



Galileel

第一种具有混合共识算法的通用加密货币，
Zerocoin动态权益证明，交易证明和主节点投票，
以周期为基础的奖励燃烧投票

白皮书 V1.11

迈克 布罗梅¹, 十一月 2019



目錄

摘要	3
介绍	3
伽利略币 (Galileel Coin)	3
问题和解决方案	4
Zerocoin动态权益证明 (dzPoS)	4
交易证明 (ghPoT)	6
混合证明 (ghPoS)	7
定期存款 (gTD)	9
货币供应控制 (gMSC)	10
即时主节点奖励 (gIOMN)	12
特点和规格	13
競合分析	17
发展路线图	19
帮助	20
重要鏈接	21
附录	22



摘要

虽然法定货币已经定义并证明了数百年的经济标准，但数字货币的情况却不同。数字货币是一种具有不可预测价值的高风险投资，而且不断消失的开发团队放弃的大量区块链项目。政府发现了这个问题，初始硬币发行（ICO）法规将在未来几年内解决。此外，具有独特区块链特征的数字货币很有可能脱颖而出从而定义未来的数字货币标准。Galilel将通过实施本白皮书中概述的其独特功能并参与此过程。

介绍

伽利略币Galilel Coin是一个社区驱动的加密货币，具有完全透明性并利用开源的开发方式。投资者与项目团队之间的信任关系是成功的关键。因此，我们创建了一个名为 *Galilel-Project*² 的GitHub组织，该组织跟踪公共存储库中的所有开发活动，包括我们的所有后端代码，并通过了*Know Your Developer (KYD)*³ 公共验证。该项目主要使用 *MIT*⁴、*GPLv3*⁵ 和 *CC-BY-NC 4.0*⁶ 开源和开放内容许可。翻译和本地化使用 *Transifex*⁷ 平台。

伽利略币 (GALILEL COIN)

Galilel Coin (GALI和zGALI) 是一种开源的公共和私人的交易权益Proof-of-Stake数字加密货币，用于快速（使用SwiftX），隐私（ZeroCoin⁸ 协议）和安全的微交易。我们的主要目标是创建一个去中心化的完全安全和匿名的网络来运行应用程序，这些应用程序不依赖于任何中央主体控制。通过使用分布式系统，数千名用户将负责维护应用程序和数据，从而不会出现单点故障。



问题和解决方案

区块链技术炒作产生了巨大的兴趣，在全球范围内受到欢迎，许多公司在数字货币之外还用于不同的使用目的。但是，使用它作为支付服务的基础需要特定功能以验证，存储和验证数千个交易。虽然已经使用现有的一致性的算法来解决这一问题以在链中生成区块，但是在当前的区块链实现中存在若干弱区域以实现数字货币的主流采用。

ZEROCOIN动态权益证明 (dzPoS)

Zerocoin Proof-of-Stake (zPoS) 是PIVX开发团队于2018年推出的最具创新性的区块链功能。但是，技术实现以区块链的特定方式完成，并且不允许轻松采用其他人，因为他们的奖励结构静态地包含在源代码中。

