BULWARK

CRYPTOCURRENCY

加密电子货币白皮书

Bulwark 核心团队：

Eatbatterys（项目协调）

Jack（市场总监）

SerfyWerfy（区块链程序开发）

Frogman（通讯主管）

Patrick（品牌和设计）

Stu（生态系统开发）

Bulwark 核心团队

2017 年 12 月

我们，Bulwark 核心团队，确认本白皮书中提出的工作是我们原创。如果信息是从其它来源获得的，我们确保会注明。

摘要

Bulwark（股票代码：BWK）是一个社区导向的货币，通过观察主节点隐私货币空间内的一般不公平行为而诞生。我们商讨出的，公平的启动策略使参与者有机会在开始时加入一个有前途的项目。我们提供一个简单的价值主张，没有宏大的承诺：我们将通过利用来自 DASH 和 PIVX 的最佳实践，提供一个现在和未来都能蓬勃发展的隐私货币。没有幻想的愿景和有限的交付前景，而是一个支持未来在有实用性的平台上的实用的货币。这并不意味着我们不计划创新，相反，我们会提供结果而不是炒作。有太多的货币被炒作而疯狂——但是完全没有实质性的东西——我们也不想搅入这些货币的虚假增长中，虚高的承诺却无以兑现。由于没有 ICO，一个软启动的奖励提升过渡，少量预挖矿和利好矿工的奖励分配，Bulwark 的采用者将有一个具有底层访问权限的隐私货币所提供的主节点和当前最好的隐私货币技术的结合，同时有意义非凡的发展路线图。主节点将在发行时可用并运作，并且是这个货币的构想的基石，并将稳定流通性、保护网络安全性、并提供重要的功能。

致谢

如果没有比特币，Peercoin，Blackcoin，Talkcoin，Dash 和 PIVX 团队的先前杰出工作，Bulwark 将不可能实现。开源软件及其贡献者正在不断为新的和令人兴奋的创新铺平道路。当信息和知识可以自由发展时，整个社会就会受益。感谢我们的前辈让我们有机会为这个不断发展的生态系统做出贡献。

目录

第1章 加密数字货币简介

1.1 背景

在 2009 年，中本聪发表了一篇名为“*比特币：一个点对点电子现金系统*”的文章，详细介绍了他的开拓性构想。中本聪的构想详细介绍了一个基于哈希算法的工作证明支持的点对点货币系统。网络会将交易时间标记在一个持续进行的帐本，如果不重做工作证明就无法更改。由最大的哈希计算池见证，节点会选择最长的链作为事件的证明。只要网络哈希计算能力的≥51％不恶意攻击节点，它们产生的链将保持最长（中本聪，2009）。

1.2 区块

网络中的每个区块都有一个 80 字节的头部，头部包含前一个区块头部的双 SHA256 哈希副本，merkle 根（由在区块中发生的所有哈希计算的双 SHA256 哈希衍生），工作证明的时间戳开始，这个头部的哈希值必须小于或等于的，矿工们达到这个难度目标的随机数。因此，任何修改区块交易的尝试都将导致网络矿工们拒绝该区块（比特币核心团队，2017）。

1.3 区块链

交易组形成区块，这些区块按时间顺序排列成链——形成区块链。区块链创建了网络内所有活动的行进的历史记录，并作为分布式共识模型，在任何时候都可以验证任何交易（Crosby 等，2015）。

1.4 工作证明

工作证明是一个验证系统，在这个验证系统中，用户必须投入有形的资源（电力、硬件成本）来解决任意的概率*字谜难题*。如果一个坏人要通过欺诈交易来污染区块链，他们必须完成迄今为止的所有证明（Okupski，2016）。

