GALILEL CORE

The first general purpose crypto currency with Hybrid Consensus Algorithm,
Dynamic Zerocoin Proof-of-Stake, Proof-of-Transaction and
Masternode voting for period based reward burning

White Paper v1.9

Maik Broemme[1], January 2019

Table of Contents

Executive Summary

While fiat money has defined and proved economic standards for hundreds of years already, the situation with digital money is different. Digital money is a high-risk investment with unpredictable value and disappearing development teams leaving orphaned blockchains. Governments identified this problem and Initial Coin Offering (ICO) regulations will solve it in the next few years. Moreover, the digital currencies, which implement unique blockchain features, have a high probability to define the future standards of digital money. Galilel will be part of this process through implementing the unique features outlined in this paper.

Introduction

Galilel Coin is a community driven crypto currency with full transparency and utilizing a public development method. The trust relationship between investors and the project team is the key to success. Therefore, we have created a GitHub organization named *Galilel-Project*[2], which tracks all our development activities in public repositories including all our backend code and passed *Know Your Developer (KYD)*[3] public verification. The project uses mostly *MIT*[4], *GPLv3*[5] and *CC-BY-NC 4.0*[6] open source and open content licenses. The translation and localization uses *Transifex*[7] platform.

Galilel Coin

Galilel Coin (GALI and zGALI) is an open-source public and private Proof-of-Stake digital crypto currency for fast (using SwiftX), private (*Zerocoin*[8] protocol) and secure micro transactions. Our main goal is to create a decentralized fully secure and anonymous network to run applications, which do not rely on any central body control. By having a distributed system, thousands of users will be responsible for maintaining the application and data so that there is no single point of failure.

Problems and Solutions

The blockchain technology hype generates huge interest, gaining popularity around the globe and is in use by many companies for different purposes beside digital money. However using it, as base for payment services require specific features to validate,

store and verify thousands of transactions. While this is already solved using existing consensus algorithm to generate blocks in the chain, there exist several weak areas in current blockchain implementations to achieve mainstream adoption of digital money.

Dynamic Zerocoin Proof-of-Stake (dzPoS)

Zerocoin Proof-of-Stake (zPoS) was the most innovative blockchain feature introduced in 2018 by the PIVX development team. However, the technical implementation done in a specific way for their blockchain and does not allow easy adoption to others as their reward structure is statically included in the source code.

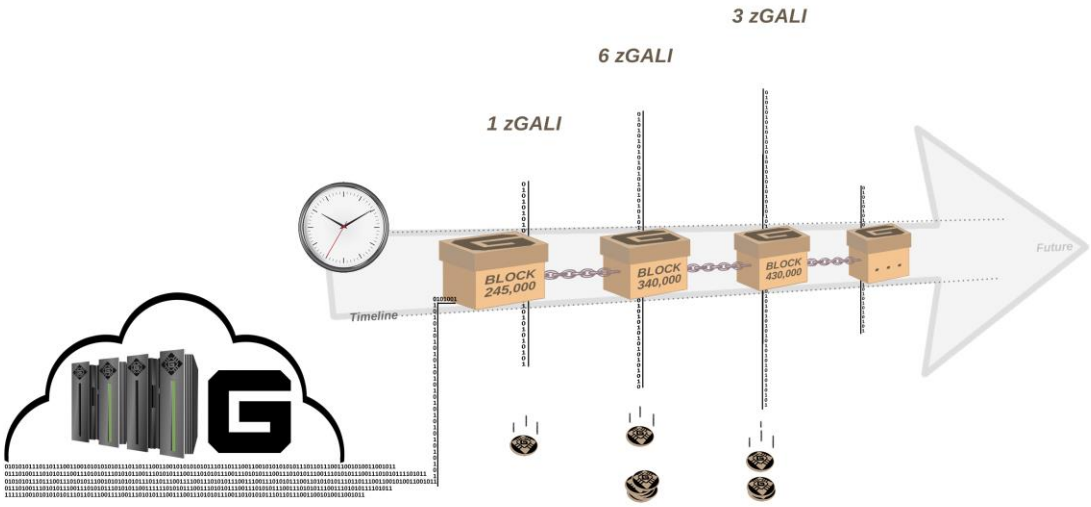

Figure 1. Dynamic Zerocoin Proof-of-Stake reward based on blockchain phase.

