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.

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/Dynemix, please refer to the white paper. Any updates to this document can be made without prior notice.

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

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 2014, a fundamentally new blockchain platform – Ethereum – was born. Unlike Bitcoin, it was not strictly a cryptocurrency, and it was primarily meant to become not just a means of payment or storage of value but rather a decentralized virtual machine (also often called a distributed Turing machine, since its state machine used the Turing-complete instruction set) for running various kinds of applications, including so-called “smart contracts” that enabled value transfers and the automatic enforcement of other various types of obligations under multiple conditions.

As Ethereum offered many new ways of using blockchain technology, while at the same time retaining all the main capabilities of Bitcoin, it was called a “blockchain 2.0” platform. We believe such a classification to be incorrect, however.

The reason is that we believe Ethereum-like platforms to be a separate branch of DLT, which is connected to decentralized payment systems horizontally, but not vertically. Providing a blockchain platform with Turing complete scripts does not make it a better payment system, but on the opposite, it degrades the properties of a given blockchain system as a payment processor, since it applies complications that do not serve payment functions but rather make the platform a more universal tool.

We believe that to create the ultimate decentralized payment system (an actual cryptocurrency), we need to endow it with a specific set of features and accept a certain set of tradeoffs that are not fully compatible with the decentralized virtual machine concept.

Despite our respect for Bitcoin as the primordial cryptocurrency, we must acknowledge that Bitcoin also did not initially possess the required set of features to seriously compete with the conventional finance framework. As a result, Bitcoin became a speculative asset and an inflation-hedging tool, and it will likely remain as such from now on.

Following the appearance of Ethereum, the concept of Bitcoin-like payment systems was abandoned for good, and since that time we have not witnessed any serious attempts to bring about a next-generation blockchain system concentrated solely on payment functions.

We can state that to date there is still not a single true cryptocurrency (meaning a decentralized global electronic payment system that operates with tokens that function as a universal medium of exchange for various goods and services) available on the market.

Dynemix is designed to fill that empty niche and present a next-generation blockchain payment system capable of competing with conventional centralized payment infrastructure or even substituting it entirely.

II. The Ultimate Cryptocurrency

According to our vision, a cryptocurrency with the potential to become a global universal medium of exchange should possess the following features:

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. We do not support this approach since we believe a centralized blockchain to be essentially pointless. Instead, we should try 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 development that will be capable of overcoming the speculative stage and transitioning into a real economy. The currency should be optimized to power real market trade instead of serving as an investment or hedging asset.

4) Overcoming the 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.

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 Liberdyne 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 most 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 a 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 new economic model.**

The system features a unique coin issue and reward distribution 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. This design should help the system surpass the speculative stage and build the real economy by adjusting the supply algorithmically according to the demand and keeping the value of coins stable, thus becoming the first true cryptocurrency.

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

Dynemix is designed to use 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.

Liberdyne also serves as an integrated market platform for distributing various goods and services using dynes.

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

Unlike with the typical approach, we did not aim to use technology for the sake of technology. Blockchain is used only to the extent that it helps build a better system and improve the user experience.

a) Liberdyne uses the Dynemix namespace as a secure, decentralized, and consistent key storage that is highly resistant to MITM attacks.

b) Dynemix provides rewards for users who share their resources to support Liberdyne's features.

c) The Dynemix wallet is integrated into Liberdyne to provide a user-friendly experience with a cryptocurrency.

d) 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.

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 prejudiced filtering rules, users are free to choose another filtering solution, which renders such attempts inefficient.

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 girls, if you prefer), or *DOG*. If the sender cannot connect to the recipient, he or she 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.

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.

5) Modes of operation: anonymous or social

One of the key goals of the project is to provide the possibility of fully anonymous 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. Anonymous users can communicate with socialized users without any threat to their privacy.

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.

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) Algorithmically adjusted supply

Speculations make cryptocurrencies extremely volatile, which renders them inconvenient to use as a medium of exchange. The issue of volatility was addressed by a number of projects, from simple collateralized stablecoins (such as Tether) to sophisticated algorithmic solutions (such as Basis).

None of the currently available projects, however, managed to create a fully decentralized economic model capable of taming volatility. Even algorithmic schemes still require external oracles to get the information on prices and/or governance to manage the reserves and the vector of the monetary policy.

In Dynemix, we introduce a groundbreaking model of the supply control that is fully decentralized and independent. Dynes are not pegged to any particular asset and the supply is controlled intrinsically without the need to engage either external sources or governance. No special assets are created within the system for that purpose, which helps the platform avoid any troubles with financial regulators (which was the reason why the Basis project was shut down eventually).

2) Wide 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 exchanges, will more likely use them directly to purchase actual goods or services.

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 Liberdyne's active users, thus making the Dynemix monetary policy an embodiment of the concepts of *helicopter money* and *basic income*.

3) Overcoming the speculative phase

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. As the speculative pressure raises the market cap of the platform, the rewards become even larger in a fiat equivalent, thus attracting more reward hunters.

With the help of this solution, we expect the speculative factor to be mitigated 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 those.

1) Liberdyne – the 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 decribed above) can also put an end to biased censorship, which has been applied by major social platforms during the past years.

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 download and try it.

2) Liberdyne – the 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 "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). If desired, through the settings, the user can both either increase the amount of resources spent (thereby increasing the reward) or reduce or even disable the feature entirely.

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.