

# LIGHT PAPER

## Dynemix cryptocurrency platform

and

## Liberdyne messenger

**Dynemix** is a blockchain platform of the next generation designed to become the first worldwide-adopted cryptocurrency capable of competing with conventional consumer-level payment infrastructure on equal footing and substituting it entirely eventually.

**Liberdyne** is a P2P secure messenger powered by the Dynemix platform. Liberdyne is designed to compete with popular centralized messaging solutions on equal footing while at the same time offering users a superior level of security and privacy.

Both components of the project were developed in conjunction and are interrelated and mutually beneficial, which allows us to introduce features previously unavailable on both the cryptocurrency and instant messaging markets.

The following light paper contains a brief description of the project. To learn more details about Liberdyne and Dynemix, please refer to the respective white papers. Any updates to this document can be made without prior notice.

The following paper does not contain any coin purchase offerings or any other information on the initial coin distribution.

[www.liberdyne.com](http://www.liberdyne.com)

# I. Background

In 2009, the first modern cryptocurrency, Bitcoin, was created. It was introduced by its creator as a decentralized payment system (literally “a peer-to-peer electronic cash system”) and was apparently supposed to provide an alternative to the modern conventional fiat financial framework. In practice, however, it failed to fulfill the creator’s intentions and became a speculative asset or an inflation-hedging tool instead of an alternative monetary asset.

All subsequent projects followed the same path, and we can state that to date there is no cryptocurrency that we can actually call a currency, i.e., a financial asset that can perform all three main functions of money:

- Medium of exchange.
- Unit of account.
- Store of value.

Dynemix is designed to fill that empty niche and present a next generation blockchain payment system capable of competing with conventional centralized payment infrastructure and even substituting it entirely, thus becoming the global money of the future.

# II. The Ultimate Cryptocurrency

To bring our vision to life, we put our best effort into creating solutions for the four main issues that are unresolved in current generation platforms:

## 1) Convenience

Most people are used to the level of convenience provided by the modern financial infrastructure. Unfortunately, current generation blockchains cannot offer the same user experience, which is why despite all the benefits that decentralization can bring, we cannot count on the mass adoption of a cryptocurrency unless we are able to match the level of convenience of conventional payment systems.

## 2) Decentralization

The recent trend shows that in the pursuit of reaching better scalability, many developers forget the fundamental reason for blockchain’s existence and unhesitatingly trade decentralization for higher potential throughput and other parameters. We do not support this approach since we believe a centralized blockchain to be essentially pointless. Instead, we managed not only to reach the same level of decentralization provided by Bitcoin but to outclass it by far.

## 3) Economic potential

The cryptoeconomy in its current state is mostly characterized by speculative trade. If we intend to introduce a cryptocurrency that will serve as a medium of exchange, we should provide a completely different model of economic management with an incorporated flexible policy rule, which can perform in a similar manner as central banks.

## 4) Overcoming entry threshold

Current generation platforms generally cannot provide user-friendly interaction, and this keeps many ordinary users from trying out crypto. We need a simple, familiar product with an intuitive interface that allows access to the cryptoworld even for users without any specific knowledge. If we manage to provide users with some coins on a free basis, and without the need to employ

exchanging services, this could also trigger more interest from a general audience. To achieve this, the cryptocurrency should be distributed as a part of a complete user-friendly product.

### III. Dynemix Cryptocurrency Platform

Dynemix is a decentralized, permissionless, account-based blockchain system powered by a unique proof-of-stake BFT consensus protocol.

Dynemix is designed to achieve one goal: to become the first widely adopted decentralized means of payment (commonly called a cryptocurrency) and compete with conventional centralized payment infrastructure on equal footing. To achieve this goal, we have developed a novel consensus protocol from scratch and introduced a number of new approaches to various aspects of DLT.

Dynemix operates in a symbiotic relationship with the Liberdyn messenger, which allows it to introduce features not previously available and to progress toward the stated aim.

Dynemix is endowed with the following features:

**a) Transactions are free.**

In blockchain systems, users have to pay fees for transactions to be processed. Fees are not fixed and are defined by the current system load and the complexity of the smart contract (in decentralized virtual machine platforms).

This severely detracts from the user experience in comparison to the conventional centralized payment infrastructure where fees are either predefined or charged to vendors (which is why payment by credit card appears to be free of charge for a user).

With Dynemix, on the other hand, common transactions are free. Fees are charged only for business-related transactions that require multi-outputs, which makes the user experience superior not only to other blockchains but to centralized payment systems as well.

**b) All transactions are finalized within 6 to 16 seconds after being sent to the system.**

Most current-generation blockchains rely on a leader who proposes block candidates. Other nodes vote for the proposed block, and the network either accepts or rejects it.