In Galilel, we implement a dynamic version of Zerocoin staking. Zerocoin staking generates rewards in denominations, which represent an integer value. The smallest possible denomination is one [1]. In the first version – warmup phase – we always use the smallest denomination value for testing purposes. The drawback of this approach is that Zerocoin staking is very CPU intensive and probability to generate an orphan block is higher as a public coin stake can solve the block later but distribute it to the chain earlier. In the second version – full phase – we auto determine the best denomination structure based on the block reward amount. This significantly reduces the probability to generate orphan blocks.

Proof-of-Transaction (ghPoT)

In traditional economics with money transfers between bank accounts, it is possible to specify a subject so that the recipient can assign the amount to a specific invoice. It is not possible in current wallet implementations. It allows specifying a comment or comment-to value, which is not part of the transaction and only stored locally. To assign an invoice to a particular payee it is necessary to create a wallet address with a one-to-one mapping between both stakeholders.

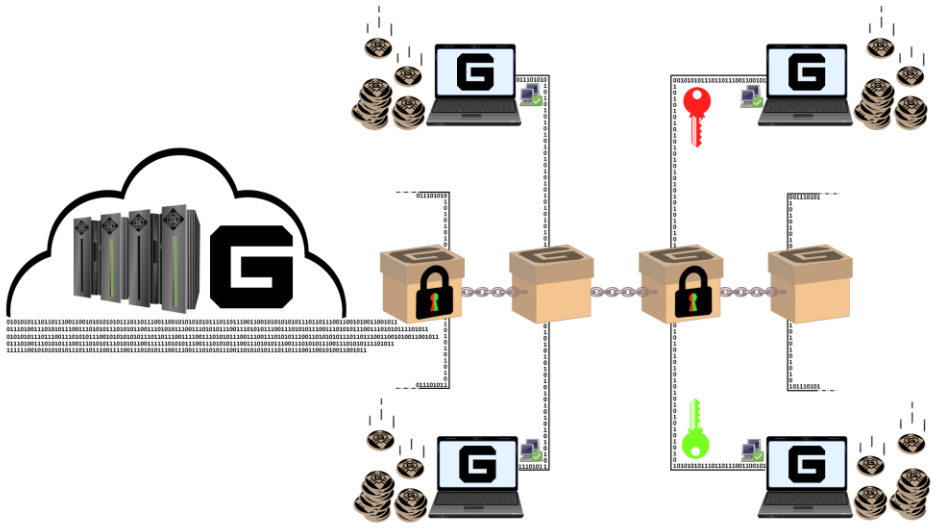

Figure 2. Proof-of-Transaction with encrypted subject.

In Galilel, we include an additional data field and attach it to the transaction, which is stored in the block. It is an encrypted field and decryption is only possible by the wallets, which negotiated the transaction. It solves the transaction assignment problem and allows payment-processing gateways to identify the payee of an invoice as it is with traditional fiat invoices.

Hybrid Proof-of-Stake (ghPoS)

While Proof-of-Stake (PoS) is an environmentally friendly consensus algorithm, it creates rewards only as long as the desktop wallet is running. One solution to this problem is to sign-up to any shared Proof-of-Stake pool and stake in the cloud. However, the disadvantage is that user need to trust the staking pool and transfer specific amount of coins to it. It can lead to situation that huge amount of coins are stored in a few wallets. This is a weak situation for a decentralized network approach and is a

fundamental part to reach consensus. Private staking, so called Zerocoin Proof-of-Stake (zPoS), has the same problems and limitations.

