



# Galileel

第一種具有混合共識算法的通用加密貨幣，  
Zerocoin動態權益證明，交易證明和主節點投票，  
以週期為基礎的獎勵燃燒投票

## 白皮書V1.11

邁克 布羅梅<sup>1</sup>, 十一月 2019



## 目錄

摘要 .....	3
介紹 .....	3
伽利略币 (Galileel Coin) .....	3
問題和解決方案 .....	3
Zerocoins動態權益證明 (dzPoS) .....	4
交易證明 (ghPoT) .....	5
混合證明 (ghPoS) .....	6
定期存款 (gTD) .....	8
貨幣供應控制 (gMSC) .....	9
即時主節點獎勵 (gIOMN) .....	11
特點和規格 .....	12
競合分析 .....	16
發展路線圖 .....	18
幫助 .....	19
重要鏈接 .....	20
附錄 .....	21



## 摘要

雖然法定貨幣已經定義並證明了數百年的經濟標準，但數字貨幣的情況卻不同。數字貨幣是一種具有不可預測價值的高風險投資，而且不斷消失的開發團隊放棄的大量區塊鏈項目。政府發現了這個問題，初始硬幣發行（ICO）法規將在未來幾年內解決。此外，具有獨特區塊鏈特徵的數字貨幣很有可能脫穎而出從而定義未來的數字貨幣標準。Galilel將通過實施本白皮書中概述的其獨特功能並參與此過程。

## 介紹

伽利略幣Galilel Coin是一個社區驅動的加密貨幣，具有完全透明性並利用開源的開發方式。投資者與項目團隊之間的信息關係是成功的關鍵。因此，我們創建了一個名為 *Galilel-Project*<sup>2</sup> 的GitHub的組織，該組織跟蹤公共存儲庫中的所有開發活動，包括我們的所有後端代碼，並通過了*Know Your Developer (KYD)*<sup>3</sup> 公共驗證。該項目主要使用MIT<sup>4</sup>，GPLv3<sup>5</sup> 和CC-BY-NC 4.0<sup>6</sup> 開源和開放內容許可。翻譯和本地化使用Transifex<sup>7</sup> 平台。

## 伽利略幣 (Galilel Coin)

Galilel Coin (GALI和zGALI) 是一種開源的公共和私人的交易權益Proof-of-Stake數字加密貨幣，用於快速（使用SwiftX），隱私（Zerocoin<sup>8</sup> 協議）和安全的微交易。我們的主要目標是創建一個去中心化的完全安全和匿名的網絡來運行應用程序，這些應用程序不依賴於任何中央主體控制。通過使用分佈式系統，數千名用戶將負責維護應用程序和數據，從而不會出現單點故障。

## 問題和解決方案

區塊鏈技術炒作產生了巨大的興趣，在全球範圍內受到歡迎，許多公司在數字貨幣之外還用於不同的使用目的。但是，使用它作為支付服務的基礎需要特定功能以驗證，



存儲和驗證數千個交易。雖然已經使用現有的一致性的算法來解決這一問題以在鏈中生成區塊，但是在當前的區塊鏈實現中存在若干弱區域以實現數字貨幣的主流採用。

## Zerocoin動態權益證明 (dzPoS)

Zerocoin Proof-of-Stake (zPoS) 是PIVX開發團隊於2018年推出的最新創新的區塊鏈功能。但是，技術實現以區塊鏈的特定方式完成，並且不允許輕鬆採用其他人，因為他們的獎勵結構靜態地包含在源代碼中。