According to this approach, the leader assembles the block at his or her own discretion and is free to reject any transaction, which severely degrades the user experience compared to conventional payment systems, as they process all transactions without any preference. Furthermore, this approach creates the preconditions for censorship.

With Dynemix, on the other hand, every transaction broadcast into the network is added to the next block, which is instantly finalized. This is achieved through our novel multivalued block proposal algorithm, which provides a level of user experience very close to conventional payment systems and is far superior to any currently available blockchain design.

Being linearly consistent, the Dynemix protocol guarantees that no forks can occur unless an attack is committed, which is why finality is reached instantaneously without any additional confirmations.

**c) Dynemix scales to 10,000 TPS and higher.**

We put a lot of effort into the optimization of the protocol to make it capable of scaling up with the growth of demand. According to our expectations, Dynemix should be able to scale to 10,000 TPS and beyond with moderate hardware and bandwidth requirements. With the help of our sharding scheme, such throughput can be achieved within the first layer, which means that no second-layer solutions, such as payment channels, are necessary.

Moreover, the Dynemix protocol is designed in such a way that it can be further adjusted to provide more scalability if needed.

**d) Dynemix is highly decentralized.**

Unlike many recent blockchain projects, which solve the scalability issue by adopting a highly centralized architecture, Dynemix is designed specifically to provide the highest level of decentralization, one which surpasses the level of classic PoW blockchains such as Bitcoin as well as many recent solutions.

We believe decentralization to be the main reason for the invention of blockchain technology, which is why we put a lot of effort into making Dynemix truly decentralized and consistent with the original ideas of Satoshi that were embedded, but not embodied, in Bitcoin.

**e) Dynemix is highly secure.**

Making the system more scalable with the help of a sharding solution inevitably reduces security. With the help of our novel two-layer validation model, Dynemix manages to increase scalability without sacrificing security.

The first layer provides a reduced overhead, thus improving decentralization, and the second layer increases the adversarial threshold, at the same time keeping the achievements of the first layer intact.

**f) Dynemix can be minted on a common PC at home.**

Due to its excellent optimization, the use of sharding technology, and the new consensus protocol, it is possible to run a full node on common home-class hardware. No professional hardware is required.

This helps Dynemix to remain a true peer system and resist minting professionalization (which leads to the concentration of power), thus embodying the initial ideas behind blockchain technology.

**g) Dynemix introduces a revolutionary economic model.**

The system features a unique coin supply management system that provides a solution to the problem of economic development.

The Dynemix design enables it to fairly distribute newly issued coins among almost all users of Liberdyne instead of accumulating them in the hands of professional minters, thus bringing in an innovative cryptoeconomic model based on the concepts of helicopter money and basic income.

The incorporated model of a decentralized algorithmic central bank is far ahead of the current stablecoin implementations, since it allows to target the desired macroeconomic variables instead of simply balancing the value of coins against exogenous currencies.

**h) Dynemix is compatible with financial privacy.**

Dynemix is designed to incorporate a new cryptographic solution that encrypts transaction data and can allow financial privacy to be provided to all users.

The protocol is optimized for the use of an additive homomorphic cryptosystem with ZK-proofs to encrypt balances and hide user interaction.

**i) Dynemix solves the entry threshold issue by being integrated into Liberdyne.**

Dynemix is integrated into the Liberdyne messenger to provide users with a more familiar experience. Newcomers do not have to study the peculiarities of cryptocurrency technology to start using Dynemix. Instead, the user only needs to install Liberdyne and start using a familiar type of app that happens to have additional functions, which are available through a simple

and intuitive interface. Minting functions are set up automatically, so the user does not need to do anything at all.

*The combination of these features makes Dynemix the ultimate blockchain payment platform and a true breakthrough in cryptocurrency technology.*

## IV. The Liberdyne Messenger

Liberdyne is a decentralized P2P messenger with an emphasis on security and privacy.

Liberdyne uses the account base and transport protocols of the Dynemix blockchain system, which greatly improves the messenger's capabilities.

Liberdyne is designed to withstand the significant load created by a userbase of a size comparable to that of popular centralized solutions.

### 1) Liberdyne and Dynemix blockchain

Liberdyne is not entirely blockchain-based. We didn't aim to use DLT for marketing purposes, and blockchain is only engaged to the extent that helps build a better system and improve the user experience:

- Liberdyne uses the Dynemix namespace as a secure, decentralized, and consistent key storage that is highly resistant to MITM attacks.
- Dynemix provides rewards for users who share their resources to support Liberdyne's features.
- The Dynemix wallet is integrated into Liberdyne to provide a user-friendly experience with a cryptocurrency.
- Liberdyne shares low-level transport protocols with Dynemix, making user interaction significantly more secure and greatly impeding malicious meta data analysis.

