通过 BIP9 选择了实施这种方式，那么在接下来的两年内每天都会有大约0.14％的无人认领的 Bitcoin Private 被销毁。在这种情况下，Bitcoin Private 将在所有相关钱包中被平均销毁，即：每个无人认领的 Bitcoin Private 钱包中将每天失去约其总量 0.14％的 Bitcoin Private，并持续 2 年。这种方法将为矿工释放大量的 Bitcoin Private 供挖掘，同时给用户足够的时间认领分叉出来的 Bitcoin Private。此外，每天低额的销毁率避免了对市场总值的冲击。

作为备份措施，Bitcoin Private 用和以太坊（Ethereum）类似的方式实施了一个“难度炸弹”，[19] 以便未来做出的重大改变。使用时，难度炸弹将应用于旧的区块链代码来提醒矿工采用新的代码以推进持续改进。这个方法是只会在极端情况下才使用的最后手段。比如，这个难度炸弹可以被实施来引入一个新的治理系统，例如、但不限于 Decred 所特有的系统。[20] 这将允许 Bitcoin Private 区块链进一步民主化和去中心化。目前，难度炸

弹日期定在 2019 年 3 月 2 日，但是可以用 BIP9 来无限期地延迟这个日期。

8. 商业应用

支付处理仍然是比特币今天最广泛的应用之一。2017 年，商家使用比如 BitPay 等比特币支付处理公司交易了可能超过 10 亿美元的比特币。这些比特币支付公司的钱包用户每个月储存了超过 10 亿美元的比特币资产，并且每月能产生 15 亿美元的钱包之间的比特币转账。[21] 就像互联网带来了一种革命性的新支付方式一样，加密货币也是如此。

消费者希望用价值换取商品和服务时获得一定程度的便利，这就是为什么网上支付已经司空见惯。在期望得到便利的同时，消费者也假设这些交易有一定程度的隐私保护。不幸的是，在过去的二十年中，有些实体通过跟踪在线信用卡交易来创建消费者的在线“档案”而获利。[22] 这非常具有侵略性，这也是为什么消费者想要用加密货币进行在线交易。然而在当前最流行的加密货币的技术设计中，消费者不应期望在这些区块链上获得这种隐私。[14] 但是，Bitcoin Private 可以通过 zk-SNARKs 交易满足消费者的隐私需求。

Bitcoin Private 将在数字资产的 P2P 和商业支付中发挥主要作用。它为商家提供一种经过测试、安全且被广泛采用的加密货币技术，并具有可被证明的匿名性和隐秘性。Bitcoin Private 有潜力在商业中应用到成百上千个使用场景。虽然其他采用 z 协议的加密币也可能实现这一作用，但它们都没有被用户选择或取得成功。这可能是由于隐秘交易的高 CPU 和内存要求；然而，‘Jubjub 树苗’的发布将允许移动端隐秘交易。Bitcoin Private 贡献团队强烈希望让加密货币被主流接受，从而实现广泛使用。因此，一个更对商家友好的隐秘交易服务将在新‘树苗’应用后的不久发布。

除了一般的网上商用场景，Bitcoin Private 移动钱包平台还可以应用于实体商业中通过透明和隐秘交易的方式存储和支付 Bitcoin Private。此外，这个平台可以被任何用户使用，并不仅限于商户。截至目前，已经有各类供应商和商家接触 Bitcoin Private 作为其商品的支付选项。这些商业交易的一部分可以被收费来注入 Bitcoin Private 基金，使基金会无需再通过挖矿的方式募集资金。

9. 社区主导项目

许多加密货币项目，无论是 Utility Token 还是加密币，都声称是社区驱动和开源的。虽然这在某种程度上是属实的，但这些项目通有一个核心开发团队完全控制整个项目的未来。在极少的例外中（如 Decred），社区对项目未来有实际的控制权，即使如此，这些开发团队通常仍然处于闭门工作状态。虽然社区成员可以对相应的代码提出修改建议，但这些请求可能会被忽视。Bitcoin Private 项目真正代表了社区的努力，目前有超过 100 个贡献者（2018 年 2 月 6 日），并且每天都在增长。