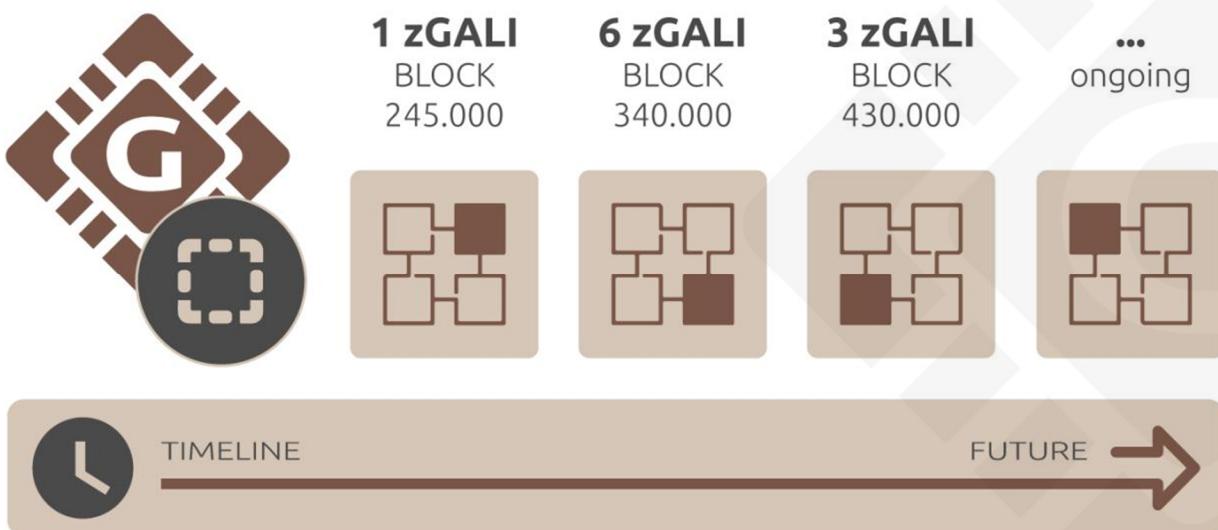


圖1.區塊鏈階段的Zerocoin 動態權益證明獎勵。

在Galileel，我們應用了Zerocoin權益的動態版本.Zerocoin權益 (Zerocoin staking) 以面額表示獎勵，表示整數值。最小可能的面額是一[數字1]。在第一個版本 - 預熱階段 - 我們總是使用最小面額值進行測試。這種方法的缺點是Zerocoin權益導致是CPU使用十分緊張，並且生成孤立塊的可能性更高，因為公共硬幣權益可以往後處理區塊，但是更早地將其分配到區塊鏈。在第二個版本 - 完整階段 - 我們根據塊獎勵金額自動確定最佳面額結構。這能顯著降低了生成孤塊的可能性。



## 交易證明 (ghPoT)

在傳統經濟學中，銀行賬戶之間有資金轉賬，可以指定一個主題，以便收款人可以將金額分配給特定發票。在當前的錢包實現中是不可能的。它允許指定註釋或註釋值，該值不是事務的一部分，只存儲在本地。要將發票分配給特定收款人，必須創建一個錢包地址，並在兩個利益相關者之間進行一對一映射。

