GNIXCOIN

Developer:
Magnus Gräsberg
grasberg@gmail.com

1 May 2018

rev 1.3

INTRODUCTION

Gnixcoin is a new cryptocurrency based on the CryptoNote technology.

The technology provides great security and private use for both senders and receivers of transactions and the main goal for Gnixcoin is to make it as usable as cash and credit cards but more convenient in an everyday situation.

You should be able to use it for splitting dinner checks with friends, making a small payment for ice cream and even buying your weekly groceries in stores.

DISCLAIMER

The information provided in this document does not constitute investment advice, financial advice, trading advice, or any other sort of advice, and you should not treat any part of the document as such. Nothing in this document should be taken as an offer to buy, sell or hold a cryptocurrency. Do conduct your own due diligence and consult your financial advisory before making any investment decision. I will not be held responsible for the investment decisions you make based on the information provided in this document.

Accuracy of Information

I will strive to ensure accuracy of information stated in this document although it will not hold any responsibility for any missing or wrong information. You understand that you are using any and all information available here AT YOUR OWN RISK. You should take adequate steps to verify the accuracy and completeness of any information in this document.

Price Risk

The price of cryptocurrencies is very highly volatile. It is common for prices to increase or decrease in a single day. Although this could mean potential huge profits, this also could mean potential huge losses. Cryptocurrency trading may not be suitable for all people. Anyone looking to invest in cryptocurrencies should consult a fully qualified independent professional financial adviser.

General

ALL INFORMATION CONTAINED IN THIS DOCUMENT IS FOR GENERAL INFORMATIONAL USE ONLY AND SHOULD NOT BE RELIED UPON BY YOU IN MAKING ANY INVESTMENT DECISION. THE DOCUMENT DO NOT PROVIDE INVESTMENT ADVICE AND NOTHING IN THE DOCUMENT SHOULD BE CONSTRUED AS BEING INVESTMENT ADVICE. BEFORE MAKING ANY INVESTMENT CHOICE, YOU SHOULD ALWAYS CONSULT A FULLY QUALIFIED FINANCIAL AND/OR INVESTMENT ADVISER.

ALTHOUGH I USE ITS REASONABLE EFFORTS TO ENSURE THAT INFORMATION IN THIS DOCUMENT IS ACCURATE AND COMPLETE, IT CANNOT GUARANTEE THIS TO BE THE CASE. CERTAIN INFORMATION AND DATA PROVIDED MAY BE DELAYED AS SPECIFIED BY FINANCIAL EXCHANGES OR INFORMATION PROVIDERS.
YOUR ACCESS TO, AND USE OF, THE MATERIALS AND INFORMATION AVAILABLE IN THIS DOCUMENT IS ON AN "AS-IS", "AS AVAILABLE" BASIS AND I WILL NOT BE HELD RESPONSIBLE FOR ANY ACTIONS YOU MAY TAKE.

TABLE OF CONTENT

Innehåll

CONCEPT

Bitcoin pioneered the knowledge of cryptocurrencies among people and today almost everyone has heard of Bitcoin, but only a few knows how to use them.

Gnixcoin is going to change this by adding to the online option to also be available via mobile phones apps and physical NFC terminals for small shops and stores.

You only need to swipe your NFC phone, smartcard, NFC implant, prepaid NFC chips or any other NFC hardware and your payment is done.
No pin codes to remember, no long wallet addresses to enter or signing needed.
The platform also allows for phone to phone transfers by simply moving the phones close together.

To Gnix

We call this way of payment "to Gnix".
It's a verb that you use when making the payment. E.g. "To gnix", "Have you Gnixed me yet?"

Gnix Platform

The Gnix platform, based on NFC technology, is the software, hardware and API developed to be used in real world everyday situations.

Anonymous

Contrary to Bitcoin with its connected debit cards (VISA or MASERCARD network) Gnixcoin allows you to transfer your coins to your NFC device from your own wallet on your computer or from your mobile phone which makes even the topups private and secure. Gnixcoin network have untraceable and unlinkable transactions and therefore offers a totally anonymous use.

