LINC

Decentralized Data Exchange Service

Whitepaper
Version 0.1
March 23, 2018

❑ CONTENTS

DISCLAIMER: this whitepaper is the preliminary description of the project which is now still at the beginning development stage. It includes only general concept and approximate development path. In the development process some technical details can be altered or added.

❑ INTRODUCTION

Bitcoin cryptocurrency, being created nearly 10 years ago, has given the world an amazing Blockchain technology and on its own example shown its exclusiveness and promise.

Decentralization, integrity, immutability and encryption are significant advantages of this technology and open the wide range of opportunities for realization of various projects sensitive to these factors. The most well-known at the moment application of this technology is cryptocurrency.

No doubt, cryptocurrencies have changed the whole world. It is pretty much impossible to imagine more successful blockchain application in real life of people, capable to create a huge community around, having a large coverage worldwide.

It should be noted also that in primary development the privacy issue wasn't considered. One of the blockchain main properties is transparency and availability to each participant and observer. Despite relative linkability complexity, all transactions in the network have excellent traceability.

At the same time, the privacy issue is particularly sharp now. And though after some time another cryptocurrencies were invented which provide an opportunity to carry out transactions in untraceable way, there still are open questions out of the financial sphere, but the privacy issue is not less sharp there. And last but not least, it concerns storage and data transmission issues.

❑ ISSUES IN DATA EXCHANGE

■ DATA BREACH

Leakage of data has significantly taken place in the recent year. Basically statistics from security companies, analysis institutions and government companies faces the problems of data leakage.

The root causes of data breaches are grouped into three categories. From the distinct data leak cases, the main reason of the data leak is from data leak by the human mistake. The two others are malicious or criminal attacks and system glitches.

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information, Personally identifiable information, trade secrets of corporations or intellectual property.

■ DATA SUBSTITUTION

Lack of integrity control can lead to the possibility of substitution of source data. In the vast majority cases certain data is need to be downloaded from central resources. The authenticity and integrity of the data is provided only by trust in the resource. Of course there are some hash checks or digital signatures but in most cases this is not paid due attention. Data available in one place can be changed without notice, whether authorized or not, not excluding the intention of causing harm. In most cases the recipient is not able to verify the reliability and authenticity of the information received.

Such an attack can be committed by the malicious actor for the purpose of misleading, having an informational influence or gaining access to the user's workplace by substituting an executable file on a trusted source.

■ DATA PRIVACY

In most cases data exchange goes through a central platform that acts as an transmission intermediary or an storage agent. Placing open data in temporary or permanent manner carries the risk of disclosure by a third party using access to a platform, authorized or not. Personal data, trade secret, intellectual property, internal corporate correspondence may be under the threat.

❑ LINC CORE

LINC provides a secure channel for digital data transmission without a possibility of intervention or any other type of influence by the third parties.

Integrity and security are ensured by a whole stack of technologies, where blockchain is the basic one.

■ DATA EXCHANGE BASED ON MASTERNODES NETWORK

First we should mention one of the major Bitcoin features. Its implementation has solved a complicated math problem. The bitcoin network works in parallel to generate a chain of Hashcash style proof-of-work (known as mining). The proof-of-work chain is the key to overcome Byzantine failures and to reach a coherent global view of the system state.

After that there was a variety of ideas offered applicable to cryptocurrencies and based on the PoW concept, but using alternative resources as Proof. The most common at the moment is the Proof-of-Stake concept. The Proof-of-Service is not less significant, though.

The DASH project has taken a big step in the Proof-of-Service concept development, having created the Masternode system carrying out useful services for the network and earning a certain reward for the contribution.

The PoSe concept has been borrowed and used in the LINC platform. The masternodes' role in the network is stated as the key nodes which provide reliable, safe and private way of data exchange between the network participants.

■ DATA EXCHANGE PROTOCOL

The LINC platform gives a chance to both exchange data between two certain participants and distribute data among a great number of recipients.

Data transmission is initialized on the client side. Before being sent the data is hashed, if necessary is split up, also. Then for each piece of data a special date transaction is formed which contains the recipient's address, the data hash, the encrypted data and the signature. Transaction is broadcasted to the network of masternodes.

Masternode, having received the signed transaction, checks its validity. This stage removes any possibility of data substitution via request interception from the client to the node by the third party (so-called MITM attack). Also all the limits are checked including the maximum size of the data transmitted, compliance of fee.

If the transaction was accepted by masternode, depending on the parameters the data are spread between a certain quantity of masternodes, each of which saves the data transmitted. The transaction is recorded in the network. At the same time the data itself isn't stored in blockchain, but their hash is.