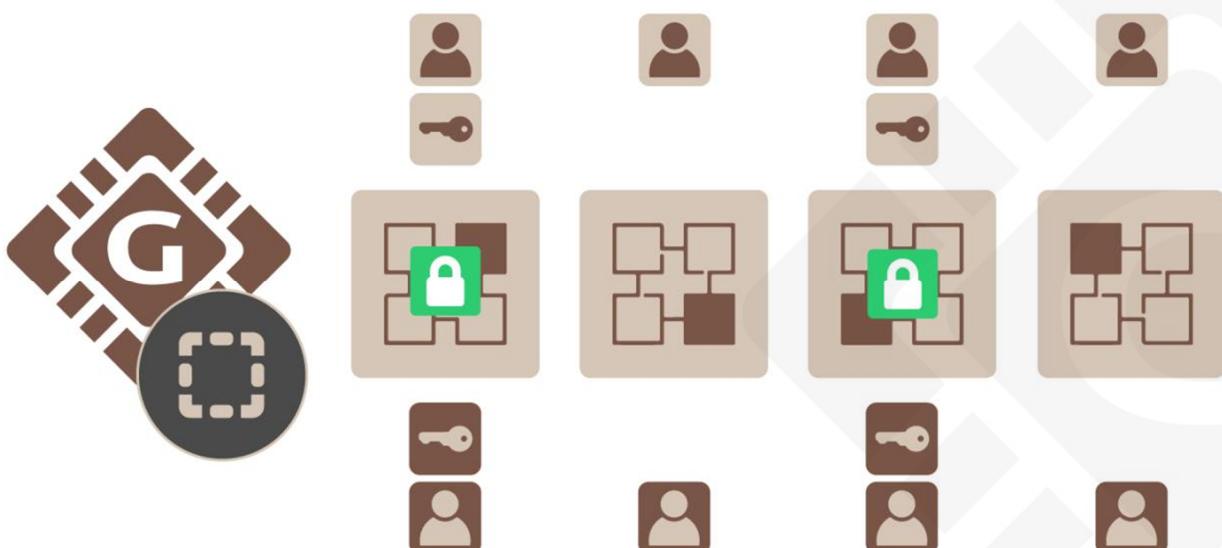


圖2.加密主題的交易證明。

在Galilel中，我們包含一個附加數據字段並將其附加到事務中，該事務存儲在塊中。它是一個加密字段，只有通過協商交易的錢包才能進行解密。它解決了交易分配問題，並允許支付處理網關識別發票的收款人，就像傳統的法定發票一樣。



## 混合證明 (ghPoS)

雖然Proof-of-Stake (PoS) 是一種環保的一致性算法，但只要桌面錢包正在運行，它就會產生獎勵。此問題的一個解決方案是註冊任何共享的Proof-of-Stake池並放入雲 (cloud) 中。然而，缺點是用戶需要信任POS的池並將特定數量的硬幣轉移給它。它可能導致大量硬幣存放在幾個錢包中的情況。對於去中心化的網絡方法而言，這是比較薄弱的一面去是達成共識的基本部分。權益證明，即所謂的Zerocoin Proof-of-Stake (zPoS)，具有相同的問題和局限性。



圖3.從Galileel網絡獲得獎勵的可能方式。

在Galileel，這個問題的解決方案將是一個名為Galileel Hybrid Proof-of-Stake (ghPoS) 的完全混合共識算法。我們將通過移動staking功能擴展Proof-of-Stake，用於公共和私人staking。如果移動設備的錢包找到塊，移動設備staking會總是以在TEN [10] 百分比的塊獎勵支付。在這種情況下，九十[90]百分比支付給masternode持有人。移動錢包將作為區塊鏈的輕節點工作，並且最小塊數等於重組深度。



### 混合權益證明獎勵結構

STAKING 分類 <sup>1</sup>	STAKING	MASTERNODE
電腦Online (GALI)	30%	70%
電腦Online (zGALI)	60%	40%
移動設備Mobile (GALI)	10%	90%
移動設備Mobile (zGALI)	20%	80%