第2章 Bulwark 简介

2.1 坚实的基础

每个家庭需要一个坚实的地基，Bulwark 也不例外。Bulwark 建立在 *PIVX* 之上，它本身是建立在流行的 *DASH* 加密电子货币上的。虽然谱系可以追溯到原来的中本聪核心，但每个项目都选择了一个特定的方向，其目标和理想代表了他们所服务的社区。我们将通过探索新技术来扩展并重视前辈平台的隐私功能，同时为 Bulwark 整合到当今的技术平台而创造工具包和机会。

2.2 一个致力于社区的团队

对于一些项目，社区是后来的想法。然而 Bulwark 的首要任务是服务社区。通过赠品、比赛、热烈的讨论平台和对新手骚扰的零容忍政策，Bulwark 努力成为各种终端用户的加密数字货币。我们的用户基础成员已经提供了有用的脚本和指南，以进一步增强用户体验。

2.3 公平和平衡

在写这篇文章的时候，涌入了一批依赖于相似基础的加密数字货币。虽然基础技术是坚实的，但是通常对其规范和区块链参数的深入检查会揭示其一些不公平的做法。

2.4 预挖矿的麻烦

2.4.1. 案例研究：FooBarBaz 币

加密电子货币领域的一个增长趋势是选择未来的一个任意日期，然后在当时的循环供应基础上设定一个预挖矿的百分比。让我们来看看一个 *DASH* 叉，虚构的 FBC（*FooBarBaz 币*）例子。

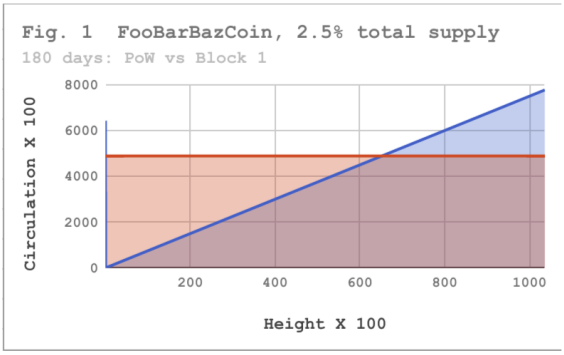
- 区块奖励：15
- 区块时间：2.5 分钟
- 工作证明/主节点分成：50/50%
- 初始难度算法：KGW
- 补贴每年降低 12%
- 最大货币供应量：约 2500 万
- 预挖矿 2.5%

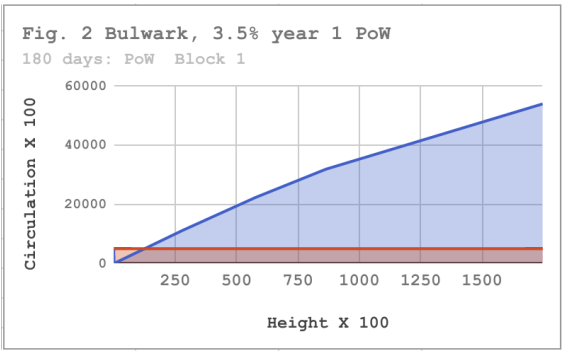
在这个例子中，粗略一看，宣传的 2.5%预挖矿相当于 643,000 个币（基于大约 2500 万总币量）似乎是合理的。然而，对于工作证明和主节点两者来说，都需要大约 43,000 区块才能抵上开发者所持的货币。在每个区块 2.5 分钟的目标下，矿工需要大约 150 天（或整体 75 天）才能生成相同数量的货币。75 天后，开发者仍然可以控制当时一半的总币量。

2.5 更公平的方案

Bulwark 团队认识到了这一点，并决定先发制人。我们预挖矿的 489,720 个币（3.5%），稍多于 12 天的工作证明挖矿量，或略多于 10 天的总产量。希望这样做能够使社区和平稳定，在一定程度上，市场不会因为核心团队所持有的币量而大幅贬值。从下列图中可以看出，每个场景均是 180 天，差别非常明显。我们希望以坦诚的态度来处理这个问题，开创先例，从而有利于整个社区。