The recipient scans blockchain, checking if he needs to receive any data. In general, if there is such request, the recipient asks the network of masternodes to give him the data, having sent a special request with his digital signature. The network first checks the request reliability, and after that spreads the request among the network with an order to give the data to the client. After the receipt confirmation the data is removed from the network.

The data is still stored on the masternode for the certain period of time determined by the client and corresponding to the transaction fee. This way the maximum protection against overload and overflow is achieved.

The network uses InstantX and PrivateSend technologies for usual transactions for the purpose of money transmission. For data transmission special expansions for the modules realizing these technologies shall be used.

■ INTEGRITY AND DELIVERY GUARANTEE

Thanks to creation of peer-to peer network architecture, application of data encryption and also use of the uniform transparent database based on blockchain technology, the complete integrity of the data transmitted is ensured.

Delivery is ensured by data distribution inside Masternode network. This minimizes the possibility of losing the data even if one or few masternodes fail.

■ DATA-TRANSCATIONS

Data-transactions are the network special transaction intended for data exchange between participants. These transactions have the zero-input option. In other words, you don't have to specify the number of coins you are sending, but fee is obligatory.

Besides standard data, each data-transaction contains hash of the data transferred, data encrypted with a private key and the signature.

However, each transaction has a few parameters regulating data sending and storing protocol such as data distribution depth inside the network, storage duration, anonymous transfer parameters.

Depending on these parameters the fee amount is calculated.

The purpose of fee is to stimulate the processing of such transactions by the network. Also it works as one of the network overload protection mechanisms. This fee is spread between masternodes only.

In general, these transactions processing is based on InstantX technology.

■ P2P EXCHANGE

LINC network provides participants with opportunity to initiate peer-to-peer exchange directly with no need to involve any third parties. This exchange method is way more preferable since it decrease significantly the network load, and therefore the fee for participants is lower, too.

To establish the exchange channel between participants each of them broadcasts the data-transaction with disposable keys in the network. The point is to exchange those between participants and then establish encrypted and protected channel.

Each participant can use any of the network nodes in case if he cannot open the external port on his own because his location is outside the NAT. In situations like that the node initiates the so-called tunnel hoping.

■ DATA FRAGMENTATION AND MULTI OUTPUTS

The network has the data fragmentation option. A data package can be divided into several parts and sent to the recipient by few separate transactions. Each data package has its own header containing its queue information. This way the client when receiving a few transactions, can define the exact queue of each part and, having scanned all the necessary transactions, he can put them back together.

Data-transactions, just like ordinary ones, can use multi outputs. This option might be very useful when you need to send the same package to different recipients. In this

case the data is sent once and there is no need to broadcast one package into the network over and over again for each recipient.

PRIVATE DATA EXCHANGE

Another network main feature is anonymous data exchange. This opportunity gives the exchange participants a chance to minimize the trackable connection between them both for each other and the third party observer.

To hide the sender the PrivateSend module add-on is used. First the fee amount necessary to send the package is calculated. After that the same mechanism is run which denominates the money into some indistinguishable standard nominal values which are subsequently spread among newly created anonymous wallets. The minimal nominal value is the fee amount necessary to send the minimal data package.

After denomination the package for sending is shredded in a very specific way. It is divided into several parts defined randomly, and each part's size equals one of the possible nominal values.
Then, with compliance to the same PrivateSend principle, the transactions are recorded in the network.

Another method to hide the send is to use the so-called Void transactions. These ones don't contain the recipient address explicitly. The address in encrypted with the recipient's public key. And to get the data, he has to scan all the transactions of similar type, trying his private key to decode the address.
Such transaction may be used both for ordinary data sending and for hidden P2P channel establishment.

Additional anonymization is achieved by using a simple relay mechanism when calling the masternodes.

NETWORK OVERLOAD PROTECTION

Data exchange mechanism via the limited number of nodes implies risk of network overload as by the participants' legitimate actions, as malicious attempts.

Therefore the overload protection is crucial problem to solve for ensuring the network workability and failure prevention. That's why it's important to include a number of features providing full protection from all possible factors threatening the network's proper operation.

To prevent the failure inside the network the following methods may be used:

- Usage of P2P by clients only when that's possible. This approach significantly accelerates the data transferring process and decreases the network load. The only thing network does is allows its participants to be sure about correctness and integrity of the data transferred. But this method requires a certain trust level between participants.
- Fees imposed on the data size, its storage duration inside the network and additional anonymization parameters. This way the possibility of flood and spam is significantly lowered since the feasibility of such mailing methods is decreased by influencing the economical aspect.
- Additional parameters, such as size, speed and load limits, may be set inside the network.
- Fragmentation, deferred sending. The data may be divided into several parts and sent one by one while the network load is decreasing.
- Network scaling. Addition of the auxiliary nodes level.