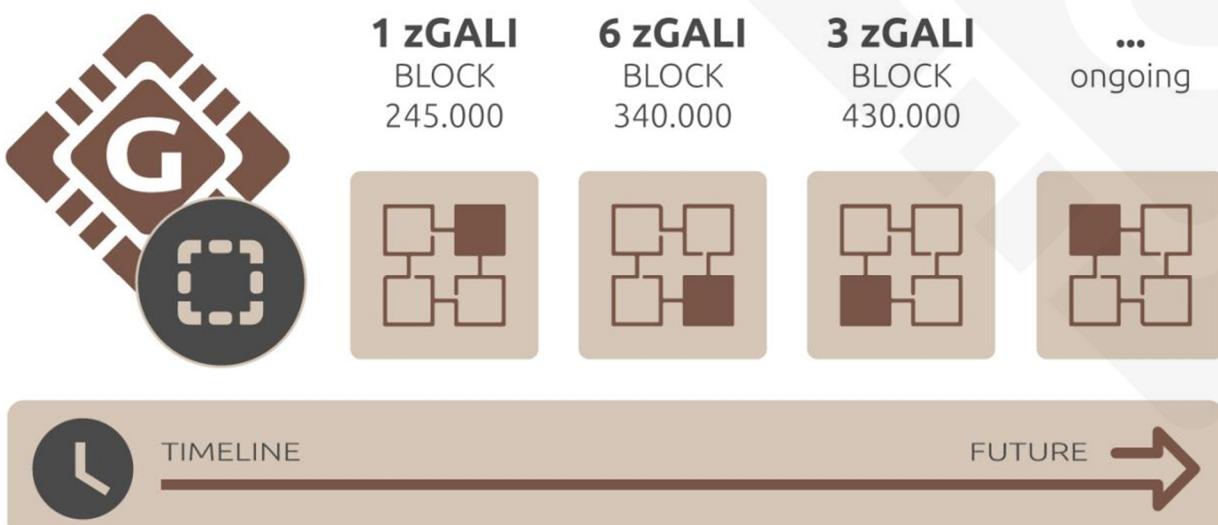


圖1.區塊鏈階段的Zerocoin 动态权益证明獎勵。

在Galileel，我们应用了Zerocoin权益的动态版本。Zerocoin权益 (Zerocoin staking) 以面额表示奖励，表示整数值。最小可能的面额是一 [数字1]。在第一个版本 - 预热阶



段 - 我们总是使用最小面额值进行测试。这种方法的缺点是Zerocoin权益导致是CPU使用十分紧张，并且生成孤块的可能性更高，因为公共硬币权益可以往后处理区块，但是更早地将其分配到区块链。在第二个版本 - 完整阶段 - 我们根据块奖励金额自动确定最佳面额结构。这能显著降低了生成孤块的可能性。



交易证明 (ghPoT)

在传统经济学中，银行账户之间有资金转账，可以指定一个主题，以便收款人可以将金额分配给特定发票。在当前的钱包实现中是不可能的。它允许指定注释或注释值，该值不是事务的一部分，只存储在本地。要将发票分配给特定收款人，必须创建一个钱包地址，并在两个利益相关者之间进行一对一映射。

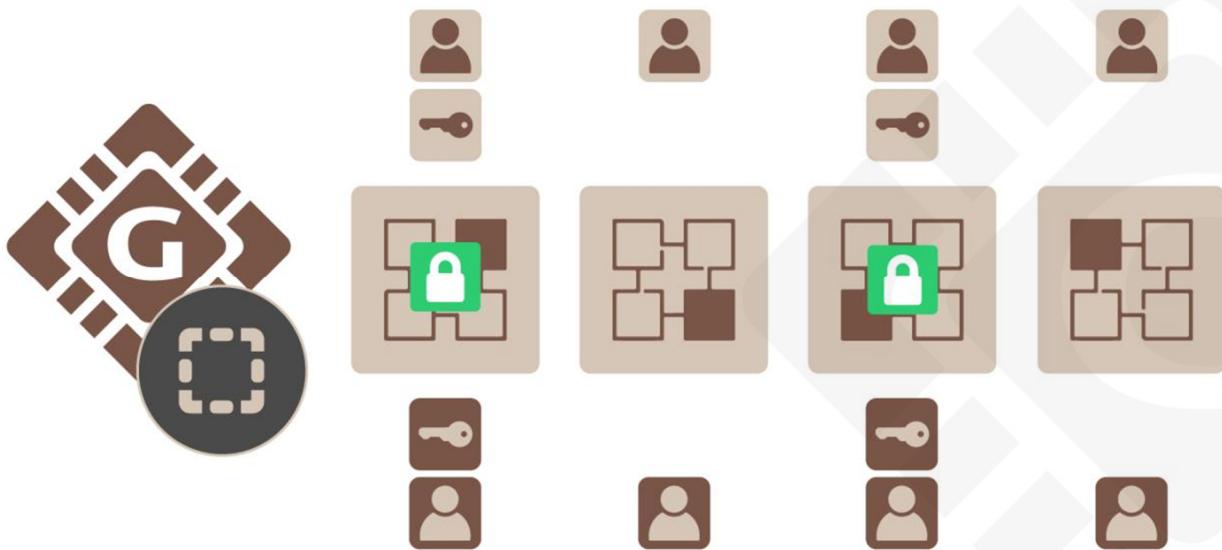


圖2.加密主題的交易證明。

在Galilel中，我们包含一个附加数据字段并将其附加到事务中，该事务存储在块中。它是一个加密字段，只有通过协商交易的钱包才能进行解密。它解决了交易分配问题，并允许支付处理网关识别发票的收款人，就像传统的法定发票一样。



混合证明 (ghPoS)