2.5.1. 两种方案的比较





2.5.2. 瞬时挖矿和我们的方案

Dash（达世币）提供了一个对需要保护瞬时挖矿的有趣案例研究。在达世币启动的头几天内，由于一些富于进取的用户，几乎有 10-15%的达世币供应被创造出来（Wiecko，2017）。我们对瞬时挖矿问题的解决方案是双重的。我们利用了一个缓慢的补贴，其中前 960 个区块（1 天）线性地攀升到完整的区块奖励，当天 100%的区块奖励也都给于矿工。历史上，类似方案曾被应用过，即在某一区块高度，从一非常小的区块奖励突然跃升到完整的区块奖励，然而，这种方案往往导致矿池被故意的 DDoSed 或不勘重负于新矿工的流量。随着奖励的线性增加，试图干扰矿工或矿池运作者以获得金钱利益将失去意义。

2.5.3. ICO？更像 IC-NO！

让我们面对它，在写这篇文章的时候，我们一直在被质问关于 *ICO*。虽然它们在加密数字货币生态系统中拥有合法的地位，但往往它们只是为了创造集中的财富。考虑到 Bulwark 提供主节点奖励，而且在第二阶段进行利益证明奖励，这种财富集中可以引起巨大的市场波动，并且这种管理体系将严重利好最早（最富有）的采用者。虽然财富的集中是不可避免的，但我们相信只要有任何机会使游戏场保持公平，我们都将采取行动。我们推出了一个逐步攀升的区块奖励策略，一个公平的启动机制，以鼓励 Bulwark 广泛分布于众多用户，在理想的情况下，能避免一些在其它项目中看到的财富集中现象。

2.6 快速且实用

通过 90 秒的区块时间，主节点的共识和交易锁定，合理的发行时间表，以及对生态友好的股权分配，Bulwark 立志成为一个真正快速和实用的加密数字货币。

第3章 我们的区块链参数

3.1 Bulwark 参数一览

表 3.1： Bulwark 的参数一览

参数	描述
代码	BWK
算法	NIST5
RPC 端口	52541
P2P 端口	52543
区块间距	90 秒
难度算法	Dark Gravity Wave v3.0
区块大小	1MB
挖矿/挖矿成熟度	67 区块（约 100 分钟）
确认	6 区块（约 9 分钟）
流通（1 年）	14,505,720 BWK
流通（5 年）	27,668,220 BWK
工作证明时期	区块高度 ≤345，600
利益证明时期	区块高度 ≥345，601
协议支持	IPV4，IPV6，TOR
利益证明	Blackcoin v3.0 PoS，PIVX SeeSaw 奖励

3.2 慢启动

我们公平的启动提供了以下代码片段（借鉴于 *ZCash*）：

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {  //如果区块高度小于 480
    nSlowSubsidy /= 960;          // 将 nSubsidy 设为 .05208333
    nSlowSubsidy *= nHeight;      // 将当前区块高度乘以 .05208333
} else if (nHeight < 960 {// 例: 区块 200, BR 将是 10.41666600
    nSlowSubsidy /= 960;          // 致谢: ZCASH 团队
    nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave 3.0 从一开始就被 Bulwark 用作重新定义工作证明的难度的一种方法。它使用了一个简单的移动平均方法，可以在几个区块内响应大幅的网络哈希算力增长或下降。这样可以缓解经常由于多个计算池引起的“区块卡住效应”，并能防止一个人通过增加大量的计算能力而立即求解多个区块。

第4章 区块奖励

4.1 工作证明（PoW）的区块奖励

表格：工作证明时期的区块奖励参数

补贴	区块	工作证明	主节点	流通
489720	1	100%	NA	489200
约 25（平均）	2-960	100%	NA	513150
50.000	961-28800	80%	20%	1953150
50.000	28801-57600	75%	25%	3393150
50.000	57601-86400	66%	33%	4833150
43.750	86401-172800	50%	50%	8613150
37.500	172801-2 59200	50%	50%	11853150
31.250	259201-345600	50%	50%	14553150