Marketing

Gnixcoin will be marketed towards all age groups and genders.
We strive to be the number one go to app for small transactions between family members and friends and as a payment options in your local shop.

CURRENCY SPECIFICATIONS

Name: Gnixcoin
Symbol: GIX
Total supply: 8,589,869,056 GIX
Decimal point: 8
Address prefix: g
Premined coins (1% of total): 85,898,690 GIX

Presale is 50% of Premined coins
Starting presale price: $0.5 per GIX

HOW GNIXCOIN WORKS

A case study

User to User

Users can transfer funds between wallets, between their loaded NFC chips and between NFC chip and wallet.

User to Store

Users can pay with their mobile wallet app or they can “gnix” with their NFC device (swiping it over the merchant’s reader).

Store to user

Store owners can make refunds to a NFC payment done. The user holds the chip over the merchants NFC reader/writer and the merchant initiate the transfer from their wallet software.

Online

When using Gnixcoin online you will make a payment from your wallet like any other cryptocurrency.

Implant NFC

Since the Gnix platform allows for using any kind of NFC chip with Gnixcoin loaded on them. You can use your NFC implant to make payments. Just hold the chip over your NFC reader/writer and send from your wallet to add funds to it and then you can use it for payment in stores by just Gnixing (swiping your chip over the merchants reader).

Prepaid NFC chip

Since the Gnix platform allows for selling prepaid NFC chip with gnixcoin loaded on them. You can use them in stores just like your NFC on your mobile phone.

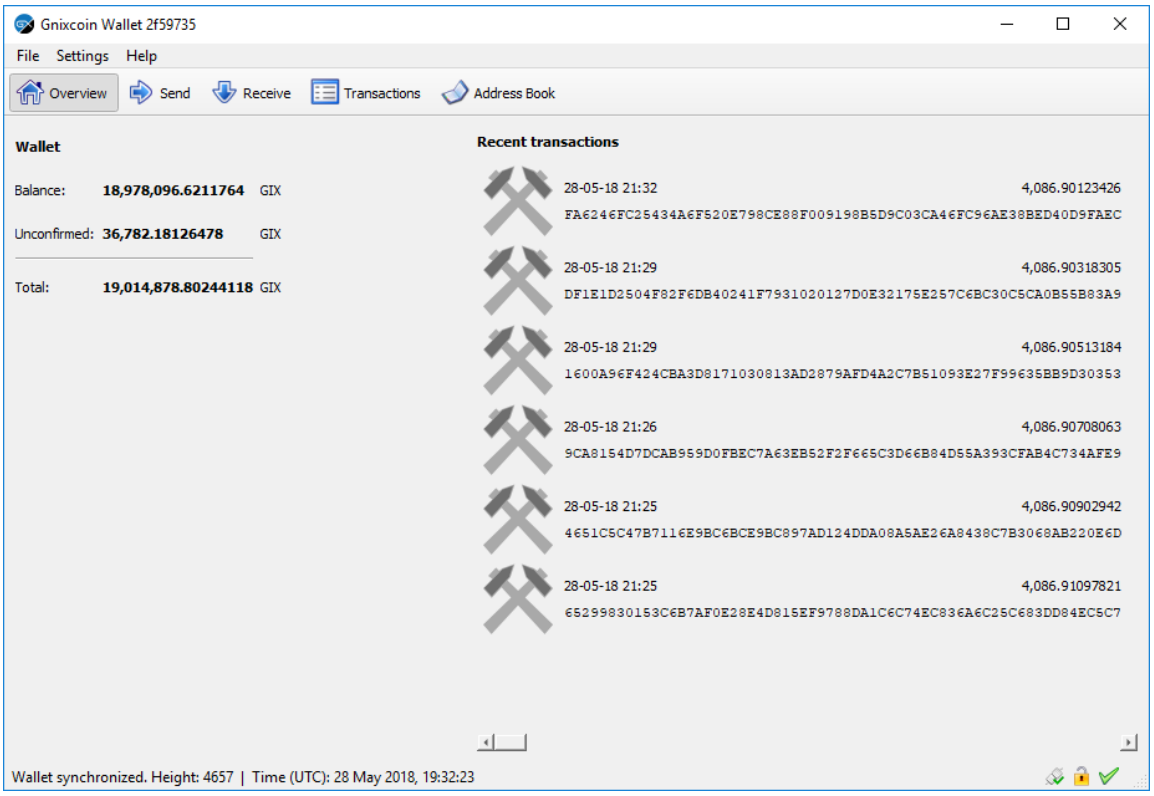
THE DIFFERENT PARTS OF THE GNIXCOIN PLATFORM

