# Galilel

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

# LITE PAPER V1.0

Ehsan Khademi and Maik Broemme, November 2019

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

The purpose of this summary is to give a brief overview of the aims of the Galilel Core project. The main focus lies on giving a non-technical explanation of the Blockchain features and the rationale behind them with regard to real world applications and dynamics. For a technically detailed explanation of the features presented here please refer to our *Whitepaper*[1].

## INTRODUCTION

The Galilel cryptocurrency (further simply referred to as GALI) is a general purpose coin. This means that its sole purpose is to act as a medium for transactions. It is not bound to a platform or specific use case. Bearing this in mind the blockchain features behind the currency itself aim to emulate properties of fiat currencies and the monetary systems that build the underlying infrastructure of those currencies. Money as our society knows it has three classical properties. It's a store of value, a medium for exchange and a unit of account. In order to being a medium for exchange and a unit of account it's fundamental to establish money as a store value which is something most cryptocurrencies are still struggling with. GALI tackles this problem by implementing blockchain features that aim at providing those properties. Specifically this means to establish blockchain imminent features that allow to control the monetary supply and make it attractive for transaction purposes.

## BLOCKCHAIN FEATURES

The first blockchain feature that was implemented is Dynamic Zerocoin Proof-of-Stake (dzPoS).The Zerocoin Protocol is used with the specific goal that the privacy feature will emulate real life business situations. A company or person who wants to pay with a currency may not want transactions to be tracked or its financial situation to be known. While in the real world, financial market intermediaries serve as a gateway where it is not possible to track transactions by the receiver, this is not the case when using cryptocurrencies. The obvious advantage is the absence of a controlling centralized body which is the biggest selling point of cryptocurrencies. However, on the other hand everyone can track those transactions on the blockchain. This can and will be a major obstacle when trying to convince a business to use a respective crypto currency for transaction purposes. Therefore the Zerocoin Protocol is an important feature for GALI going forward as it will anonymize transactions. However, with recently discovered Zerocoin design issue, this feature is going to be reimplemented with a new privacy protocol.