<sup>1</sup> 其計算基於5 GALI獎勵 > 塊 430,000



## 定期存款 (gTD)

雖然移動賭注取決於網絡難度和staking的硬幣數量，但 *Term Deposit*<sup>9</sup>功能允許鎖定硬幣一段時間並產生獎勵。

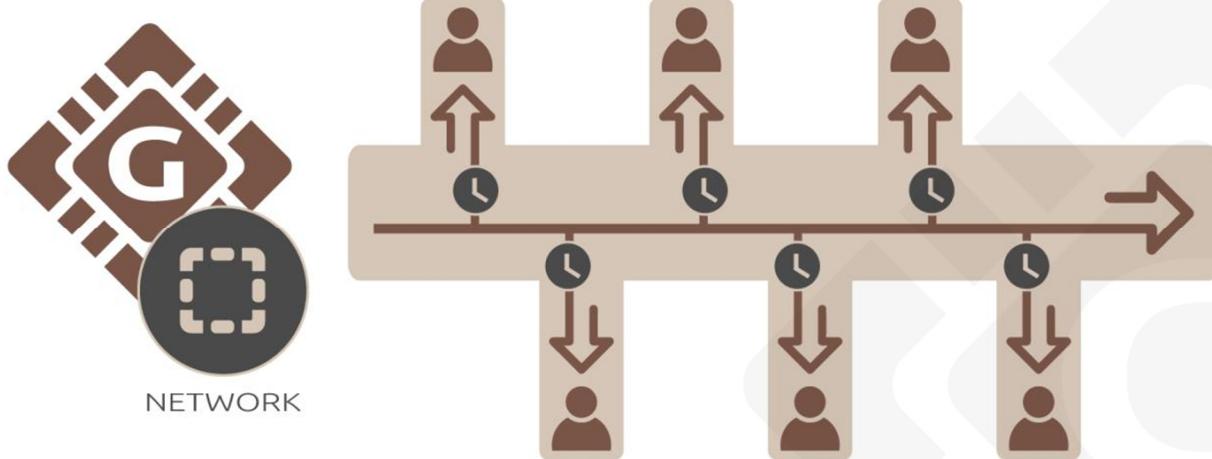


圖4.離線錢包中基於歷程表的定期存款。

使用Galileel定期存款 (gTD) 所需的最低硬幣數量是五千[GALI]。鎖定期為一年[1]年。塊獎勵是TEN [10]%，並且不同錢包的鎖定硬幣被加權。隨著網絡中的新塊，帶有鎖定硬幣的錢包根據其份量獲得金額。在定期存款期結束之前，此獎勵被鎖定。一旦鎖定，移動其硬幣或花錢購買是不可能的，在到期時間之前取消定期存款也是不可能的。這將有效地減少鎖定期間的硬幣供應。



## 貨幣供應控制 (gMSC)

通貨膨脹控制是數字貨幣被認可和接受作為法定貨幣的替代品中最具挑戰性的部分。沒有任何控制機制，任何數字貨幣的價值都是不可預測的。這導致投資者開始押注價值的情況（囤積），這可能會在數小時內嚴重損害市場，並立即消除將數字資金推向市場的可能性作為公認的支付選項。通過控制通脹，我們相信數字貨幣領域之外的人們會被吸引使用它，因為沒有必要每天都在他們的投資組合中尋找。與法定貨幣的中央銀行不同，沒有觀察和維持貨幣供應的中心位置。在Galileel，我們實施了一種分散的方法來刻錄硬幣，即私人和公共放樣硬幣的所謂燃燒證明proof of burn<sup>10</sup>機制。雖然這是控制貨幣流通的必要步驟，但主節點所有者有可能投票減少獎勵或在特定時期內完成燃燒以減少硬幣生成。