SCALING

In the process of the network development some components will be implemented allowing to increase the network capacity and expand the opportunities it gives to participants. Thus, the following features is soon to be available:

- Deferred data transfer. Clients will have an opportunity to get the network current parameters defining data exchange duration. If need, the data might be divided into several parts and sent one by one with some time intervals.
- DxNodes implementation. Such nodes are not actual masternodes and they don't need to get the obligatory deposit from the holder. These ones cannot work with InstantX and PrivateSend transactions, but they can process data-transactions and store the data. In order to accept the node the masternode voting system is planned to be used. This way a certain trust level and undesirable actions can be achieved.
- For masternodes and DxNodes the Scoring system is going to be implemented. This is a special mechanism of node participation rating inside the network. Thus, nodes with best capacity, disk space and RAM will get the highest ratings. This rating will define the share the node will receive from fee for each data-transaction processed.

❑ LINC PRODUCTS

On the basis of LINC platform development of few more products is planned. All of them are extensions of ordinary data-transactions and whole LINC network. Each of them has the following purposes:

- to provide a friendly interface for using LINC features: to exchange data whether it will be emails, instant messages or even voice and video messages;
- to provide users with the most reliable and protected data exchange channel with no need to make any extra preparatory measures, cryptography or encryption methods knowledge. The only thing required is to exchange their addresses and use the program friendly interface;
- to provide a new beginning for LINC network by attracting new users interested in this kind of products.

At the moment two products are already planned:

- LINC EmailClient
- LINC File Exchanger
- LINC Instant Messenger
- LINC VoIP Client

It's planned to launch products compatible with all platforms, both desktop like Windows, OS X, Linux, and mobile like Android, iOS.

All products will work together within one program based on LINC Wallet.

■ LINC EMAIL

LINC Email allows the network participants to exchange messages using the habitual email concept and receiving/sending system.

All messages are encrypted and stored on the local storage device of each user. Thanks to data-transactions technology, almost all functions of email services are available, including copying the message to several recipients, hidden copy, Reply-To, Return-Path, delivery notification.

In the classical form the email address function will be performed by LINC network address. Later the aliases are planned to be integrated, too.

Since LINC mail client will work similar to POP3-protocol, the possibility of POP3->LINC Network adapter creation sure can't be removed. This way participants

will have an opportunity to send emails via almost the same programs they've already got used to.

■ LINC FILE EXCHANGE

The purpose of this product is to provide users with a friendly interface of file exchange via LINC network.

Besides its main function of files exchange, some extra functions will be implemented, such as the following:

- friendly interface to set the sending parameters
- file preview (images, texts)
- built-in file and directory collector
- built-in file compression to save the traffic and lower the fee

■ LINC INSTANT MESSENGER

The purpose of this product is to provide users with an opportunity to send instant message to each other via protected channel using P2P or masternode session.

When using P2P session, the network receives only one transaction from each client (to exchange the encryption keys). After that the direct connection between the clients is established without LINC network assistance.

When using masternode session the permanent two-way information exchange is required in real-time mode via LINC network. Since the standard exchange method would overload the network and fill the blockchain with excessive records, this type of session requires the data exchange optimization solution. The planned solution at the moment is to hold the certain deposit by the msternode participating in the exchange process. The deposit size is set by user when the session is initiated. Then control over money is given to the masternode. When the session is terminated, the masterode returns the deposit minus the fee.

■ LINC VOIP CLIENT

VoIP client will allow users to call each other and send voice message.
Just like the previous product, this one implies both direct and P2P sessions and exchange via LINC, network with deposit holding procedure.
One of the product greatest prospects is opportunity to make calls not only inside the network, but in the GSM via gateways. Users will be able to pay for such services by LINC cryptocurrency.

❑ LINC PLATFORM DEVELOPMENT

Besides main products on the basis of LINC platform, implementation of two important network components is planned: LINC Decentralized Governance and LINC DataMarket.