Software

Windows Wallet

Wallet software and mining software are already compiled and tested working with the newly created blockchain.

Windows Wallet has also been compiled and tested working. The wallet will also have a NFC transfer option that is specific for the Gnixcoin platform.



Mobile Wallet

Apps for both IOS and Android will be available. There will also be a special software for transferring funds between your NFC and your wallet.

Merchant Software

There will be a special software for receiving NFC payment connected to the mercants Gnixcoin wallet for receiving and refunding payments.

Mining Software

Mining software will be available after ICO is complete.

Hardware

Most mobile phones have NFC chip and you are able to receive and send payments from your Gnixcoin wallet to these.
If you want to transfer funds from your wallet on your PC you need to have a NFC reader/writer connected to your computer.
The wallet software makes the connection between your wallet and your nfc chip via the NFC reader.
The Gnix platform also works with NFC implants that you can put under your skin. These have been tested to work fine with most NFC readers connected to a computer.

The Gnix platform will also be able to handle Prepaid NFC chip that you can buy preloaded with Gnixcoins.

MERCHANTS OPTIONS

To be able to reach our goal we are developing an easy way for merchants to implement our Gnix platform.
As a physical store you only need to add a NFC reader to your computer and with software connect it to your Gnixcoin wallet.

For online merchants we have options for the most used ecommerce software like WooCommerce.
API is available for merchant and users to develop their own Gnix platform solutions.

TECHNICAL SPECIFICATIONS

NFC

Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1.6 in) of each other.

NFC devices are used in contactless payment systems, like those used in credit cards and electronic ticket smartcards and allow mobile payment to replace/supplement these systems.

NFC reader/writer

Enables NFC-enabled devices to read information stored on inexpensive NFC tags embedded in labels or smart posters.

NFC peer-to-peer

Enables two NFC-enabled devices to communicate with each other to exchange information in an adhoc fashion.

Network

Gnixcoin uses a peer-to-peer network. In the peer-to-peer network there are two different kinds of nodes. The seed nodes are the backbone of the network allowing incoming connections contrary to peer nodes that does not allow incoming connections. All nodes are constantly asking seed nodes if anything new happened in the blockchain, therefore they are always synchronised.

Untraceable payments

The ordinary digital signature (e.g. (EC)DSA, Schnorr, etc…) verification process involves the public key of the signer. It is a necessary condition, because the signature actually proves that the author possesses the corresponding secret key. But it is not always a sufficient condition.

Ordinary signature

Ring signature [1] is a more sophisticated scheme, which in fact may demand several different public keys for verification. In the case of ring signature, we have a group of individuals, each with their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a member of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her.

Ring signature

This concept can be used to make digital transactions sent to the network untreaceable by using the public keys of other members in the ring signature one will apply to the transaction. This approach proves that the creator of the transaction is eligible to spend the amount specified in the transaction but his identity will be indistinguishable from the users whose public keys he used in his ring signatures.

Untraceable transactions

It should be noted that foreign transactions do not restrict you from spending your own money. Your public key may appear in dozens of others' ring signatures but only as a muddling factor (even if you already used the corresponding secret key for signing your own transaction). Moreover, if two users create ring signatures with the same set of public keys, the signatures will be different (unless they use the same private key).