已经实施的各种举措将 Bitcoin Private 与其他社区加密币区分开来。例如，一个全球性的多语言 Bitcoin Private 大使计划已经启动，其中社区成员可以积极参与帮助推广 Bitcoin Private 并壮大社区。此外，Bitcoin Private 已经开启了任何人都可以申请的“开发者招募”计划，即使是那些区块链技术的新手，也能以有意义的方式为项目做出贡献。新手可以从这个开发者计划中学习并熟练掌握区块链技术/工程技术。这两项计划在几天内增加了一百多名新贡献者，将我们的日常贡献团队扩展到 300 多名成员。Bitcoin Private 贡献团队的规模表明该项目致力于社区主导的理念，在我们的团队看来这项成就是没有其他任何加密货币实现了的，这充分展示了 Bitcoin Private 开发真正的去中心化。

10. 结论

Bitcoin Private 是一个由多元化社区开发和维护的加密货币。来自全球各地的团队成员每天协作，使该项目取得成功。他们这样做是因为他们认同该项目实现了中本聪的最初愿景，即通过快速、低费、去中心化以及隐私实现金融自由。Bitcoin Private 对纳入 BIP9 软分叉提案的前瞻性将允许项目的进一步发展，如果届时证明 BIP9 无效，一个难度炸弹将用于推进替代治理方法。 Bitcoin Private 有无数的商业应用：从全球快速交易到在当地商店购物都可应用。比特币的巨大追随群体和 Zclassic 隐秘交易技术的合并将迎来一个可证明和无需信任的区块链隐私的新时代。

11. 感谢

我们要感谢矿工社区通过自愿矿工贡献计划提供的慷慨捐赠。我们还要感谢咖啡因分子，帮助团队渡过了许多漫长的昼夜；没有咖啡，这个项目是不可能成功的。我们也需要非常感谢杰出的开发团队 – 你们是我们所依赖的基础。最后，我们要感谢整个 Bitcoin Private 社区 – 你们是这个项目的中坚力量，如果没有你们，我们不会在这里。

12. 引用

[1] *Dutch Banks Tax Agency Under DdoS Attacks a Week after Big Russian Hack Reveal*. https://www.bleepingcomputer.com/news/security/dutch-banks-tax-agency-under-ddos-attacks-a-week-after-big-russian-hack-reveal/ (Accessed Feb. 5, 2018).

[2] The Biggest Data Breaches of the 21st Century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (Accessed Feb. 6, 2018).

[3] *What Chase and Other Banks won't Tell you about Selling your Data*. https://www.forbes.com/sites/adamtanner/2013/10/17/what-chase-and-other-banks-wont-tell-you-about-selling-your-data/#5eacaaf62c41 (Accessed Feb. 5, 2018).

[4] *Santander Totta has no Known Legal Basis to Block Bitcoin Related Transactions says Portuguese Consume Watchdog*. https://www.ccn.com/santander-totta-has-no-known-legal-basis-to-block-bitcoin-related-transactions-says-portuguese-consumer-watchdog/ (Accessed Feb. 5, 2018).

[5] Nakamoto S.; (2008) *Bitcoin: A peer-to-peer electronic cash system.*

6 *List of Cryptocurrencies.* https://cryptocurrencyfacts.com/list-of-cryptocurrencies/ *(Accessed* Feb. 5, 2018).

[7] *Premine Endowment*. https://bitcoingold.org/premine-endowment/ (Accessed Feb. 2, 2018)

[8] Brandeis, L.; Warren, S.; (1890) *The Right to Privacy*.

9"BitFury Group De-Anonymizes Over 15% of the Bitcoin ... - The Merkle." 11 Jan. 2018, https://themerkle.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-new-blockchain-analysis-tool/ (Accessed Jan. 30, 2018).