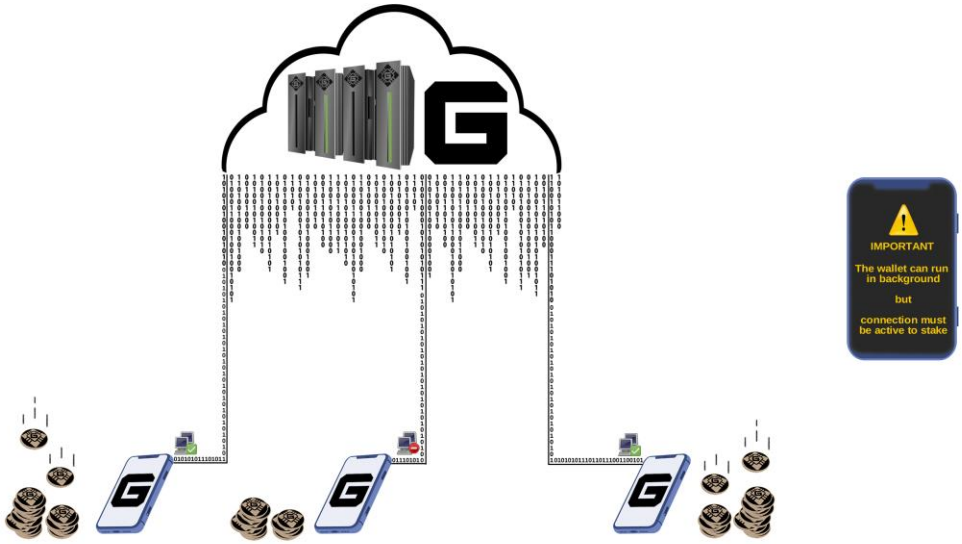

Figure 3. Possible ways to earn rewards from Galilel network.

In Galilel, the solution to this problem will be a complete hybrid consensus algorithm named Galilel Hybrid Proof-of-Stake (ghPoS). We will extend Proof-of-Stake with mobile staking capabilities for both public and private staking. Mobile staking is always on with **ten [10]** percent of the block reward paid out if mobile wallet finds a block. In this case **ninety [90]** percent paid out to masternode holder. The mobile wallets will work as a light node of the blockchain with minimum amount of blocks equal to the reorganization depth.

Hybrid Proof-of-Stake Reward Structure		
Staking Type[1]	Staking	Masternode
Online (GALI)	30%	70%
Online (zGALI)	60%	40%
Mobile (GALI)	10%	90%
Mobile (zGALI)	20%	80%

[1] Calculation is based on 5 GALI reward > block 430000

Term Deposits (gTD)

While mobile staking is dependent from network difficulty and amount of staked coins, the *Term Deposit*[9] function allow to lock coins for a certain period and generate rewards.

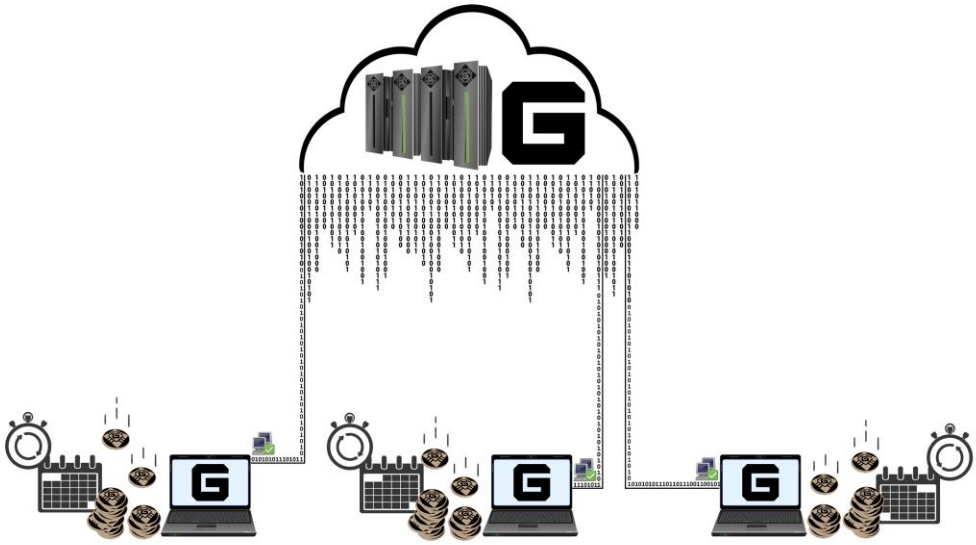

Figure 4. Calendar based term deposit in an offline wallet.