[1] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In ASIACRYPT, pages 552–565, 2001

Unlinkable transactions

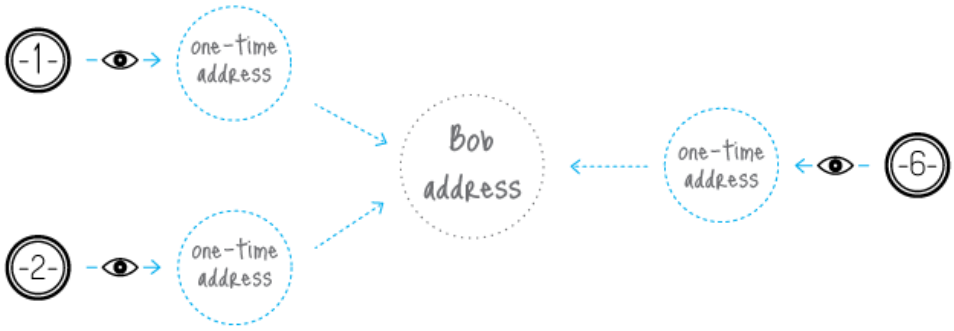
Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature. To avoid linking you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address.

Linkable transactions

Gnixcoin solves this dilemma by an automatic creation of multiple unique one-time keys, derived from the single public key, for each p2p payment. The solution lies in a clever modification of the **Diffie-Hellman exchange protocol** [1]. Originally it allows two parties to produce a common secret key derived from

their public keys. In our version the sender uses the receiver's public address and his own random data to compute a one-time key for the payment.

The sender can produce only the public part of the key, whereas only the receiver can compute the private part; hence the receiver is the only one who can release the funds after the transaction is committed. He only needs to perform a single-formula check on each transactions to establish if it belongs to him. This process involves his private key, therefore no third party can perform this check and discover the link between the one-time key generated by the sender and the receiver's unique public address.



Unlinkable transactions

An important part of our protocol is usage of random data by the sender. It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions (that is why the key is called "one-time"). Moreover, even if they are both the same person, all the one-time keys will also be absolutely unique.

[1] Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE Transactions on Information Theory 22 (6): 644–654, 1976.

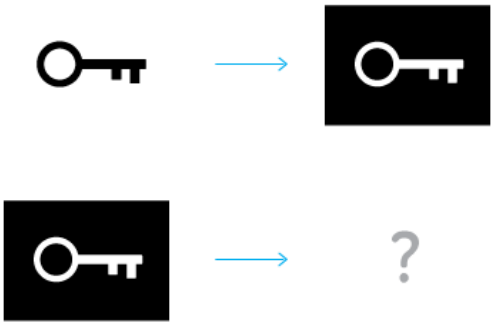
Double-spending proof

Fully anonymous signatures would allow spending the same funds many times which, of course, is incompatible with any payment system's principles. The problem can be fixed as follows.

A ring signature is actually a class of crypto-algorithms with different features. The one Gnixcoin uses is the modified version of the "**Traceable ring signature**" [1]. In fact we transformed traceability into linkability. This property restricts a signer's anonymity as follows: if he creates more than one ring signature using the same private key (the set of foreign public keys is irrelevant), these signatures will be linked together which indicates a double-spending attempt.

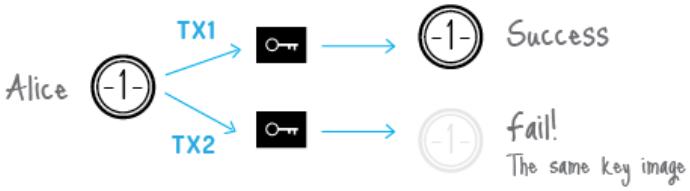
To support linkability Gnixcoin introduced a special marker being created by a user while signing, which we called a **key image**. It is the value of a

cryptographic one-way function of the secret key, so in math terms it is actually an image of this key. One-wayness means that given only the key image it is impossible to recover the private key. On the other hand, it is computationally impossible to find a collision (two different private keys, which have the same image). Using any formula, except for the specified one, will result in an unverifiable signature. All things considered, the key image is unavoidable, unambiguous and yet an anonymous marker of the private key.