[10] Ben-Sasson, E; Chiesa, A; Garman, C.; Green, M,; Miers, I.; Tromer, E.; Virza, M. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin.

[11] *Interpreter.*cpp. https://github.com/BTCPrivate/BitcoinPrivate/blob/6b6abb3d121ba5231e5d775e9e2287dbbf76 87f6/src/script/interpreter.cpp#L1089 (Accessed Feb. 9, 2018)

[12] *Homa*kov, I. (2017) *Stop. Calling. Bitcoin. Decentralized*. https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27 (Accessed Feb. 4, 2018)

[13] Biryukov, A.; Khovratovich, D.; (2016) *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.*

Zcash - How zk-SNARKs works in Zcash. https://z.cash/technology/zksnarks.html *(Accessed* Feb. 3, 2018).

[14] *BTCP Developer Community, LLC Bylaws.* https://btcpfoundation.org/bylaws.pdf

[15] *What is Jubjub?* https://z.cash/technology/jubjub.html *(accessed* Feb. 1, 2018).

[16] *Bitcoin Developers Reveal Roadmap for 'Dandelion' Privacy Project* https://www.coindesk.com/bitcoin-developers-reveal-roadmap-dandelion-privacy-project/ (accessed Feb. 5, 2018).

[18] *BIP9*. https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki (Accessed Feb. 7, 2018)

[19] *What is the Ethereum Difficult Bomb*. https://themerkle.com/what-is-the-ethereum-difficulty-bomb/ (accessed Feb. 5, 2018)

[20] *Decred Documentation.* https://docs.decred.org/ *(Feb.* 1, 2018).

[21] *Bitcoin Transactions aren't as Anonymous as Everyone Hoped*. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/ (Accessed Feb. 5, 2018).

[22] *Google Now Tracks Your Credit Card Purchases and Connects them to its Online Profile of you.* https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchases-and-connects-them-to-its-online-profile-of-you/ (Accessed Feb. 5, 2018).

13. 重要披露及其他信息

本文中所有的内容均为原创并由 Bitcoin Private 研究和制作，除非另有表述。未经 Bitcoin Private 明确同意，本文内容的任何部分不得以任何形式被复制或在任何其他出版物中被引用。

本文仅供参考，并不构成出售要约、或试图在任何认为此类要约或招揽出售证券的活动属于非法的司法管辖区内征求购买或招揽出售任何证券。本文没有足够的信息来做出财务决策，文中包含的任何信息也不应被用于此类目的。本文不构成个人建议，也没有考虑到读者自身特殊的投资目标、财务情况或需求。读者应该充分考虑本文中的任何建议是否适合于他们的特殊情况，并在适当的时候征求专业意见或税务咨询。本研究中提到的加密货币的价格和价值、以及其带来的收入可能会有波动。过去的表现不是未来表现的指导，未来的回报不能保证，并可能发生本金的损失。汇率波动可能对某些投资的价值、价格或从中获得的收入有不利影响。在此提供的关于 Bitcoin Private 的信息并不打算用于、也不应被理解为或用作投资建议、税收建议、法律建议、推荐、出售要约或购买 Bitcoin Private 加密币的邀约。

此处包含的某些陈述可能是基于 Bitcoin Private 的观点和假设而做出的对未来的期望和其他前瞻性表述，其中包含已知和未知的风险和不确定性并可能导致实际结果、表现和发生的事件与在本文中的表达或暗示有重大差异。除了基于上下文的前瞻性表述之外，“可能，将、会，应该，可以，期望，计划，打算，预期，相信，估计，预测，潜在“以及类似的表达属于前瞻性表述。 Bitcoin Private 不承担更新任何包含在这里具有前瞻性的信息。虽然 Bitcoin Private 已经采取了合理的措施以确保本文所包含的信息准确无误，Bitcoin Private 没有表达或暗示过对本文的准确性、可靠性或完整性的陈述或保证（包括对第三方的责任）。