### 2) Unbiased content filtering

Since the Dynemix protocol features embedded strong censorship resilience, we used the emerging opportunities for censorship-free interaction to develop a novel approach to content filtering.

To ensure free communication and at the same time prevent users from malicious activities, we decided to apply limited content filtering via guardian oracles, which turns content filtering into a separate service.

These oracles can be hosted and administrated by different parties, whereas a particular solution (or a combination of such) that is engaged at any given time is set through the preferences of the app.

This ensures an unbiased approach to filtering and at the same time provides sufficient protection from malicious content distribution. Even if the developers (or other entities controlling the default guardian oracle) try to apply any biased filtering rules, users are free to choose another filtering solution, which renders such attempts inefficient.

Content filtering as a service is a novel approach that provides a solution to a highly relevant issue of biased censorship applied by Big Tech in favor of certain political agenda.

### 3) Delivery to offline guys (DOG)

If the recipient of the message is offline, direct P2P interaction is not possible and the message cannot be delivered. In centralized messengers, servers are used as delivery relays, so the message is stored on a server that remains online until the recipient reconnects to the network, and thus the

problem is solved. In a P2P network, peers perform the relay functions, which is why such a solution does not work.

To solve this problem, we implemented a special protocol of delivery to offline guys or *DOG*. If the sender cannot connect to the recipient, he finds several other peers, called DOG nodes (or simply *dogs*), and commits the delivery to them, thus forming a *pack*. The pack then delivers the message when the recipient reconnects to the network. Dogs are rewarded with newly issued dynes, which serves as the main solution for the distribution of *helicopter coins* in Dynemix.

#### 4) Secure anonymous tunneling across network (SATAN)

P2P architecture does not completely solve the metadata collection problem. Although it greatly obstructs malicious analysis attempts in comparison to a centralized design, an adversary can still run a number of peer nodes to keep partial track of user interactions. To solve this issue completely, a specific solution was required.

We have implemented a secure anonymous tunneling across the network (*SATAN*) protocol that allows users to send and receive messages through a chain of relays, thus completely hiding their IP addresses behind the relay nodes. Furthermore, the relay nodes cannot know for sure which particular node is the sender or the recipient of the message.

All that a possible intruder can see is that the recipient's user account has received some sort of message from an unknown account. Essentially, *SATAN* uses the principles of onion routing (like the Tor browser).

#### 5) Modes of operation: private or social

One of the key goals of the project is to provide the possibility of fully private system usage and to secure personal data. The problem is that many features that consumers are used to are not compatible with such standards of security and privacy, so it is necessary to sacrifice one for the sake of the other.

At the same time, we understand that the majority of users do not care much about privacy and may be ready to trade it for better functionality. This means that we either have to compromise or offer two separate solutions – one for better privacy and one for a better user experience.

We have chosen to follow the second path and develop an application that can function as a tool for secure and anonymous communication or as a social platform, depending on the user's needs.

A very important feature is that users of both modes will stay in the same single ecosystem and be able to interact without any difficulties. Privacy mode users can communicate with socialized users without any threat of disclosure.

As the features and preferences of these modes differ drastically, instead of just offering to let users tweak everything themselves, which can turn out to be a challenging task, *Liberdyne* will feature a simple switch that activates one of the modes. The user will be able to switch to the social mode any time, however, the return to the private mode can become unavailable if the user engages certain features that deanonymize the user irreversibly.

## V. Economics of Dynemix

We believe that neither Bitcoin nor any other currently available platform can accomplish the initial goal of blockchain technology: to become a *global universal medium of exchange*. Apart from technological imperfections, the problem also lies in an inappropriate economic model.

To date, the cryptomarket is characterized mostly by speculative trade and has little prospects to create a real economy. To accomplish this task, the *Dynemix/Liberdyne* platform was endowed with the following features:

## 1) Decentralized algorithmic central bank

The economic model of Dynemix features a breakthrough design of a *decentralized algorithmic central bank* capable of simultaneously balancing the value of native coins against fiat currencies and directly maintaining a targeted *interest rate*, which allows to indirectly target an optimal level of *inflation* and *output growth*.

Unlike previous attempts to build a cryptocurrency that is capable of performing the functions of money, which were concentrated around the concept of a stablecoin, we took a step further and designed a model of a stable economy. The key difference is that our model engages all channels of monetary transmission:

- a) When Dynemix is used as an ancillary currency in addition to an exogenous fiat currency, it balances the demand discrepancies that originate from the exchange rate and nominal interest channels, thus keeping the exchange rates stable. A significant upgrade over typical stablecoins is the ability to balance the value against all exogenous assets simultaneously instead of being pegged to a particular asset or a set of such, which provides independence.
- b) When Dynemix performs as a fully-fledged economy and an exclusive legal tender within a specific economic zone (up to the entire global economy), it can target a desired natural rate of interest directly and desired inflation and GDP growth indirectly. This feature is exclusive to our model and is not supported by any available cryptocurrency.