The minimum required amount of coins to use Galilel Term Deposit (gTD) is **five thousand [5,000]** GALI. The lock period is **one [1]** year. The block reward is **ten [10]** percent and locked coins of different wallets are weighted. With a new block in the network, wallets with locked coins get the amount according to their weight. Until Term Deposit period ends this reward is locked. Once locked, moving or spending coins for purchases is impossible, cancellation of term deposit before expiration time is impossible. This will effectively reduce the coin supply during the lock period.

Money Supply Control (gMSC)

Inflation control is the most challenging part for digital money to be recognized and accepted as alternative to fiat money. Without any controlling mechanism, the value of any digital money is unpredictable. This leads to situation when investors' starts betting on the value and this can seriously damage the market within hours and immediately eliminates the possibility to push digital money into market as accepted payment option. With inflation control, we believe that people outside the digital money sphere are attracted to use it, as there is no need to look every day at their portfolio. Unlike central banks in case of fiat money, there will be no central place for watching and maintaining money supply. In Galilel, we implement a decentralized approach to burn coins, so called *Proof-of-Burn*[10] mechanism for private and public staked coins. While this is one necessary step to control money circulation, masternode owners get the possibility to vote for reward reduction or complete burning for a specific period to reduce coin generation.

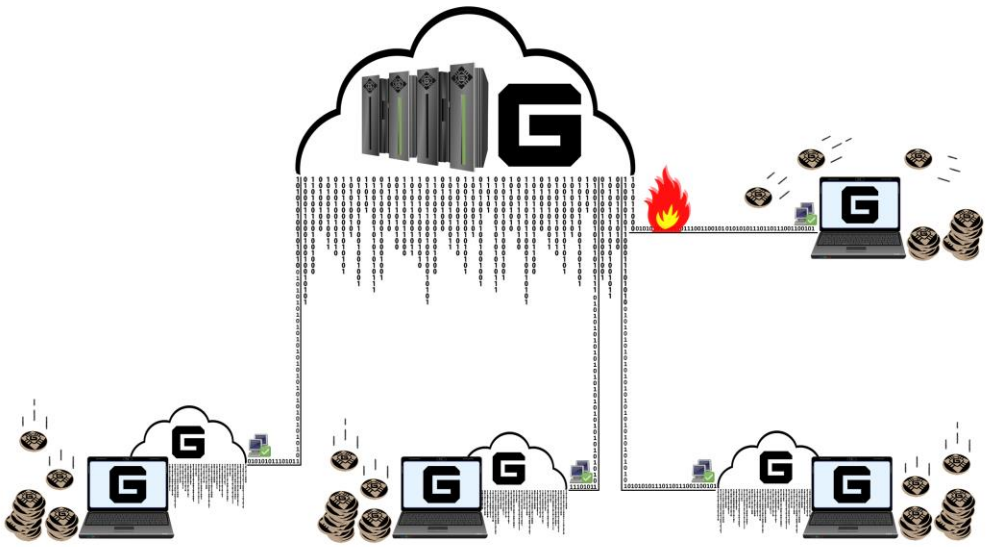

Figure 5. Masternode voting to reduce reward generation.

We name it Galilel Money Supply Control (gMSC), effectively Proof-of-Burn v2. This mechanism burns only rewards, never term deposits and development budget. The period for coin burning will be **one [1]** month, in steps described in reward burning structure table decreasing annual supply. Masternode holders are applicable to vote every month. The proposal can be made once a month, starting **one [1]** week before current reward burning period ends. The blockchain accepts any proposal starting from **thousand [1000]** GALI. Once proposal distributed in the blockchain, masternode holders can vote with spending additional **one [1]** or more GALI. The proposal with the highest amount of coins and with more than **fifty [50]** percent of masternode votes after proposal period ends, will win. If proposal period ends and is accepted, coins locked in proposals are burned and reward-burning period starts from next burn block. If minimum requirements for proposal acceptance not reached, locked coins will be unlocked.