虽然Proof-of-Stake (PoS) 是一种环保的一致性算法，但只要桌面钱包正在运行，它就会产生奖励。此问题的一个解决方案是注册任何共享的Proof-of-Stake池并放入云 (cloud) 中。然而，缺点是用户需要信任POS的池并将特定数量的硬币转移给它。它可能导致大量硬币存放在几个钱包中的情况。对于去中心化的网络方法而言，这是比较薄弱的一面去是达成共识的基本部分。权益证明，即所谓的ZeroCoin Proof-of-Stake (zPoS)，具有相同的问题和局限性。

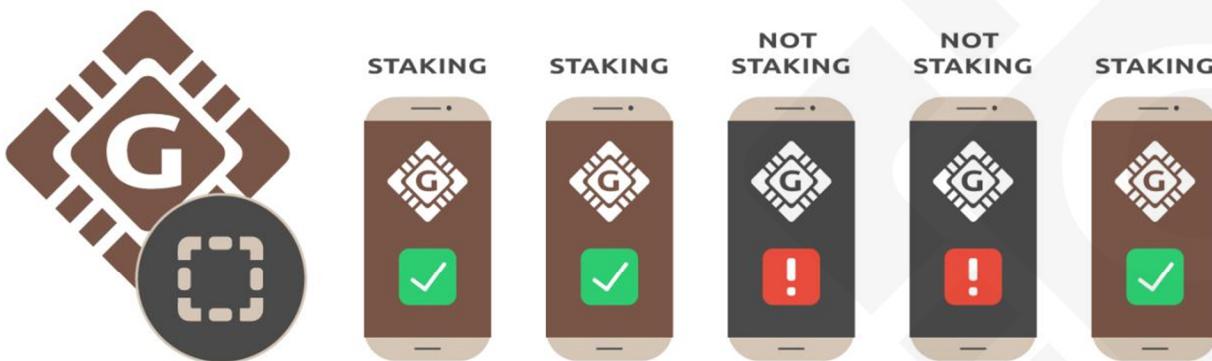


圖3.從Galileel網絡獲得獎勵的可能方式。

在Galileel，这个问题的解决方案将是一个名为Galileel Hybrid Proof-of-Stake (ghPoS) 的完全混合共识算法。我们将通过移动staking功能扩展Proof-of-Stake，用于公共和私人staking。如果移动设备的钱包找到块，移动设备staking会总是以在TEN [10] 百分比的块奖励支付。在这种情况下，九十[90]百分比支付给masternode持有人。移动钱包将作为区块链的轻节点工作，并且最小块数等于重组深度。



混合权益证明奖励结构

STAKING 类别 ¹	STAKING	MASTERNODE
电脑Online (GALI)	30%	70%
电脑Online (zGALI)	60%	40%
移动设备Mobile (GALI)	10%	90%
移动设备Mobile (zGALI)	20%	80%

¹ 其计算基於5 GALI獎勵 > 塊 430,000



定期存款 (gTD)