■ LINC DECENTRALIZED GOVERNANCE

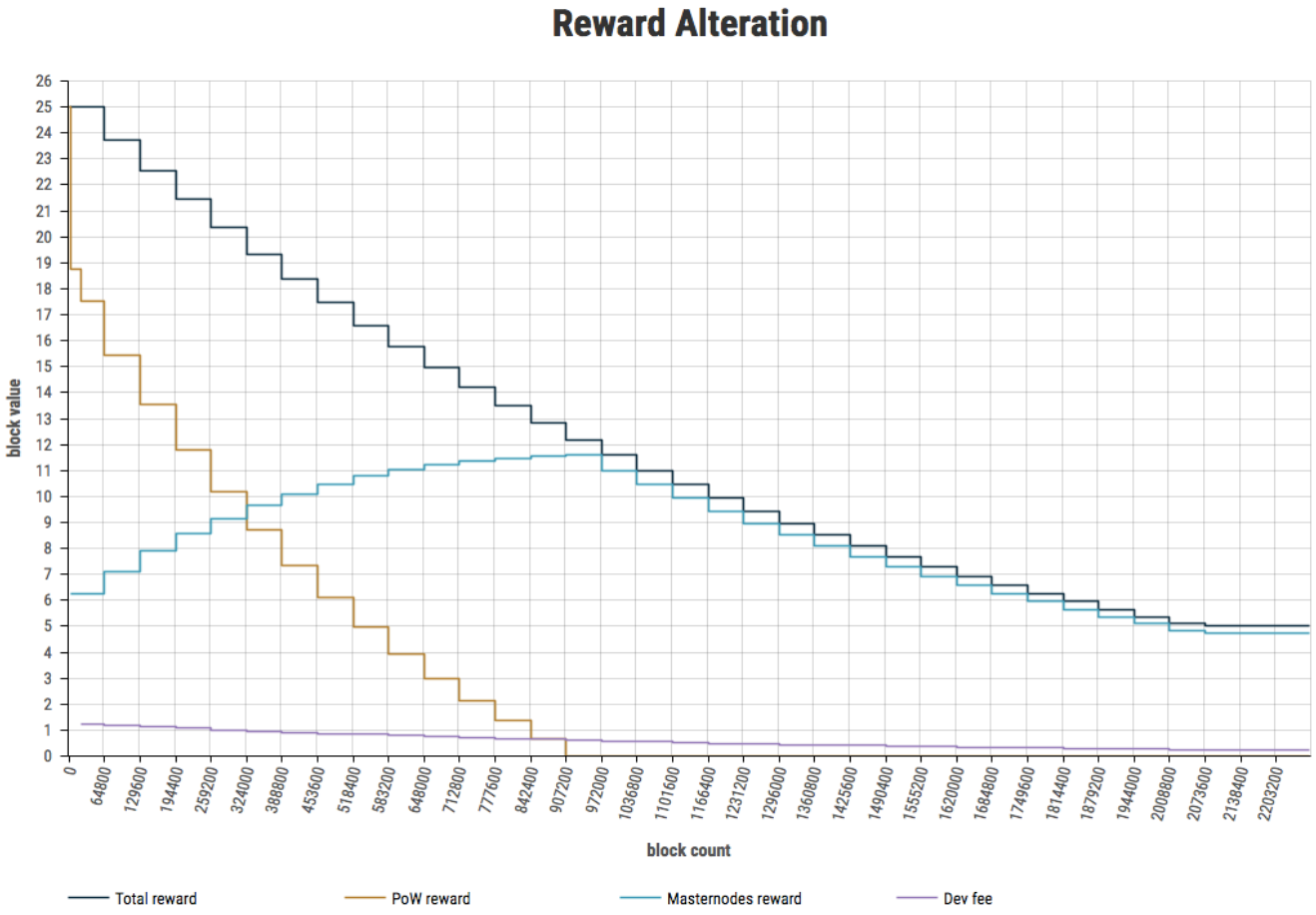
This component uses the same name DASH project technology and allows key network participants (masternode owners) to make decisions on the product development. Every month the certain budget is allocated depending on the fees acquired. This budget then can be spent on various initiatives. Such initiatives support is carried out by masternode owners using simple voting system. Any network participant can offer an initiative by paying for it a certain amount of fee. In total 30% fees will go to budgeting.
Launch of each such component is going to be a major event for the whole network and it might have a great influence on the following platform development vectors.

■ LINC DATAMARKET

This component implies a great variety of functions with wide opportunities which will be described in detail later according to the terms specified in the RoadMap. The main function is to provide an opportunity for data trading between the network participants.

❑ TECHNICAL SPECS

TICKER	**LINC**
TYPE	**PoW/PoSe** Blocks 2-3600 - PoW Blocks 3601-907200 - PoW / Masternodes Blocks 907201-max - full PoSe
TOTAL SUPPLY	**50.000.000**
ALGO	**Neoscrypt**
DIFFICULTY ADJUSTEMENT ALGO	**DGW (every block)**
BLOCKTIME	**120s**
INITIAL REWARD	**25**
INITIAL REWARD ALLOCATION	**70% / 25% / 5%** PoW / Masternodes* / dev fee** * starting from 3600 block ** starting from 21600 block
REWARD ALTERATION	**every 64800 block** - total reward will be decreased by 5% - Masternodes reward will be increased by 5% from total reward - PoW reward will be decreased by 5% from total reward After reaching ~2.100.000 blocks reward will be fixed to 5 LINC Budget system allocation may be implemented in the future
MASTERNODE COLLATERAL	**2500**


Reward Alteration
block value
block count
Total reward
PoW reward
Masternodes reward
Dev fee