Reward Burning Structure	
Burn percentage	**Burn amount per month[1]**
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

[1] Calculation is based on 5 GALI reward > block 430000

Instant On Masternodes (gIOMN)

Masternodes gained already a lot of attraction in digital money sphere. While many new digital crypto currencies try to create ridiculous high return of investment (ROI) coins and fail after coin inflation kicks in as well as having unbalanced reward distribution between masternodes and staking wallets, this is not the main purpose for running a masternode. In Galilel, the main use-case for masternodes is securing the network while having the opportunity to vote of future development aspects as well as maintaining coin circulation. However, the main weak point for available masternode implementations is the requirement to have the blockchain synced and indexed on each machine acting as a masternode.

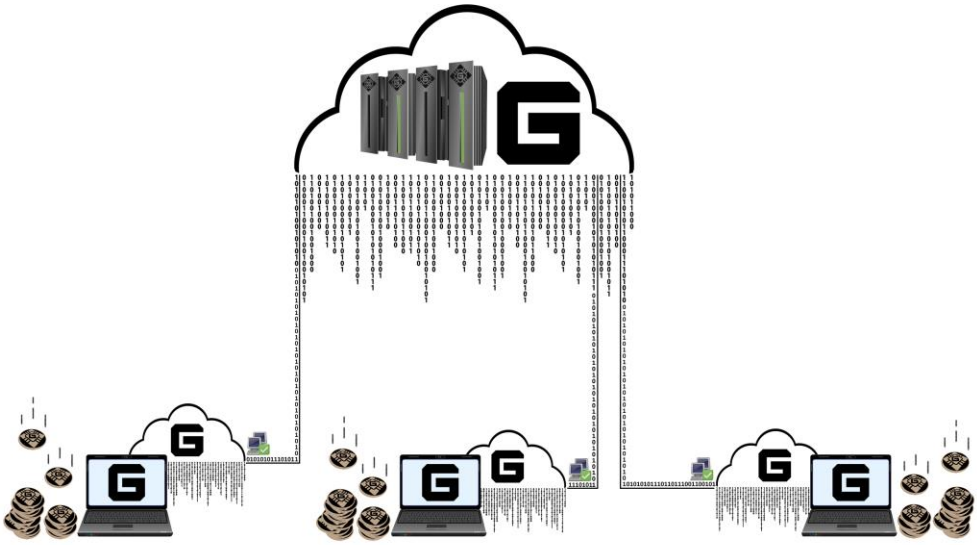

Figure 6. Multiple masternodes connected to single blockchain in the Cloud.

Galilel Instant On Masternode (gIOMN) solves this problem by implementing a shared blockchain to run *one-to-many*[11] wallet daemons in a client server model. It is comparable to “Instant On” model available in *Electrum*[12] client.

Features and Specifications

Coin Specifications	
Coin Name	Galilel
Coin Ticker	GALI
Hash Algorithm	Quark
Consensus Algorithm	PoS + zPoS Hybrid
Block Size	2 MB
Block Time	60 Seconds (Re-targeting every block)
RPC Port	36002
P2P Port	36001
Type	PoW / PoS / zPoS / MN
Minimum Staking Age	2 Hours
Maturity	120 confirmations
Send Eligibility	6 confirmations
Rewards (till block 1500)	MN 60%, PoW 40%
Rewards (till block 205000)	MN 60%, PoS 40%
Rewards (from block 205001)	MN 70%, PoS 30%
Last PoW Block	1,500
Masternode Collateral	15,000
Max Coin Supply (January 2020)	19,035,999 GALI
Max Coin Supply (January 2030)	45,315,999 GALI
Max Coin Supply (January 2040)	71,595,999 GALI
Max Coin Supply (January 2050)	97,875,999 GALI
Dynamic Coin Supply	Transaction fees & zGALI minting fees are burnt
Community Donation Address	UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX
Dev Budget (from block 250001)	10% in monthly superblock