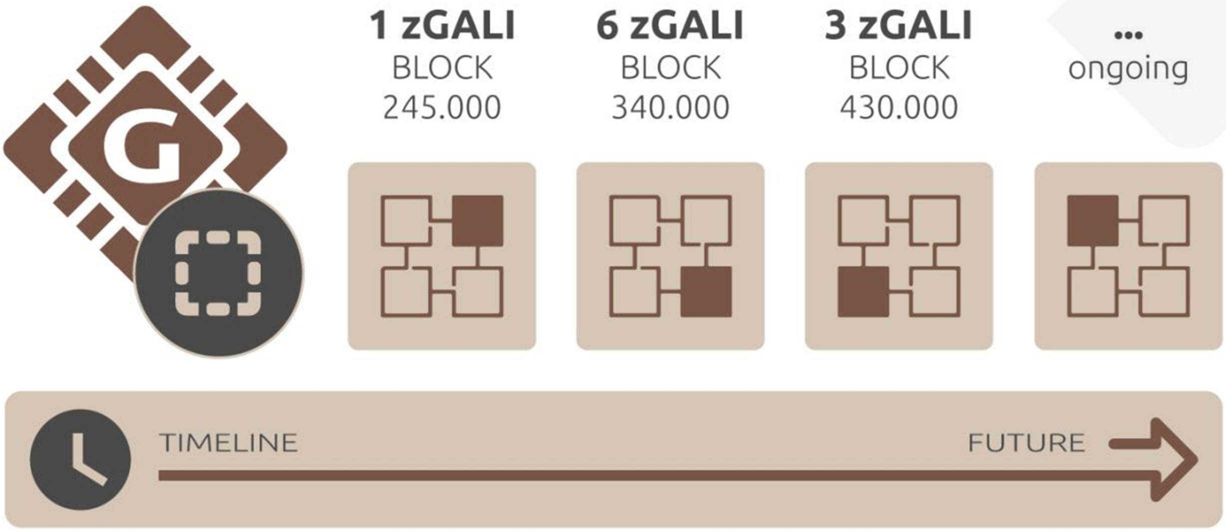
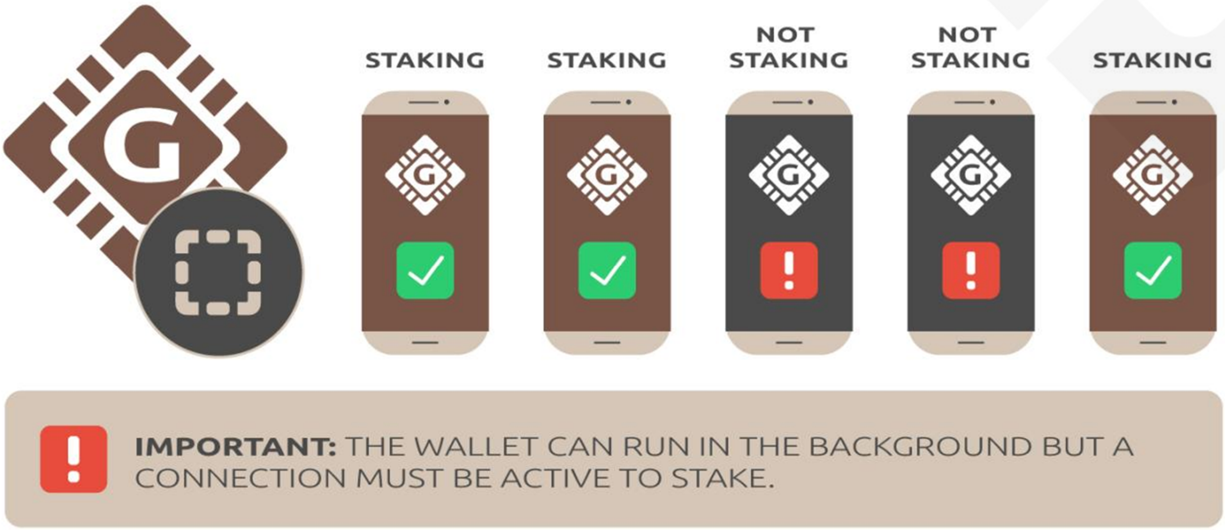


*Figure 1. Dynamic Zerocoin Proof-of-Stake reward based on blockchain phase.*

We apply a dynamic version of it with regard to staking which means that someone who stakes GALI on the private Zerocoin chain gets higher block returns than an average Staker or a Masternode holder. This way we want to ensure that there is a high amount of coins in the private chain which increases the degree of anonymization. GALI is currently the only cryptocurrency which utilizes a privacy feature in this way with regard to incentivizing staking on the private chain. Furthermore we will implement Hybrid Proof-of-Stake (ghPoS). This means that the classic Proof-of-Stake mechanism will be extended with mobile staking capabilities for both public and private staking. In order to achieve this the GALI mobile wallets utilize a light node that is more resource friendly. The classic staking mechanism requires a computer to be constantly online which requires a lot of resources. Since mobile phones are turned on 24/7 a resource friendly staking solution will ensure a high degree of network difficulty since it's not required to run a wallet on a desktop computer in order to solve blocks via staking. A higher network difficulty in turn means that the blockchain is better suited to process transactions especially on a large scale since it is more robust to network congestion.