虽然移动赌注取决于网络难度和staking的硬币数量，但 *Term Deposit*⁹功能允许锁定硬币一段时间并产生奖励。

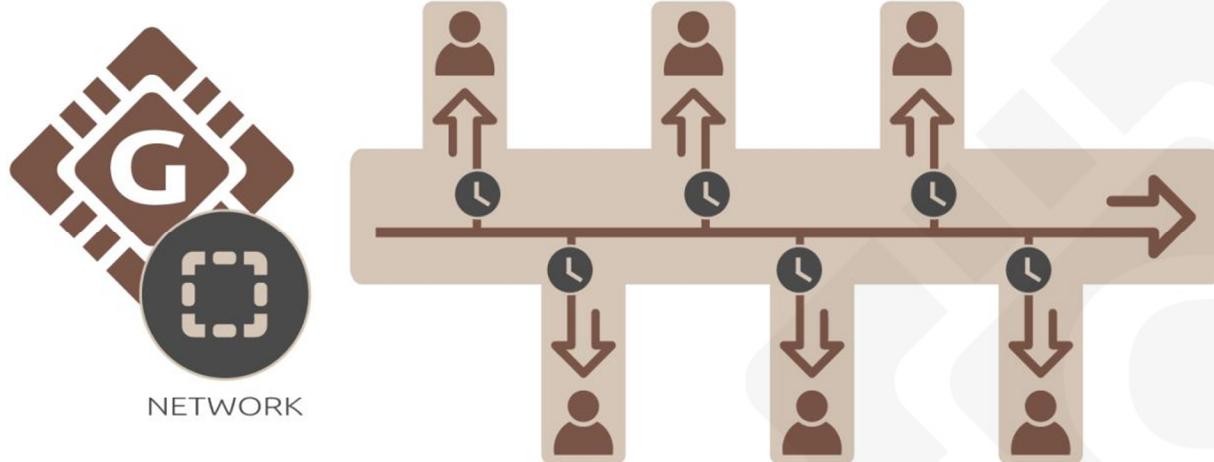


圖4.離線錢包中基於歷程表的定期存款。

使用Galileel定期存款 (gTD) 所需的最低硬币数量是五千[GALI]。锁定期为一年[1]年。块奖励是TEN [10]%，并且不同钱包的锁定硬币被加权。随着网络中的新块，带有锁定硬币的钱包根据其份量获得金额。在定期存款期结束之前，此奖励被锁定。一旦锁定，移动其硬币或花钱购买是不可能的，在到期时间之前取消定期存款也是不可能的。这将有效地减少锁定期间的硬币供应。



货币供应控制 (gMSC)

通货膨胀控制是数字货币被认可和接受作为法定货币的替代品中最具挑战性的部分。没有任何控制机制，任何数字货币的价值都是不可预测的。这导致投资者开始押注价值的情况（囤积），这可能会在数小时内严重损害市场，并立即消除将数字资金推向市场的可能性作为公认的支付选项。通过控制通胀，我们相信数字货币领域之外的人们会被吸引使用它，因为没有必要每天都在他们的投资组合中寻找。与法定货币的中央银行不同，没有观察和维持货币供应的中心位置。在Galileel，我们实施了一种分散的方法来刻录硬币，即私人和公共放样硬币的所谓燃烧证明proof of burn¹⁰机制。虽然这是控制货币流通的必要步骤，但主节点所有者有可能投票减少奖励或在特定时期内完成燃烧以减少硬币生成。

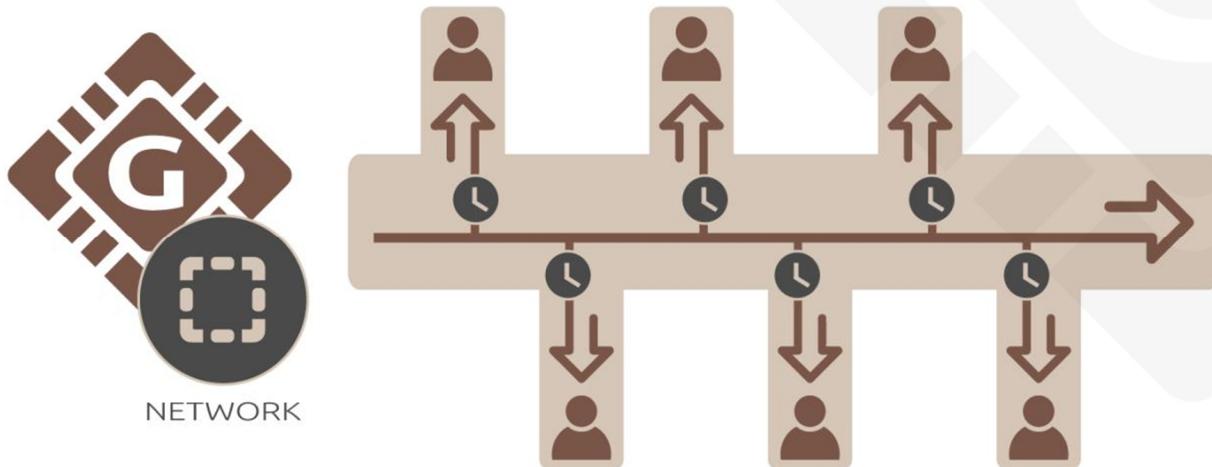


圖5. Masternode投票減少獎勵的產生。

我们将它命名为Galileel Money Supply Control (gMSC)，有效地使用了燃烧证明。这种机制只会带来奖励，而不是定期存款和发展预算。硬币燃烧的时间将是一个月[1]个