In addition to that, the economic model of Dynemix doesn't require any special assets as seigniorage-style models do. Dynemix operates exclusively with native utility coins, which circumvents the engagement of securities and the necessity to comply with the respective legal procedures and requirements of regulators.

## 2) Wide egalitarian reward distribution

In current generation blockchains, newly issued coins are distributed as rewards between block producers. Since PoW miners or PoS validators both adhere to the professional approach, coins are mostly perceived as a speculative asset, which impedes the development of a real economy.

To break the self-reinforcing speculative loop, coins should be dispersed among the majority of common users, who, instead of transferring them to stock exchanges, will more likely use them directly to purchase actual goods or services, thus forming the real market.

To achieve this goal, Dynemix features a two-level coin distribution model: only a fraction of the issued coins are collected by minters, whereas most of issued dynes are transferred to the nodes that perform DOG functions. Since DOG can be performed even on mobile devices, we assume that rewards will be distributed among the vast majority of Liberdyn's active users, thus making the Dynemix monetary policy an embodiment of the concepts of *helicopter money* and *basic income*.

## 3) Overcoming speculative phase and transitioning to real economy

Even if we make dynes initially less attractive as an investment asset, we hardly believe that the speculative phase can be avoided completely. For this reason, we designed the reward distribution system in a way that can help the platform overcome speculative pressure and transition to a real economy.

The algorithm of reward distribution for DOGs is such that the fewer users who are online, the greater the reward each of them receives. This should lure users, who, in pursuit of a larger reward, will tend to start using the system as soon as possible. The influx of users can attract speculators due to the expectations of the further growth of the platform. As the speculative pressure raises the market cap of the platform, the rewards become even larger in real terms, thus attracting more reward hunters and creating a self-reinforcing loop.

With the help of this solution, we expect the speculative factor to be balanced by the respective influx of users who will spend dynes in the real sector. After the investment potential inevitably

exhausts and the model of a stable economy is engaged, such users will form the base of the subsequent economic development.

## VI. Marketing Potential

Since our main goal is not just to create a new advanced platform for the cryptocommunity in its current state but to spread blockchain technology all over the world via the creation of the first mass-market product, it is absolutely clear that about 99% of our target audience has a very limited basic understanding of the technology. While we can convince some portion of the cryptocommunity members of Dynemix's strong potential simply by explaining all the advantages of the platform, this will not work with people who are not much into blockchain technology.

To accomplish this, we need some simple, and at the same time striking, "killer features" that can be easily explained and understood, thus driving public attention to the project by themselves. Fortunately, we have a couple of such.

### 1) Liberdyne – next generation decentralized private messenger

The revelations of Edward Snowden, according to which the US special services had been actively collecting people's private information on a global scale, led to the rise of discussions about creating a secure means of communication and forced developers of messaging apps to implement end2end encryption.

The question of user privacy can be a strong basis for a marketing campaign. Liberdyne makes a huge step toward user privacy in comparison to currently available centralized solutions; it is a next-generation product that works fully P2P without any servers involved. In combination with peer-relaying technology (SATAN), which provides a whole new level of privacy and security to every user, it can finally give users confidence that their communication is reliably secure.

Our novel approach to content filtering (which is described above) can also put an end to biased censorship, which has been applied by major social platforms during the past years and raised a lot of controversy.

Given that Liberdyne does not just offer a slight protocol improvement but is a generation ahead of all major centralized instant messaging software platforms, and at the same time keeps most current functionality and parameters available, users may have strong incentives to try it.

### 2) Liberdyne – messenger that pays you to use it

By default, the application will be configured to perform a number of functions to support the system (namely minting, DOG, SATAN relays, and storage nodes), for which each user will automatically receive a small reward, becoming a sort of a "miner." At the same time, the functionality of the mobile versions will be configured so that the user will not feel that there is a significant waste of resources (i.e. battery and Internet traffic).

As a result, users will receive a reward in the Dynemix cryptocurrency for the mere act of using the application (as "usage" includes system support, like in all P2P systems). At the same time, the algorithm of reward distribution will be such that the fewer users who are online, the greater the reward each of them will receive. According to our idea, this will encourage users to install the application as quickly as possible in pursuit of a larger reward, which should lead to an explosive growth of the userbase. When the userbase becomes large enough, people will already be interested in using the application for reasons other than receiving a reward.

*Combining these two "killer features," we can conduct a marketing campaign that will hit both the instant messaging market and the cryptocurrency market, reaching the largest potential audience and helping the platform to gain a significant userbase. We expect that this approach has the potential to secure leading positions for the project in both markets.*