Zerocoin Specifications	
Zerocoin v1 activation	block 245,000
Zerocoin v2 activation	block 245,000
zGALI Automint	10%
zGALI Rewards (from block 245,001)	1 zGALI
zGALI Rewards (from block 340,001)	MN 40%, zPoS 60%
zGALI Rewards (from block 430,001)	MN 40%, zPoS 60%
zGALI Denominators	1, 5, 10, 50, 100, 500, 1000, 5000
Accumulator Modulus	RSA-2048
Maturity	240 confirmations
Send Eligibility	20 confirmations
Fees (mint)	0.01 GALI per minted zGALI denomination
Fees (spend)	No fee

Proof-of-Work Rewards Breakdown						
Block Height	Reward	MN	PoW	Supply	Period	Stage End
Block 1	220,000	60%	40%	220,000	0 days	2018-05-25
Block 2 – 1,500	1	60%	40%	221,499	1 day	2018-05-26

Proof-of-Stake Rewards Breakdown							
Stages	Block Height	Reward	MN	PoS	Supply	Period	Stage End
Stage 1	1,501-12,000	100	60%	40%	1,271,399	7 days	2018-06-02
Stage 2	12,001-22,000	90	60%	40%	2,171,309	7 days	2018-06-09
Stage 3	22,001-42,000	80	60%	40%	3,771,229	14 days	2018-06-23
Stage 4	42,001-100,000	70	60%	40%	7,831,159	40 days	2018-08-02
Stage 5	100,001-160,000	60	60%	40%	11,431,099	42 days	2018-09-13
Stage 6	160,001-205,000	50	60%	40%	13,681,049	31 days	2018-10-14
Stage 7	205,001-250,000	25	70%	30%	14,806,024	31 days	2018-11-14
Stage 8	250,001-340,000	13.5	70%	30%	16,156,009	62 days	2019-01-15
Stage 9	340,001-430,000	10	70%	30%	17,055,999	62 days	2019-03-18
Stage X	430,001-ongoing	5	70%	30%	ongoing	ongoing	ongoing

Competitive Analysis

Every day new digital crypto currency projects are born, mostly service currencies for a specific purpose. While it is a valid scenario, it limits the use case of the coin to a particular market and size. In the end, it limits the currency value. The market of crypto currencies sharing the same set of features with different amount of digital money and different block rewards is oversaturated. In the past, some projects with unique ideas and a bright future were born. Galilel will continue this trend and improve blockchain used for digital money while building an easy to use general-purpose crypto currency for mass adoption in the market.

Feature	Galilel	Dash	PIVX	ROI Coin
Public Staking	✓	✗	✓	✗
Private Staking	✓	✗	✓	✗
Instant Send	✓	✓	✓	✗
Private Send	✓	✓	✓	✗
Masternodes	✓	✓	✓	✗
Decentralized Governance Voting	✓	✓	✓	✗
Variable Reward Distribution[1]	✗	✗	✓	✗
Dynamic Zerocoin Proof-of-Stake	✓	✗	✗	✗
Proof-of-Transaction	✓	✗	✗	✗
Variable Reward Burning	✓	✗	✗	✗
Disconnected Blockchain	✓	✗	✗	✗
Mobile Proof-of-Stake	✓	✗	✗	✗
Term Deposits	✓	✗	✗	✓

[1] Possible to implement in Galilel using Seesaw algorithm

Development Roadmap

The development of Galilel Coin is critical for the blockchain of the future. Some code has already been written and is in internal testing. The Galilel Instant On Masternode (gIOMN) feature is near completion while Galilel Hybrid Proof-of-Stake (ghPoS) require additional development and testing cycles after planned Zerocoin v2 activation at block 245,000. Our roadmap includes mainly development items only; we believe that it is

necessary to define proper goals, expectations and deliverables rather than putting fine-tuned marketing items to it.