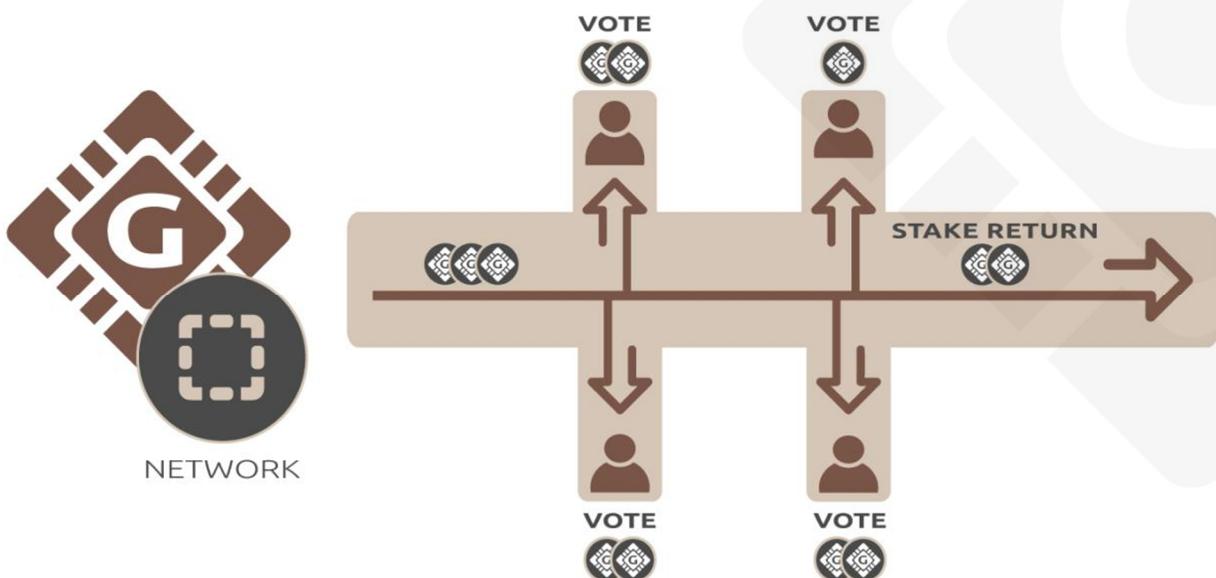


圖5. Masternode投票減少獎勵的產生。

我們將它命名為Galileel Money Supply Control (gMSC)，有效地使用了燃燒證明。這種機制只會帶來獎勵，而不是定期存款和發展預算。硬幣燃燒的時間將是一個月[1]個月，按照獎勵燃燒結構表中描述的步驟減少年度供應量。主節點持有者每月適用於投



票。該提案可以每月進行一次，從當前獎勵燃燒期結束前一周開始。區塊鏈接受從一千 [1000] GALI開始的任何提案。一旦在區塊鏈中分發提案，主節點持有者就可以投入額外的一[1]或更多GALI投票。在提案期結束後，具有最高金額和超過五十[50]% 主節點投票的提案將獲勝。如果提議期限結束並被接受，則鎖定在提案中的硬幣將被刻錄，獎勵燃燒期間從下一個刻錄塊開始。如果未達到提案接受的最低要求，則鎖定的硬幣將被解鎖。

#### 燃燒獎勵結構

燃燒比例	每月燃燒數量 <sup>1</sup>
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

<sup>1</sup> 其計算基於5 GALI獎勵 > 塊 430,000



## 即時主節點獎勵 (gIOMN)

主節點在數字金錢領域已經獲得了很大的吸引力。雖然許多新的數字加密貨幣試圖創造一個荒謬的高投資回報 (ROI) 硬幣並且在硬幣通脹開始之後失敗以及在主節點和賭注之間具有不平衡的獎勵分配，但這不是運行主節點的主要目的。在Galilel中，主節點的主要用例是保護網絡，同時有機會對未來的開發方面進行投票以及維護硬幣流通。但是，可用主節點實現的主要弱點是要求在作為主節點的每台機器上同步和索引區塊鏈。

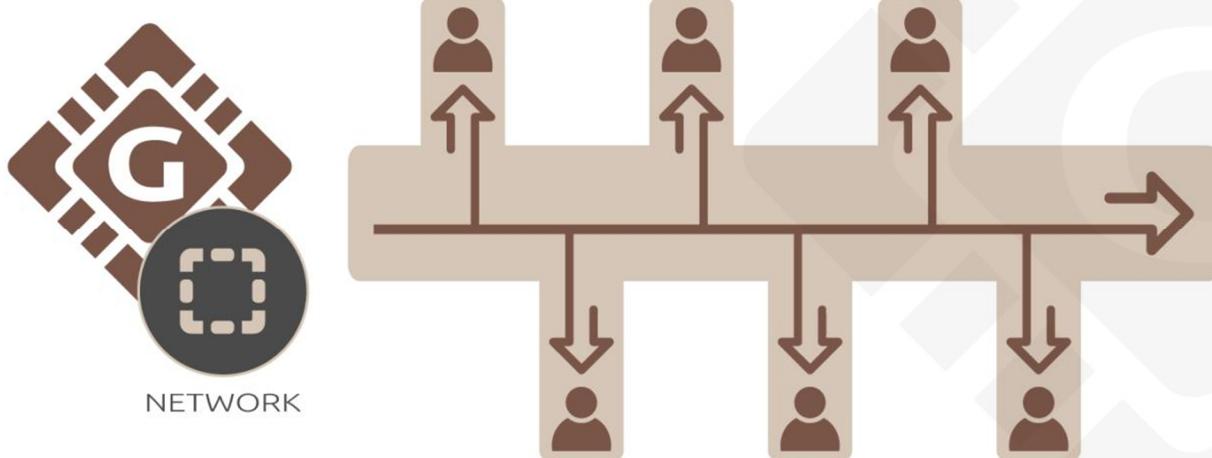


圖6.連接到雲中單個區塊鏈的多個主節點。

加利略Galilel的主節點獎勵機制 (gIOMN) 通過實現共享區塊鏈在客戶端 - 服務器模型中運行*one-to-many*<sup>11</sup> 錢包守護進程來解決此問題。它與*Electrum*<sup>12</sup> 客戶端中提供的“即時”模型相當。