月，按照奖励燃烧结构表中描述的步骤减少年度供应量。主节点持有者每月适用于投票。该提案可以每月进行一次，从当前奖励燃烧期结束前一周开始。区块链接受从一千 [1000] GALI开始的任何提案。一旦在区块链中分发提案，主节点持有者就可以投入额外的一[1]或更多GALI投票。在提案期结束后，具有最高金额和超过五十[50]%主节点投票的提案将获胜。如果提议期限结束并被接受，则锁定在提案中的硬币将被刻录，奖励燃烧期间从下一个刻录块开始。如果未达到提案接受的最低要求，则锁定的硬币将被解锁。

燃烧奖励结构

燃烧比例	每月燃烧数量 ¹
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

¹ 其計算基於5 GALI獎勵 > 塊 430,000



即时主节点奖励 (gIOMN)

主节点在数字金钱领域已经获得了很大的吸引力。虽然许多新的数字加密货币试图创造一个荒谬的高投资回报 (ROI) 硬币并且在硬币通胀开始之后失败以及在主节点和赌注之间具有不平衡的奖励分配，但这不是运行主节点的主要目的。在Galilel中，主节点的主要用例是保护网络，同时有机会对未来的开发方面进行投票以及维护硬币流通。但是，可用主节点实现的主要弱点是要求在作为主节点的每台机器上同步和索引区块链。

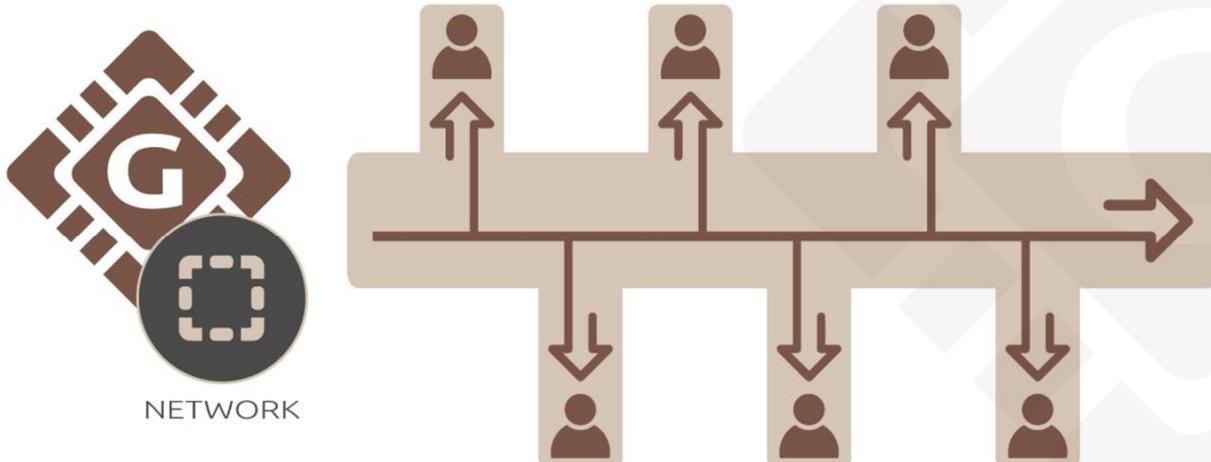


圖6.連接到雲中單個區塊鏈的多個主節點。

加利略Galilel的主节点奖励机制 (gIOMN) 通过实现共享区块链在客户端 - 服务器模型中运行 *one-to-many*¹¹ 钱包守护进程来解决此问题。它与 *Electrum*¹² 客户端中提供的“即时”模型相当。



特点和规格

硬币规格

货币名称	(伽利略) Galileel
货币缩写	GALI
算法	Quark
共识算法	PoS + zPoS 混合
区块大小	2 MB
区块时间	60 秒 (重新定位每块)
RPC 接口	36002
P2P 借口	36001
挖掘形式	PoW / PoS / zPoS / MN
最低 Staking 时间	2 小时
成熟时间	120 个确认
合格转送	6 个确认
奖励 (直至区块高度 1,500)	MN 60%, PoW 40%
奖励 (直至区块高度 205,000)	MN 60%, PoS 40%
奖励 (直至区块高度 205,001)	MN 70%, PoS 30%
最后 PoW 区块	1,500
Masternode 抵押	15,000



最大硬币供应 (一月 2020 January 2020)	19,035,999 GALI
最大硬币供应 (一月 2030 January 2030)	45,315,999 GALI
最大硬币供应 (一月 2040 January 2040)	71,595,999 GALI
最大硬币供应 (一月 2050 January 2050)	97,875,999 GALI
动态 硬币供应	交易费用& zGALI 挖矿费用将被烧毁
社区捐赠地址	<u>UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX</u>
开发预算 (由块 250,001)	10% 每月超级区块