**IMPORTANT:** THE WALLET CAN RUN IN THE BACKGROUND BUT A CONNECTION MUST BE ACTIVE TO STAKE.

*Figure 2. Possible ways to earn rewards from Galilel network.*

Classic bank transfer forms provide a reference line where a sender can fill in an order number, invoice number or any kind of numerical or alphabetical information that might help the recipient to identify and assign the payment. While this might be a trivial aspect when doing bank transfers, current wallet implementations don't provide this feature. As a result a recipient may not be able to identify incoming payments, especially when confronted with payments on a large scale. Proof-of-Transaction (ghPoT) is the blockchain feature which solves this trivial yet important issue. The wallet provides an additional reference field where information can be attached to a transaction. The information attached to the reference field is encrypted and can only be decrypted by the two wallets which are part of the transaction. This feature helps to solve the transaction assignment problem which is necessary in order to again establish transactions on a large scale by allowing payment-processing gateways to identify the payee of an invoice like with traditional fiat invoices.

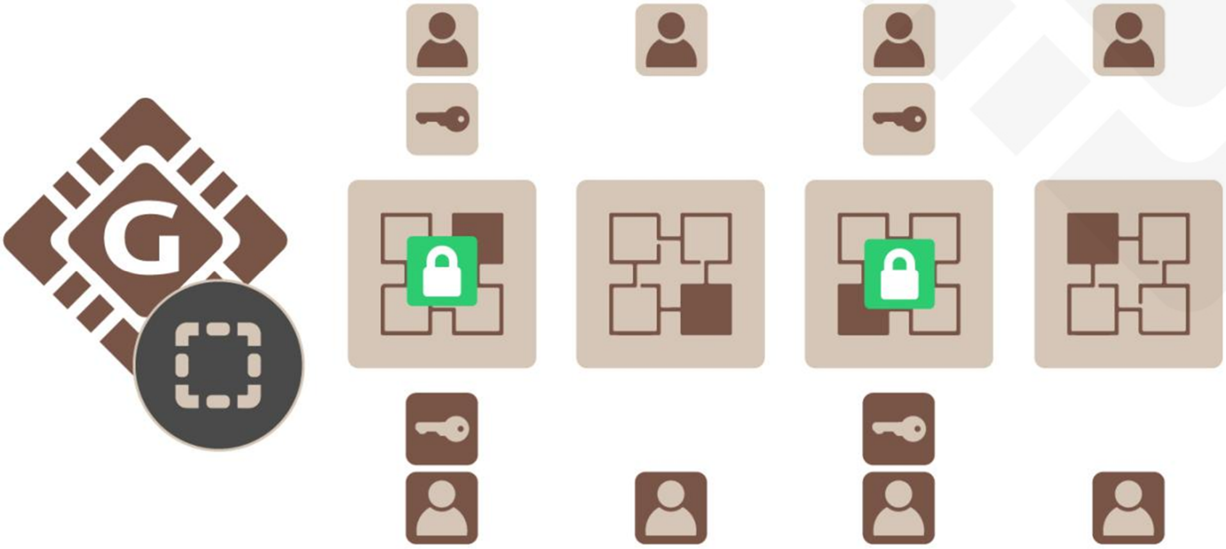


*Figure 3. Proof-of-Transaction with encrypted subject.*

The Instant On Masternodes (gIONM) feature aims to simplify running the blockchain. With time a blockchain gets bigger which requires ever more resources to store the blockchain on a hard-drive since all transactions are stored forever on the ledger. 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. Instant On Masternode (gIOMN) solves this problem by implementing a shared blockchain to run wallet daemons in a client server model. It is comparable to the "Instant On" model available in an Electrum client. Individual Masternode holders are not required to store the blockchain on their respective machine anymore. This will be an important factor with regard to adopting a currency on a large scale as a payment solution. Private chains tend to grow significantly in size with time which requires individual Masternode holders to provide ever more resources. In order to make a cryptocurrency feasible as a transaction medium it is therefore necessary to provide a solution to the circumstance that a highly adopted and used cryptocurrency with a private chain might be bigger that what common end-user hardware might be able to process.