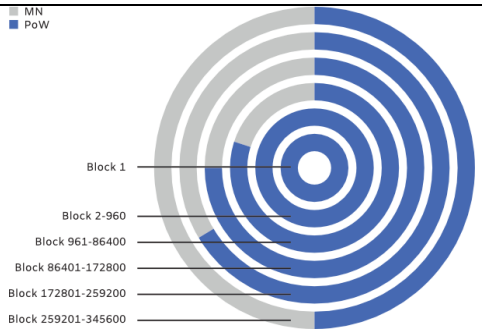


图 4.1：工作证明时期的区块奖励

4.2 利益证明（PoS）时期的区块奖励

表 4.2：利益证明时期的区块奖励参数

补贴	区块	预算	利益证明/主节点	注释
25.000	345601-432000	10%	SeeSaw	第 2 年
21.875	432001-518400	10%	SeeSaw	第 2 年
18.750	518401-604800	10%	SeeSaw	第 2 年
15.625	604801-691200	10%	SeeSaw	第 2 年
10.250	691201-777600	10%	SeeSaw	第 3 年
10.938	777601-864000	10%	SeeSaw	第 3 年
9.3750	864001-950400	10%	SeeSaw	第 3 年
7.8120	950401-1036800	10%	SeeSaw	第 3 年
6.2500	1036801-1123200	10%	SeeSaw	第 4 年
5.4690	1123201-1209600	10%	SeeSaw	第 4 年
4.6880	1209601-1296000	10%	SeeSaw	第 4 年
3.9060	1296000-1382400	10%	SeeSaw	第 4 年
3.1250	1382401-1468800	10%	SeeSaw	第 5 年
2.7340	1468801-1555200	10%	SeeSaw	第 5 年
2.3440	1555201-1641600	10%	SeeSaw	第 5 年
1.9530	1641601-1728000	10%	SeeSaw	第 5 年
1.6250	1728000+	10%	SeeSaw	永久

第5章 NIST5 哈希计算

5.1 为什么选择 NIST5

TalkCoin 在 2014 年流行，NIST5 哈希算法有适度的主流使用率。NIST5 可以在广泛的消费级硬件上开采，包括 CPU，以及 AMD 和 NVidia GPU。NIST5 不像其他一些内存硬件算法那样对 ASIC 有强抵抗性，但是我们相信，相对于那些高内存需求的算法，此折衷是可接受的，以提高系统稳定性和降低功耗。如果在我们的工作证明时期结束之前，出现了支持 NIST5 的 ASIC 硬件更新，那么我们准备切换为另一种算法。我们会组织一次社区公投来决定应对方案（如果有的话）并相应地执行。我们觉得我们短暂的工作证明时期和切换算法的意愿，会使 ASIC 制造商望而却步，从而我们并不预期会有问题。

5.2 五个入围者（NIST SHA-3 之争）

构成 NIST5 的五个哈希算法是 NIST 哈希算法之争的入围者（Chang 等，2012）。它们（按照区块被哈希计算的顺序）：

Blake（Aumasson，2013），**Grøstl**（Gauravaram1 等，2012），**JH**（Wu，2012），**Keccak**（Bertoni 等，2012）和 **Skein**（Ferguson 等，2010）。

5.3 新的 SHA-3 标准

Keccak 最终通过了最后一轮被命名为新的 SHA-3 哈希计算函数，而另外四个算法（尽管也被认为是加密安全的）由于一些小的技术问题而被裁判失了几分。我们相信新的 SHA-3 标准与其它入围算法选择的结合提供了一个快速、安全和公认的哈希算法。