ZEROCOIN 规格

Zerocoins v1 激活	块 245,000
Zerocoins v2 激活	块 245,000
zGALI 自动挖掘	10%
zGALI 奖励 (由区块 245,001)	1 zGALI
zGALI 奖励 (由区块 340,001)	MN 40%, zPoS 60%
zGALI 奖励 (由区块 430,001)	MN 40%, zPoS 60%
zGALI 分母	1, 5, 10, 50, 100, 500, 1000, 5000
蓄能器模数	RSA-2048
成熟	240 确认
合格转送	20 确认
费用 (挖掘)	每一个GALI需要0.01费用
费用 (使用)	免费



工作证明衰变

区块高度	奖励	MN	POW	供应	周期	阶段结束
块 1	220,000	60%	40%	220,000	0 天	2018-05-25
块 2 – 1,500	1	60%	40%	221,499	1 天	2018-05-26

权益证明衰变

阶段	区块高度	奖励	MN	POS	供应	周期	阶段结束
阶段 1	1,501-12,000	100	60%	40%	1,271,399	7 天	2018-06-02
阶段 2	12,001-22,000	90	60%	40%	2,171,309	7 天	2018-06-09
阶段 3	22,001-42,000	80	60%	40%	3,771,229	14 天	2018-06-23
阶段 4	42,001-100,000	70	60%	40%	7,831,159	40 天	2018-08-02
阶段 5	100,001-160,000	60	60%	40%	11,431,099	42 天	2018-09-13
阶段 6	160,001-205,000	50	60%	40%	13,681,049	31 天	2018-10-14
阶段 7	205,001-250,000	25	70%	30%	14,806,024	31 天	2018-11-14
阶段 8	250,001-340,000	13.5	70%	30%	16,156,009	62 天	2019-01-15
阶段 9	340,001-430,000	10	70%	30%	17,055,999	62 天	2019-03-18
阶段 X	430,001-ongoing	5	70%	30%	不断	不断	不断



競合分析

每天都有新的数字加密货币项目诞生，主要是针对特定目的的服务货币。虽然这是一个有效的方案，但它将硬币的使用情况限制在特定的市场和规模。最后，它限制了货币价值。加密货币市场共享相同的特征集，具有不同数量的数字货币和不同的块奖励，是过度饱和的。在过去，一些具有独特想法和光明未来的项目诞生了。Galileel将继续这一趋势并改进用于数字货币的區塊鏈，同時構建易於使用的通用加密貨幣，以便在市場上大規模採用。



功能	GALILEL	DASH	PIVX	ROI COIN
	伽利略	达世	普罗	
公共 Staking	✓	✗	✓	✗
私人 Staking	✓	✗	✓	✗
即时 转送	✓	✓	✓	✗
私人 转送	✓	✓	✓	✗
Masternodes	✓	✓	✓	✗
去中心化治理投票	✓	✓	✓	✗
可變獎勵分配 ¹	✗	✗	✓	✗
动态 Zerocoin 权益证明	✓	✗	✗	✗
交易证明	✓	✗	✗	✗
可变奖励燃烧	✓	✗	✗	✗
非连线区块链	✓	✗	✗	✗
移动设备权益证明	✓	✗	✗	✗
定期存款	✓	✗	✗	✓

¹ 可以使用Seesaw算法在Galileel中實現



发展路线图

Galileel Coin的发展对于未来的区块链至关重要。有些代码已经编写完成并且正在进行内部测试。 Galileel Instant On Master节点 (gIOMN) 功能接近完成，而Galileel的混合证明Hybrid Proof-of-Stake (ghPoS) 在块245,000计划的Zerocoin v2激活后需要额外的开发和测试周期。我们的路线图仅包括开发项目;我们认为有必要确定适当的目标，期望和可交付成果，而不是将精心调整的营销项目纳入其中。