## 特點和規格

### 硬幣規格

貨幣名稱	(伽利略) Galilel
貨幣縮寫	GALI
算法	Quark
共識算法	PoS + zPoS 混合
區塊大小	2 MB
區塊時間	60 秒 (重新定位每塊)
RPC 接口	36002
P2P 接口	36001
挖掘形式	PoW / PoS / zPoS / MN
最低 Staking 時間	2 小時
成熟時間	120 個確認
合格轉送	6 個確認
獎勵 (直至區塊高度 1,500)	MN 60%, PoW 40%
獎勵 (直至區塊高度 205,000)	MN 60%, PoS 40%
獎勵 (直至區塊高度 205,001)	MN 70%, PoS 30%
最後 PoW 區塊	1,500
Masternode 抵押	15,000



---

最大硬币供應 (一月 2020 January 2020)

19,035,999 GALI

---

最大硬币供應 (一月 2030 January 2030)

45,315,999 GALI

---

最大硬币供應 (一月 2040 January 2040)

71,595,999 GALI

---

最大硬币供應 (一月 2050 January 2050)

97,875,999 GALI

---

動態 硬币供應

交易費用& zGALI 挖矿費用將被燒毀

---

社區捐贈地址

[UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX](#)

---

開發預算 (由塊 250,001)

10% 每月超級區塊



## ZEROCOIN 規格

ZeroCoin v1 激活	塊 245,000
ZeroCoin v2 激活	塊 245,000
zGALI 自動挖掘	10%
zGALI 獎勵 (由區塊 245,001)	1 zGALI
zGALI 獎勵 (由區塊 340,001)	MN 40%, zPoS 60%
zGALI 獎勵 (由區塊 430,001)	MN 40%, zPoS 60%
zGALI 分母	1, 5, 10, 50, 100, 500, 1000, 5000
儲能器模數	RSA-2048
成熟	240 確認
合格轉送	20 確認
費用 (挖掘)	每一个GALI需要0.01費用
費用 (使用)	免費



### 工作證明衰變

區塊高度	獎勵	MN	POW	供應	周期	階段結束
塊 1	220,000	60%	40%	220,000	0 天	2018-05-25
塊 2 – 1,500	1	60%	40%	221,499	1 天	2018-05-26

### 權益證明衰變

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



## 競合分析

每天都有新的數字加密貨幣項目誕生，主要是針對特定目的的服務貨幣。雖然這是一個有效的方案，但它將硬幣的使用情況限制在特定的市場和規模。最後，它限制了貨幣價值。加密貨幣市場共享相同的特徵集，具有不同數量的數字貨幣和不同的塊獎勵，是過度飽和的。在過去，一些具有獨特想法和光明未來的項目誕生了。Galilel將繼續這一趨勢並改進用於數字貨幣的區塊鏈，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	達世	普羅	
公共 Staking	✓	✗	✓	✗
私人 Staking	✓	✗	✓	✗
即時 轉送	✓	✓	✓	✗
私人 轉送	✓	✓	✓	✗
Masternodes	✓	✓	✓	✗
去中心化治理投票	✓	✓	✓	✗
可變獎勵分配 <sup>1</sup>	✗	✗	✓	✗
動態 Zerocoin 權益證明	✓	✗	✗	✗
交易證明	✓	✗	✗	✗
可變獎勵燃燒	✓	✗	✗	✗
離線區塊鏈	✓	✗	✗	✗
移動設備權益證明	✓	✗	✗	✗
定期存款	✓	✗	✗	✓

<sup>1</sup> 可以使用Seesaw算法在Galileel中實現



## 發展路線圖

Galileel Coin的發展對於未來的區塊鏈至關重要。有些代碼已經編寫完成並且正在進行內部測試。Galileel Instant On Master節點 (gIOMN) 功能接近完成，而Galileel的混合證明Hybrid Proof-of-Stake (ghPoS) 在塊245,000計劃的Zerocoin v2激活後需要額外的開發和測試週期。我們的路線圖僅包括開發項目；我們認為有必要確定適當的目標，期望和可交付成果，而不是將精心調整的營銷項目納入其中。