5.4 可用的挖矿软件

在本文成写作时，矿工有几种选择：

名称	平台	链接
SGMiner-5.0	OpenCL	
ccminer-2.2.2	CUDA	
cpuminer-opt	CPU	

第6章 功能集合

6.1 主节点

主节点本质上是一个服务于 Bulwark 网络的分布式的网络计算机。主节点执行重要的网络功能，并获得部分区块奖励。它们通过稳定货币供应、处理交易和保护网络安全来服务于 Bulwark 生态系统。主节点需要 5000 BWK 和适度的技术知识来运作。任何控制 5000 BWK 的钱包都可以设置一个主节点。

6.2 模糊化/货币混合

Bulwark 的具有模糊化功能，基于 CoinJoin，但在原来的基础上有重大改进，并通过由主节点网络促进，分布式的混合货币完成。这为交易提供了附加的隐私层。尽管不是完全匿名的，但通过节点混合实现的模糊化远远好于标准的比特币交易。例如，所有比特币交易都是透明的。对于 Bulwark 来说，一个邪恶角色需要控制 50%的运行的主节点，才有不到 0.5%的机会来对一个与经过 8 轮模糊化相混合的单一交易进行去匿名化（Kiraly，2017b）。这一重要功能为选择模糊化交易的 BWK 用户提供了高级匿名性。

6.3 SwiftTX

SwiftTX 为交易提供了具有锁定和共识权限的主节点。当一笔交易提交到网络时，一组主节点将验证交易。如果这些主节点在交易的有效性上达成一致，那么它将被锁定，以便随后被引入到交易区块链中，与传统系统相比（例如比特币的具有多次确认的 10 分钟区块时间），交易速度大大提高。SwiftTX 使得在网络中的一个具有相同输入的区块被挖到之前可以进行多笔交易。这个系统是基于达世币的 InstantSend（Kiraly，2017a）。

6.4 Sporks

Bulwark 网络使用被称为“sporking”的多相分叉机制。这将使 BWK 网络能够实现新功能，同时最大限度地降低在部署期间发生意外网络分叉的可能性。Spork 的更改可以通过网络部署，并且可以根据需要打开和关闭，而无需节点软件更新（strophy,2017）。此功能非常有用，可以使网络对安全漏洞迅速作出反应。

6.5 TOR 和 IPV6 主节点

Bulwark 允许用户从洋葱地址或 IPV6 地址运行完整节点或主节点。我们一直在努力增加完整的 TOR 节点以加强 TOR 网络本身，和在 TOR 模式下运行 Bulwark 的用户体验。TOR 主节点支持的独特功能是能够将你的主节点作为 TOR 隐藏服务进行运行。TOR 节点使得具有稳定的互联网连接的用户从家庭网络运行主节点，而没有隐私影响或暴露他们的位置或者将他们的家庭网络暴露于潜在的攻击或危害的危险中。

6.6 社区的重要性与管理体系

Bulwark 社区是项目长期成功背后最重要的因素，它们有意义地影响货币未来的能力是至关重要的。因此，在工作证明阶段结束时，我们打算在网络上激活预算超级区块。这些超级区块，每月发放，将使社区能够对 Bulwark 的发展、品牌形象和社区事务的各个方面施加有意义的控制。延迟这个系统的激活将使我们有时间开发积极的用户体验所必需的底层框架，并最大限度地提供给矿工和主节点区块奖励。