Key image via one-way function

All users keep the list of the used key images (compared with the history of all valid transactions it requires an insignificant amount of storage) and immediately reject any new ring signature with a duplicate key image. It will not identify the misbehaving user, but it does prevent any double-spending attempts, caused by malicious intentions or software errors.



Double-spending check

[1] Eiichiro Fujisaki and Koutarou Suzuki. Traceable ring signature. In Public Key Cryptography, pages 181–200, 2007.

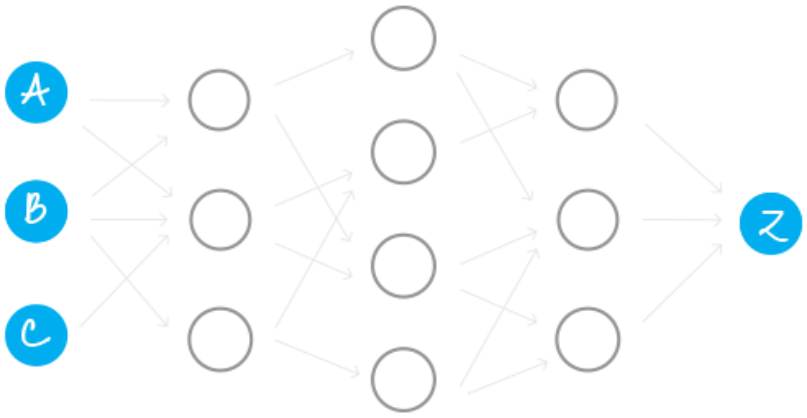
Blockchain analysis resistance

There are many academic papers dedicated to the analysis of the Bitcoin's blockchain. Their authors trace the money flow, identify the owners of coins, determine wallet balances and so on. The ability to make such analysis is due to the fact that all the transfers between addresses are transparent: every input in a transaction refers to a unique output. Moreover, users often re-use their old addresses, receiving and sending coins from them many times, which simplifies the

analyst's work. It happens unintentionally: if you have a public address (for example, for donations), you are sure to use this address in many inputs and transactions.

Gnixcoin is designed to mitigate the risks associated with key re-usage and one-input-to-one-output tracing. Every address for a payment is a unique one-time key, derived from both the sender's and the recipient's data. It can appear twice with a probability of a 256-bit hash collision. As soon as you use a ring signature in your input, it entails the uncertainty: which output has just been spent?

Trying to draw a graph with addresses in the vertices and transactions on the edges, one will get a tree: a graph without any cycles (because no key/address was used twice). Moreover, there are billions of possible graphs, since every ring signature produces ambiguity. Thus, you can't be certain from which possible sender the transaction-edge comes to the address-vertice. Depending on the size of the ring you will guess from "one out of two" to "one out of a thousand". Every next transaction increases the entropy and creates additional obstacles for an analyst.



Blockchain analysis ambiguity

Adaptive limits

A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer. Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum). Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state. Therefore, it always changes adaptively and independently, allowing the network to develop on it's own.

Gnixcoin has the following parameters which adjust automatically for each new block:

1) Difficulty. The general idea of our algorithm is to sum all the work that nodes have performed during the last 720 blocks and divide it by the time they have spent to accomplish it. The measure of the work is the corresponding difficulty value for each of the blocks. The time is calculated as follows: sort all the 720 timestamps and cut-off 20% of the outliers. The range of the rest 600 values is the time which was spent for 80% of the corresponding blocks.