- 2018年第二季度 - Fork PIVX代碼庫並啟動MAINNET。創建Discord<sup>13</sup> 頻道做為社區投票並在BitcoinTalk<sup>14</sup> 論壇中做預先的公告。
- 2018年第三季度 - 在第一個交易所和排名網站上市。實施關於獎勵分配，獎勵結構修改和主節點抵押的社區投票結果到v2.0。設計團隊為應用程序開發人員創建Galileel品牌和網站，其中包含品牌顏色，徽標和品牌指南。除了開發和設計，我們還將通過Know Your Developer (KYD) 公開驗證。
- 2018年 - 啟用並發布TESTNET，使開發人員能夠測試新的區塊鏈代碼和用戶以測試前沿功能。將Galileel代碼庫重構為最新的PIVX 3.1.1源和版本v3.0，在塊245,000處使用Zerocoin v1和v2激活，並使用分散式自治組織 (DAO) 進行區塊鏈投票，同時保持區塊鍊和網絡向後兼容。啟用Zerocoin Stof-of-Stake (zPoS) 進行私人放樣並發布v3.1。為Galileel Coin創建和發佈白皮書以及在BitcoinTalk論壇中重新發布。
- 2019年第一季度 - 完成Galileel Instant On Master節點 (gIOMN) 功能的實施，並繼續使用v4.0的通用性 (GA)。此更新將對鏈進行硬分叉並且是強制性的。移動錢包開發於Galilee Core發布後的第一季末開始。
- 2019年第二季度 - 完成Galileel 混合證明Hybrid Proof-of-Stake (ghPoS) 的實施，用於公共和私人staking。一旦我們接近v5.0的發布日期，我們將發布激活塊。此更新將對鏈進行硬分叉並且是強制性的。移動錢包發布v1.0。在第二季度末，我們開始開發下一代移動錢包，並包括Galileel 混合證明Hybrid Proof-of-Stake (ghPoS)



- 2019年第3季度 - Galileel定期存款（gTD）功能將通過錢包v5.1向公眾開放。此功能取決於Galileel 混合權益證明Hybrid Proof-of-Stake（ghPoS）並在之後開發。此更新將對鏈進行硬分叉並且是強制性的。一旦我們接近發布日期，我們將發布激活塊。
  -
- 2019年第四季度 - Galileel貨幣供應控制（gMSC）已準備好投入生產，我們繼續使用v6.0的一般可用性（GA）。此更新將對鏈進行硬分叉並且是強制性的。一旦我們接近發布日期，我們將發布激活塊。在第四季度末，我們發布了具有Galileel定期存款（GTD）功能的移動錢包2.0。
- 2020年第一季度 - 利用Galileel Money Supply Control（gMSC）發布v3.0的全面移動錢包。

雖然上面的路線圖很清晰，並將重點放在區塊鏈上，但團隊還有其他一些想法可以進一步改進技術，以簡化錢包的使用。其中一個弱點是內置的Qt錢包。有必要使用簡潔的內置網絡服務器替換它，使用前端框架，提供最佳的用戶體驗。

## 幫助

即使我們致力於實現我們的長期發展目標，任何人都可以協助或幫助實現項目目標。雖然開發是一個非常重要的部分，但歡迎任何能夠幫助營銷，撰寫文章，向非技術人員解釋功能的人。



## 重要鏈接

### 網站

<https://galilel.org/>

區塊查詢Block Explorer (MAINNET)主鏈

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

區塊查詢Block Explorer (TESTNET)測試鏈

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

### 錢包Wallet

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

### Discord

<https://discord.galilel.org>

### 推特Twitter

<https://twitter.com/GalilelEN>

### 臉書Facebook

<https://facebook.com/GalilelEN>

### 油管Youtube

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

### BitcoinTalk

<https://bitcointalk.galilel.org>



## 附錄

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](https://en.wikipedia.org/wiki/Time_deposit)
10. [https://en.bitcoin.it/wiki/Proof\\_of\\_burn](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.org**