我们将利用多阶段流程来创建和提交建议。每一步都需要全面完成。未能完成概述的步骤可能会导致一个提案未被激活。这些步骤的基本概述如下：

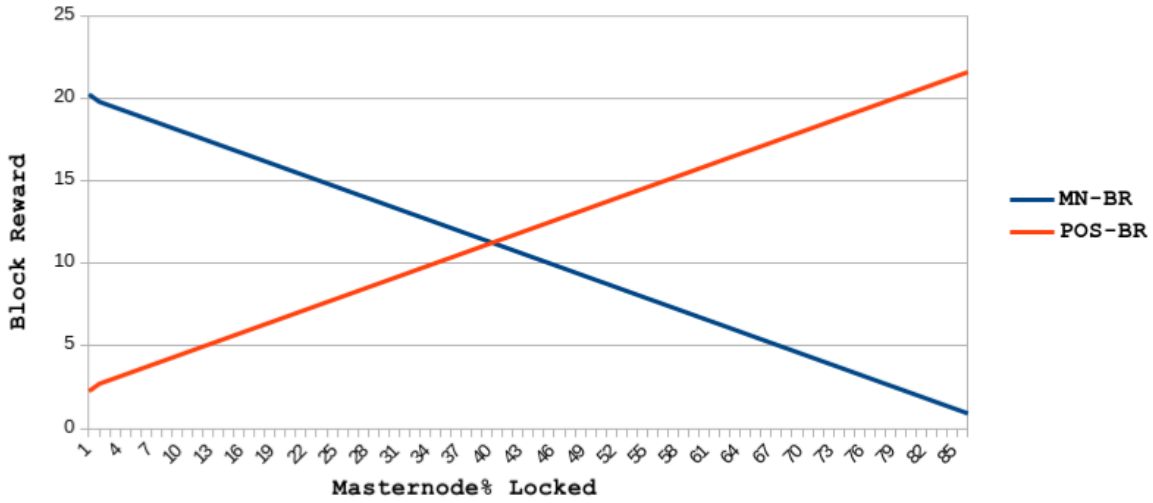
- 开始我们的 Discord 聊天，并与一些经验丰富的用户交谈。衡量利益，如果反应是肯定的，则进入下一个阶段。
- 利用多个社交媒体平台进行讨论并获得反馈。请记住 Bulwark 具有广泛的用户基础和不同级别的管理参与，达到一定的用户基础往往需要一些策略。记录这些讨论，并能够在正式的提案中引用它们。提供的引文越多越好。
- 接受社区和开发者的建议。要有灵活性，并愿意将外部想法和建议纳入你的提案中。
- 在我们网站的管理->预提案部分创建一个正式的预提案。提供在上一步中发生的所有讨论的引用。把你的预提案视作是将提交给区块链投票的终稿。
- 完成这些步骤后，你将提交你的提案到区块链。准备两个费用，一个是提交时，另一个是支付给开发者的投票费，以激活您在区块链上的提案。提交费不可退还，而投票费仅在你的提案获得批准和激活后才支付。
- 每个人都可以自由调整他们的建议包括这两个费用的报销支出。请确保在你的正式提案中声明你所要求的补贴中加入了报销部分。
- 请务必与你谈过话的每个人保持联系，这样你的想法将被投票。如果一个提案要被支付，10%的合格主节点必须对你的提案投赞成票。获得 10%共识的过程可能比听起来要困难得多，所以为了获得你的提案被支付所需的投票时要勤勉、信息丰富并且恭敬。

6.7 SeeSaw 利益证明（PoS）/主节点（Masternode）奖励

我们决定利用 PIVX 推广的 SeeSaw 奖励系统（jakiman，2017）。SeeSaw 奖励系统以 9：1 的区块奖励比例（有利于主节点）开始，并平稳地调整股权分配和节点运作者之间的奖励比率，直到流通中的货币的 41.5%被锁定在主节点中，此时利益分配奖励达到在逐个货币的基础上比主节点奖励略有优势。我们将 SeeSaw 稍微有利于利益分配奖励是因为我们想要避免像价格波动大和流动性低的问题，这些会影响流通供应中非常高比例的货币被锁定在节点上的币种。这一策略将缓解用户对货币供应的挫折感，并保持我们健壮的网络相关性。由于我们的目标之一是支持匿名交易的平台，可交易性对接受 Bulwark 和持有 Bulwark 的人来说非常重要。