2) Max block size. Let MN be the median value of the last N blocks sizes. Then the "hard-limit" for the size of accepting blocks is 2*MN. It averts blockchain bloating but still allows the limit to slowly grow with the time if necessary. Transaction size does not need to be limited explicitly. It is bounded by the size of the block.

WHERE ARE WE TODAY?

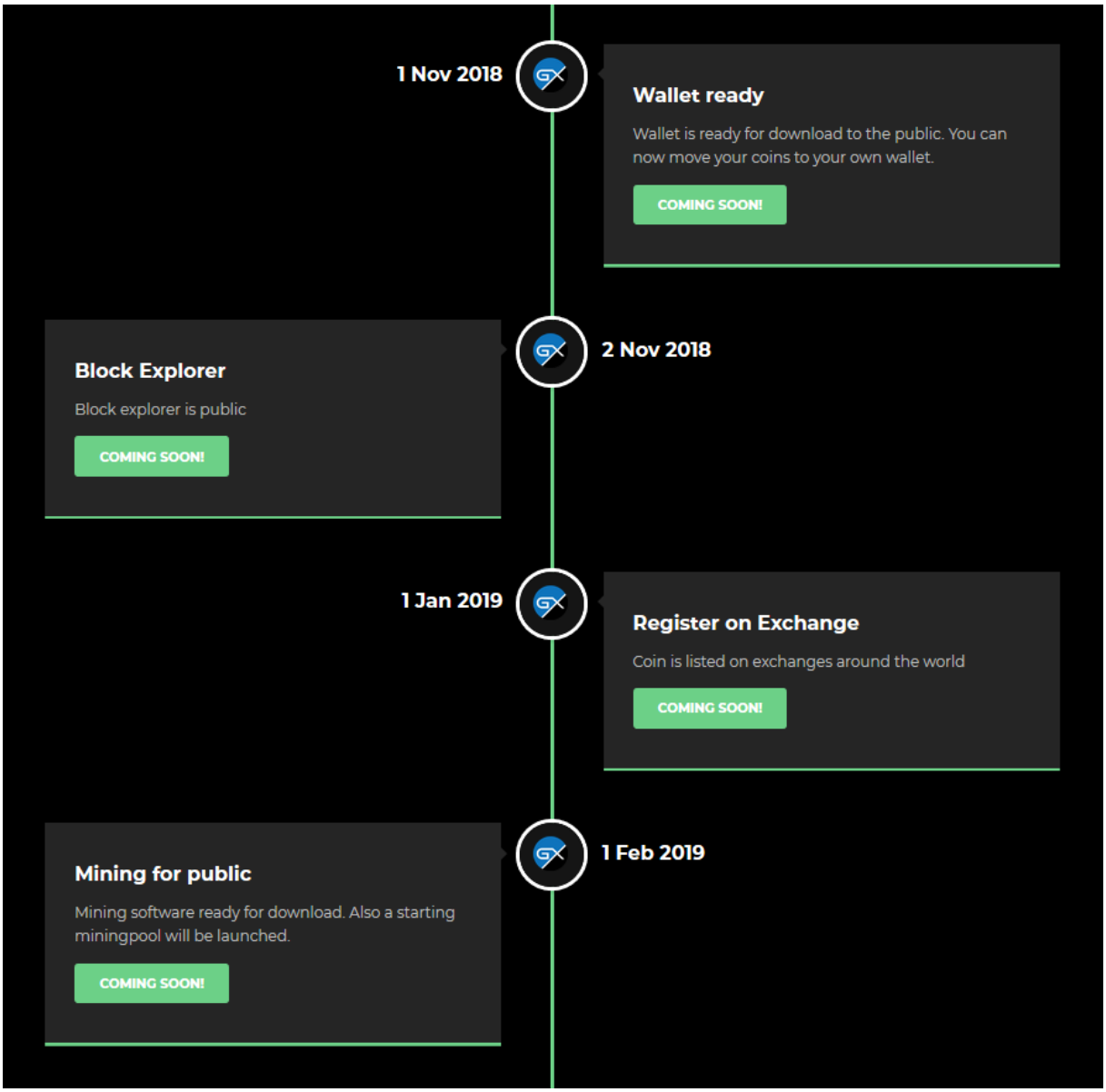
25 May 2018 - The first genesis block for Gnixcoin was mined at 25 May 2018. These are the first block in the blockchain for Gnixcoin