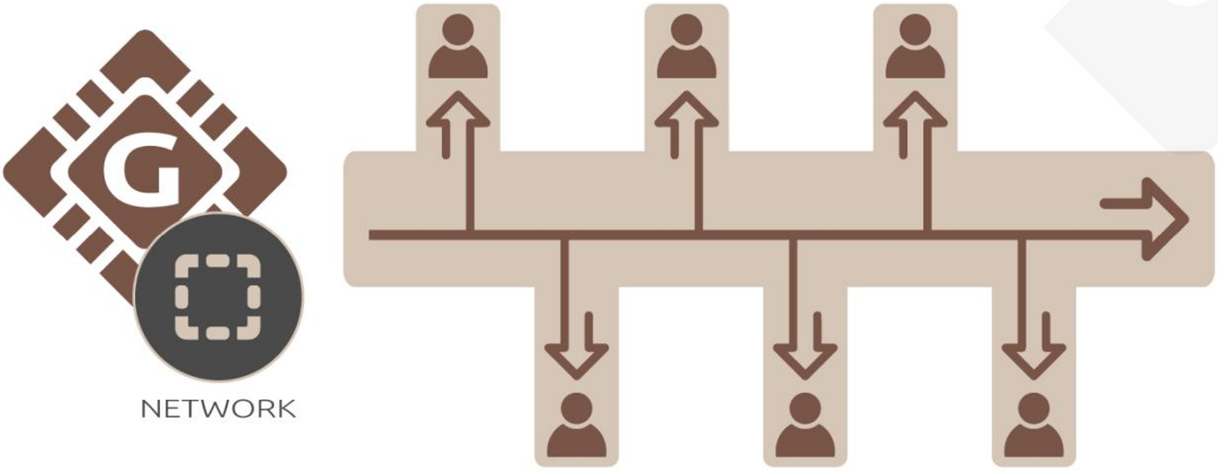


*Figure 4. Multiple masternodes connected to single blockchain in the Cloud.*

In order to emulate the underlying structure of monetary systems as applied by central banks GALI will implement Term Deposits (gTD) and Money Supply Control (gMSC). Term Deposits (gTD) reflect what most people know as time deposits on a classic bank account. GALI will offer coin holders the possibility to lock up coins for a certain period of time in order to generate a higher reward than what would be possible to achieve with staking. On the flip side those funds are not accessible to the holder and subsequently are out of circulation which acts as a market mechanism to control the overall supply of the currency.