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



第7章 未来

7.1 Bulwark 工具箱

一个代码片段、API、库、脚本和知识的集合将有助于鼓励类似市场的环境，开发者可能希望在其项目中添加加密电子货币支持，从而可以自由地交换知识、信息和代码。我们相信，为开发者提供这些工具相似于为木匠提供他们所需的工具，从而创建出令人兴奋和卓越的项目。

7.2 隐私和软件增强

我们致力于采用新的协议来增强我们用户的隐私。目前我们正在评估几条路径，计划在 2018 年上半年开始内部测试和开发。其中一些增强功能包括：

- I2P 隐私网络。
- Zerocoin 协议或隐形寻址（当我们对解决方案的成熟性有信心的时候）。
- 与比特币主线更紧密地同步我们的代码库。
- 简化/更新 QT 钱包。
- Libtox 集成。
- Bulwark 钱包的虚拟化/集装化增加了额外的安全层。

7.3 Bulwark 安全家庭节点

我们将与 CAD 专家一起设计一个小型的，独立的家居 Bulwark 节点。用户将能够将其连接到他们的家庭网络，并使用 Web UI 进行配置。我们打算推出的功能如下：

- 对于具有稳定的互联网连接的人来说，使用 TOR 隐藏服务可以很容易地建立完全的洋葱化主节点（或全节点）。
- 作为中继站来改善整个 TOR 网络的选项。
- 通过 TOR/I2P 网络进行路由，VPN 和/或代理可用于家庭互联网流量。
- Bulwark 通过虚拟化或附加设备进行连接。

为了与分布式精神保持一致，3D 打印文件和所有源代码将可用于社区中的家庭组装。

7.4 我们的品牌延伸

我们将继续扩大我们的品牌，并打算与硬件厂商和系统集成商一起工作，这些厂商和系统集成商和我们一样拥有同样的激情和理想。五年来，我们希望“Bulwark”这个名字不仅仅是加密数字货币，而是隐私、安全和尊重用户的自由。Bulwark 的主要目的是通过隐私提供选择的自由。

7.5 设计和视觉

通过研究和开发，我们的目标是为 Bulwark 打造一个视觉设计语言，使其与加密数字货币市场的竞争区别开。我们的设计团队计划创新并尝试当前的 UI/UX/Branding，最终通过搜索能够提供最佳用户体验与创新和美观的美学媒体来实现卓越的设计。这将通过研究我们的竞争对手，保持当前的技术趋势和标准，不断努力为最终用户带来新的和令人兴奋的视觉效果来实现。

第8章 结论

8.1 概要

Bulwark 是一个隐私导向的货币，具有主节点，管理和不断发展的工具生态系统。该项目始于公平发行，并以广泛的货币分配为重点。有意识地选择了慢启动、区块奖励分成和哈希算法，为重要的社区参与创造机会。并以现有技术为基础，Bulwark 推出了各种重要的隐私货币功能，开发团队正在努力推出新功能。Bulwark 旨在通过隐私而赋予选择权，并将集中精力于此。

8.2 未来的工作

主节点隐私货币生态系统最近被各种加密数字货币所淹没，它们试图吸引新的用户而承诺丰厚的投资回报，巨大的路线图充满了不可能的交付项目，以及一般聚焦于市场营销而非实际的改善。Bulwark 计划是相反的：低炒作和高实际创作。本项目的当前和未来目标将遵循具体、可测量、可实现、相关和有时间限制的公式。

参考文献：

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Available at: .

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Available at: .

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: .

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the sha-3 cryptographic hash algorithm competition. Available at: .

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: .

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Available at: .

Gauravaraml, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Available at: .

jakiman, 2017. PIVX purple paper. Available at: .

Kiraly, B., 2017a. InstantSend. Available at: .

Kiraly, B., 2017b. PrivateSend. Available at: .

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Available at: .

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: .

strophy, 2017. Understanding sporks. Available at: .

Wiecko, R., 2017. Dash instamine issue clari cation. Available at: .

Wu, H., 2012. The hash function jh. Available at: .