id <d4754733d8ff62ca1a3e0fd1abad08dbc8705426bf2c153051ca42e31f8c366d>
difficulty 1, nonce 70, tx_count 0
height 1, timestamp 1527237410, cumul_dif 2, cumul_size 301
id <95ee9114932799d39d466bceea07c53e15ca492f4de32839b70f3576baa93b8d>
difficulty 1, nonce 1291960593, tx_count 0
height 2, timestamp 1527237410, cumul_dif 3, cumul_size 301
id <f98b7cb359487d84b0efad1ab01347c731c235f98516039df2658234cb9bd5da>
difficulty 1, nonce 109678578, tx_count 0
height 3, timestamp 1527237410, cumul_dif 63, cumul_size 301
id <28bd28956d15234db23949b1309ca1b82415e6761165797ef69cc40bae38bda8>
difficulty 60, nonce 2198351041, tx_count 0
height 4, timestamp 1527237412, cumul_dif 3723, cumul_size 265
id <197c02f8c03b114886dad986ac5305642014add17e571cd295392c4a2ae8d476>
difficulty 3660, nonce 114963247, tx_count 0

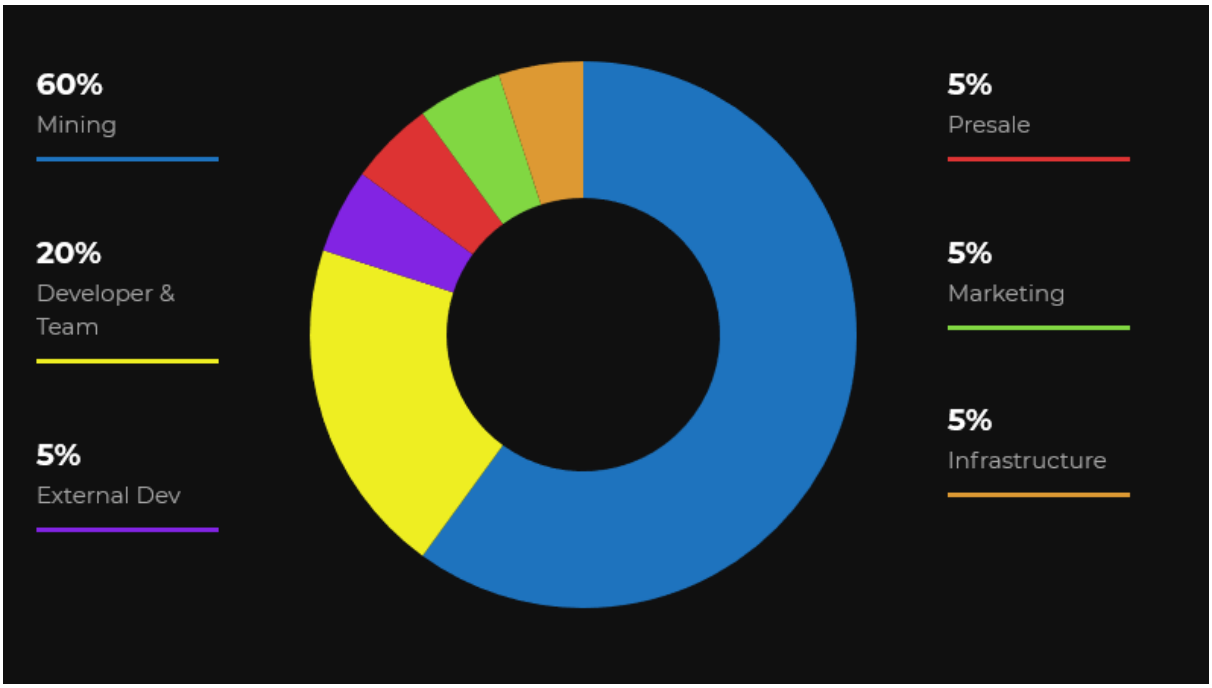
26 May 2018 - Website for Gnixcoin (https://gnixcoin.org) is online and receiving orders for premined coins.