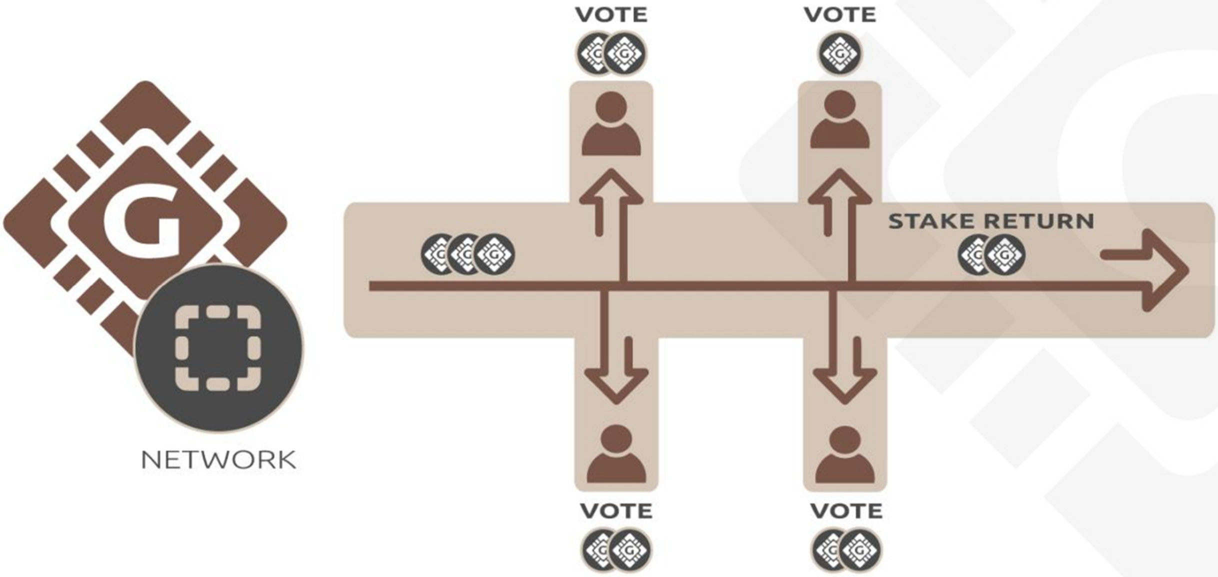


*Figure 5. Masternode voting to reduce reward generation.*

That being said individual coin holders can decide wether they want to use this feature or not. Money Supply Control (gMSC) is the inflation mechanism integrated into the GALI blockchain. This means that there will be no central body that controls inflation but it will be governed by a decentralized approach. Masternode holders are able to periodically vote (once a month) on reducing the block rewards or skip them at all. This approach can be compared to periodical central bank meetings where monetary decisions are made to control the inflation output. This gives a market based solution to inflation where the very holders of the currency have a say on the overall inflation schedule in contrast to a centralized body. In summary the GALI cryptocurrency provides the GALI coin holders with two mechanisms that will give them the possibility to control the overall available supply and to control the overall inflation output.

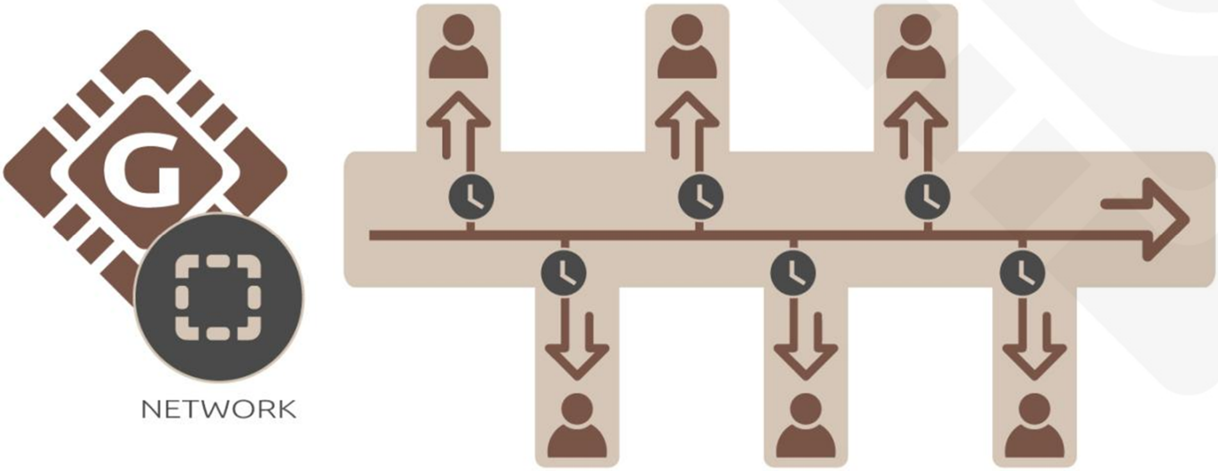


*Figure 6. Calendar based term deposit in an offline wallet.*

Galilel

## IMPORTANT LINKS

Website

https://galilel.org/

Block Explorer (MAINNET)

https://explorer.galilel.org/

Block Explorer (TESTNET)

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

Wallet

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

Discord

https://discord.galilel.org

Twitter

https://twitter.com/GalilelEN

Facebook

https://facebook.com/GalilelEN

Reddit

https://www.reddit.com/r/Galilel/

BitcoinTalk

https://bitcointalk.galilel.org

## APPENDIX

1. https://galilel.org/en/whitepapers

galilel.org