- Q2 2018 – Fork PIVX codebase and launch MAINNET. Creating *Discord*[13] channel for community voting and pre-announcement in *BitcoinTalk*[14] forum.
- Q3 2018 – Listing on first exchange and ranking sites. Implementing community vote results regarding reward distribution, reward structure modification and masternode collateral into v2.0. Design team creating Galilel brand and website with brand colors, logos and brand guide for application developers. Beside development and design, we will pass Know Your Developer (KYD) public verification.
- Q4 2018 – Enable and release TESTNET, giving developers ability to test new blockchain code and users to test bleeding edge features. Refactor Galilel codebase to latest PIVX 3.1.1 source and release v3.0 with Zerocoin v1 and v2 activation at block 245,000 and working Decentralized Autonomous Organization (DAO) for blockchain voting while keeping the blockchain and network backward compatible. Enable Zerocoin Proof-of-Stake (zPoS) for private staking and release v3.1. Creating and releasing whitepaper for Galilel Coin together with re-announcement in BitcoinTalk forum.
- Q1 2019 – Finish implementation of Galilel Instant On Masternode (gIOMN) feature and proceed with General Availability (GA) of v4.0. This update will hard-fork the chain and is mandatory. Mobile wallet development starting in late Q1 after release of Galilel Core.
- Q2 2019 – Finish implementation of Galilel Hybrid Proof-of-Stake (ghPoS) for public and private staking. We will publish the activation block once we get closer to the release date of v5.0. This update will hard-fork the chain and is mandatory. Mobile wallet release of v1.0. In late Q2, we start development of next generation mobile wallet and include Galilel Hybrid Proof-of-Stake (ghPoS).
- Q3 2019 – Galilel Term Deposit (gTD) feature will become available to the public with wallet v5.1. This feature depends on Galilel Hybrid Proof-of-Stake (ghPoS) and developed afterwards. This update will hard-fork the chain and is mandatory. We will publish the activation block once we get closer to the release date.

- Q4 2019 – Galilel Money Supply Control (gMSC) is ready for production and we proceed with General Availability (GA) of **v6.0**. This update will hard-fork the chain and is mandatory. We will publish the activation block once we get closer to the release date. In late Q4, we publish mobile wallet **v2.0** with Galilel Term Deposit (gTD) feature.
- Q1 2020 – Full-fledged mobile wallet release of **v3.0** with Galilel Money Supply Control (gMSC).

While the roadmap above is sharp and put the focus on the blockchain, the team has several other ideas in mind for further technology improvements to simplify the wallet usage. One of these weak areas is the built-in Qt wallet. For better platform interoperability, it is necessary to replace it with a thin built-in webserver using a frontend framework giving the best user experience.

Help

Even if we are committed to our long-term development goals, anybody can assist or help with the project goals. While development is a very important part, anyone who can help with marketing, writing articles, explaining features to non-technical people is welcome.

Important Links

Website

https://galilel.cloud

Block Explorer (MAINNET)

https://explorer.galilel.cloud

Block Explorer (TESTNET)

https://explorer.testnet.galilel.cloud

Wallet

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

Discord

https://discord.galilel.cloud

Twitter

https://twitter.com/GalilelEN

Facebook

https://facebook.com/GalilelEN

YouTube

https://youtube.com/channel/UC26rKBciicXp33dK8NkALmg

BitcoinTalk Announcement

https://bitcointalk.galilel.cloud

Brand Guide

https://galilel.cloud/downloads/guides/Galilel_Brand_Guide_v2.pdf

Tor Masternode Guide

https://galilel.cloud/downloads/guides/Galilel_TOR_Masternode_Guide.pdf

Appendix

1. https://www.linkedin.com/in/mbroemme/
   https://zuppy.pm/
2. https://github.com/Galilel-Project
3. https://review.kydcoin.io/galicoin/
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)
12. https://electrum.org/
13. https://discord.com/
14. https://bitcointalk.org/

www.galilel.cloud