Since 26 May 2018 working nodes have been online and supporting the network.

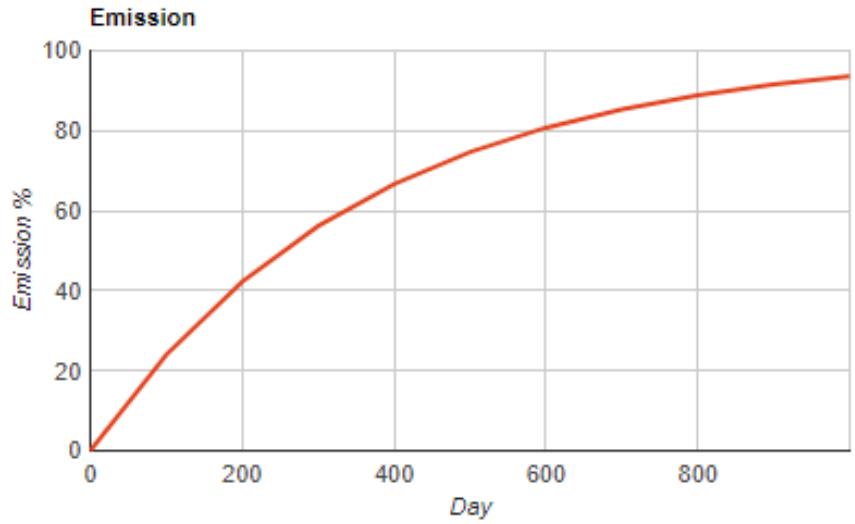
WHERE ARE WE GOING?

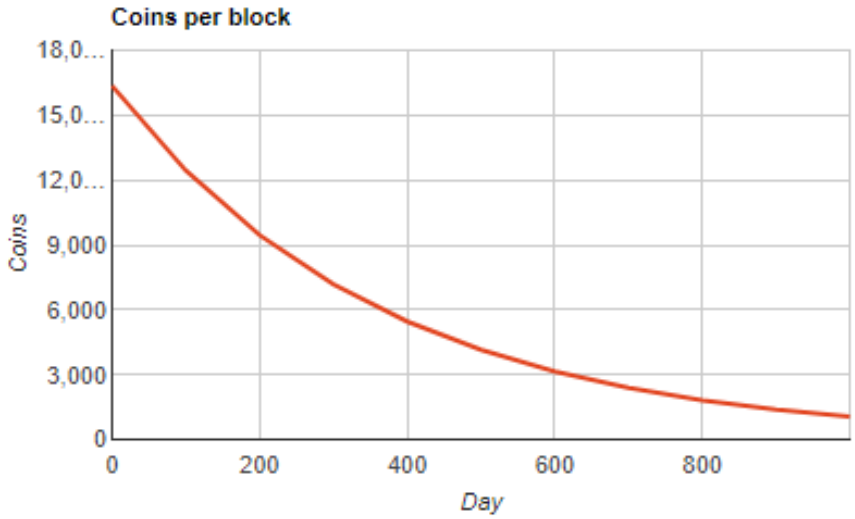


Distribution



Emission


Emission
100
80
60
40
20
0
Emission %
0
200
400
600
800
Day


Coins per block
18,0...
15,0...
12,0...
9,000
6,000
3,000
0
Coins
0
200
400
600
800
Day

REFERENCES

https://en.wikipedia.org/wiki/Near-field_communication
https://cryptonote.org/whitepaper.pdf