- 2018年第二季度 - Fork PIVX代码库并启动MAINNET。创建Discord¹³ 频道做为社区投票并在BitcoinTalk¹⁴ 论坛中做预先的公告。
- 2018年第三季度 - 在第一个交易所和排名网站上市。实施关于奖励分配，奖励结构修改和主节点抵押的社区投票结果到v2.0。设计团队为应用程序开发人员创建Galileel品牌和网站，其中包含品牌颜色，徽标和品牌指南。除了开发和设计，我们还将通过Know Your Developer (KYD) 公开验证。
- 2018年 - 启用并发布TESTNET，使开发人员能够测试新的区块链代码和用户以测试前沿功能。将Galileel代码库重构为最新的PIVX 3.1.1源和版本v3.0，在块245,000处使用Zerocoin v1和v2激活，并使用分散式自治组织 (DAO) 进行区块链投票，同时保持区块链和网络向后兼容。启用Zerocoin Stof-of-Stake (zPoS) 进行私人放样并发布v3.1。为Galileel Coin创建和发布白皮书以及在BitcoinTalk论坛中重新发布。
- 2019年第一季度 - 完成Galileel Instant On Master节点 (gIOMN) 功能的实施，并继续使用v4.0的通用性 (GA) 。此更新将对链进行硬分叉并且是强制性的。移动钱包开发于Galilee Core发布后的第一季末开始。
- 2019年第二季度 - 完成Galileel 混合证明Hybrid Proof-of-Stake (ghPoS) 的实施，用于公共和私人staking。一旦我们接近v5.0的发布日期，我们将发布激活块。此更



新将对链进行硬分叉并且是强制性的。移动钱包发布v1.0。在第二季度末，我们开始开发下一代移动钱包，并包括Galilel 混合证明Hybrid Proof-of-Stake (ghPoS)

- 2019年第3季度 - Galilel定期存款 (gTD) 功能将通过钱包v5.1向公众开放。此功能取决于Galilel 混合权益证明Hybrid Proof-of-Stake (ghPoS) 并在之后开发。此更新将对链进行硬分叉并且是强制性的。一旦我们接近发布日期，我们将发布激活块。
- 2019年第四季度 - Galilel货币供应控制 (gMSC) 已准备好投入生产，我们继续使用v6.0的一般可用性 (GA) 。此更新将对链进行硬分叉并且是强制性的。一旦我们接近发布日期，我们将发布激活块。在第四季度末，我们发布了具有Galilel定期存款 (GTD) 功能的移动钱包2.0。
- 2020年第一季度 - 利用Galilel Money Supply Control (gMSC) 发布v3.0的全面移动钱包。

虽然上面的路线图很清晰，并将重点放在区块链上，但团队还有其他一些想法可以进一步改进技术，以简化钱包的使用。其中一个弱点是内置的Qt钱包。有必要使用简洁的内置网络服务器替换它，使用前端框架，提供最佳的用户体验。

帮助

即使我们致力于实现我们的长期发展目标，任何人都可以协助或帮助实现项目目标。虽然开发是一个非常重要的部分，但欢迎任何能够帮助营销，撰写文章，向非技术人员解释功能的人。



重要鏈接

網站

<https://galilel.org/>

区块查询Block Explorer (MAINNET)主链

<https://explorer.galilel.org/>

区块查询Block Explorer (TESTNET)测试链

<https://explorer.testnet.galilel.org/>

钱包Wallet

<https://github.com/Galilel-Project/galilel/releases>

Discord

<https://discord.galilel.org>

推特Twitter

<https://twitter.com/GalilelEN>

脸书Facebook

<https://facebook.com/GalilelEN>

油管Youtube

<https://youtube.com/channel/UC26rKBciicXp33dK8NkALmg>

BitcoinTalk

<https://bitcointalk.galilel.org>



附录

1. <https://www.linkedin.com/in/mbroemme/>
<https://zuppy.pm/>
2. <https://github.com/Galilel-Project>
3. <https://review.kydcoin.io/galicoing/>
4. <https://opensource.org/licenses/MIT>
5. <https://www.gnu.org/licenses/gpl.txt>
6. <https://creativecommons.org/licenses/by-nc/4.0/legalcode.txt>
7. <https://www.transifex.com/galilel-project/galilel-project-translations/>
8. <http://zerocoin.org/media/pdf/ZerocoinOakland.pdf>
9. https://en.wikipedia.org/wiki/Time_deposit
10. https://en.bitcoin.it/wiki/Proof_of_burn
11. [https://en.wikipedia.org/wiki/One-to-many_\(data_model\)](https://en.wikipedia.org/wiki/One-to-many_(data_model))
12. <https://electrum.org/>
13. <https://discord.com/>
14. <https://bitcointalk.org/>



Galilel



galilel.org