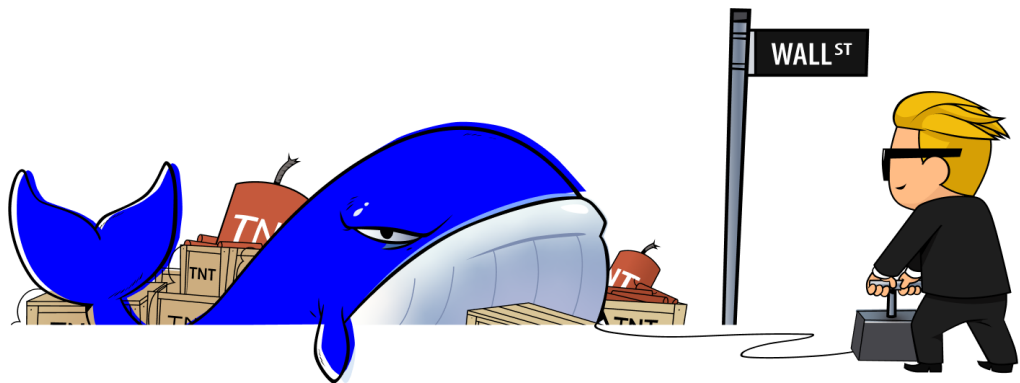




# BigShortBets White Paper

BigShortBets

January 2022. Version 1.0.1



## Contents

1	Intro	3
2	Existing Problems	3
2.1	Access to information	3
2.2	Disproportions between market participants	3
2.3	Control of governments and regulators	3
2.4	No price limit orders on DEX	4
2.5	Anonymous peer-to-peer trading in instruments (brokerage, control and asset management)	4
2.6	Creating and trading P2P instruments with the use of cryptocurrencies.	4
3	BigShortBets Platform	5
3.1	Social Information Platform	5
3.1.1	Description	5
3.1.2	Features	5
3.1.3	Information Market	6
3.1.4	Paid Baits	6
3.1.5	Reputation system and ranking	7
3.1.6	Security, Encryption and Anonymization	7
3.2	Decentralized Futures Platform - DAO Market	11
3.2.1	Decentralized Futures Contracts	12
3.2.2	How it works?	12
3.2.3	Peer-To-Peer Bets	13
3.2.4	Arbitrage	13
3.2.5	Wallet	13
3.2.6	Transactions	14
4	BigShortBets Mobile App	16
4.1	Security and Connection Anonymization	16
4.2	Access Authorization via Wallet App	16
5	BigShortBets DAO	18
5.1	BIGSB SideChain and Nodes	18
6	BIGSB Token	19
6.1	Utilities:	19
6.2	Tokenomics	19
6.2.1	Supply	19
6.2.2	De ation and staking	20
6.2.3	BuyBack and Redistribution	20
6.3	Investment Rounds	20
6.4	Revenue Model	21
7	BigShortBets Team	21
8	Risks	21
8.1	Regulatory Risks	21
8.2	Security Risks	22

## 1 Intro

The stock exchange is an emanation of the highest form of market freedom, related to the natural and inalienable right of every human being to possess.

For this reason, the idea of building a decentralized and encrypted tool was born in our heads, in which the privacy of users will be protected in the name of our natural values that we all have and consider to be the highest good. It is freedom - the basic and most valuable good that allows us (responsible market participants) to decide about property freely, freely and regardless of our internal or external factors - motivation. This was the understanding of the market at the beginning of the 17th century, when the first modern stock exchange established in 1611 by Dutch merchants in Amsterdam made its debut. Joseph de la Vega - a speculator, investor, merchant, and the author of the oldest book on speculation published in 1688, entitled *Confusion de Confusiones* 1688, writes in his work:

Of all the plays performed on the various stages of the great theater that is the world, the greatest comedy takes place on the stock exchange. It is here that speculators in a unique way compete in all sorts of tricks, do business and find various excuses, among which you can find clever ploys, concealing facts, quarrels, provocations, mockery, vain conversations, violent desires, collusion, clever deceptions, betrayals, deceptions and often a tragic end."

## 2 Existing Problems

### 2.1 Access to information

Currently, access to first-hand information is very limited. Every piece of information reaching a retail investor is truncated in significant parts or arrives at a time that does not provide an appropriate response in the markets. Access to high-quality, first-hand information requires a huge amount of money and time.

### 2.2 Disproportions between market participants

There is huge information and capital gap between retail investors and funds, commonly known as the Wall Street whales. Little investors have no chance or tools to stand against such whales, and any attempt of organization ends in a blockade and repression.

### 2.3 Control of governments and regulators

The current status quo is controlled by huge funds using internal connections to manipulate the market. A fund representing 1,000 people is privileged to more than 1,000 small investors organizing in a public forum. Such a division of rights is a pathology of the market and leads to situations in which funds can bend the rules of the game and are almost unpunished, and attempts are made to draw the consequences from small investors and even cut off the possibility of trading assets.

## 2.4 No price limit orders on DEX

The structure of DEX exchanges does not allow for placing orders with a price limit. This means that the purchase/sale of an asset only takes place at a particular moment, and it is not possible to change the entry/exit price. This severely limits the possibilities of profitable trading/arbitrage, as it does not allow for accurate buying and selling prices and speculation.

## 2.5 Anonymous peer-to-peer trading in instruments (brokerage, control and asset management)

The availability of instruments on traditional markets is limited due to the requirements set by the entities that provide them. One of the main requirements is to pass the identity verification process. Due to the local nature of certain exchanges, this practice limits the availability of instruments to investors who, for various reasons, cannot use banking services in a given country. For example, in order to purchase financial instruments on the WSE/NewConnect markets in Poland, it is required to have an account with a brokerage house within the local banking system. This state of affairs means that the provision of services on the market is limited to a small group of financial institutions, which creates a kind of monopoly in the context of brokerage and asset management, as the control is ultimately exercised by one central body. The only way out of this hermetic circulation is to create a system in which location, currency or local law do not limit the availability of instruments, and thus a system that allows you to operate in an anonymous manner. The world of cryptocurrencies and DeFi gives this opportunity.

## 2.6 Creating and trading P2P instruments with the use of cryptocurrencies.

The availability of instruments that allow to "play" stocks, commodities and indices using crypto is a marginal phenomenon - it almost does not exist. Today's centralized exchanges only allow you to bet on crypto-crypto contracts. DEX exchanges, on the other hand, have limitations related to their design, which eliminates the possibility of dynamic trading with a price limit, and also forces users to create a pool of liquidity and then trade, while increasing the risk of investment. Contrary to the above, BigShortBets is the ability to create any instruments / bets paired with stablecoins (crypto) and trade them directly with other users on a Peer-2-Peer basis.

### 3 BigShortBets Platform

The solution to the presented problems is a multifunctional platform built on the Tor network with a use of blockchain technology. The combination of these two solutions guarantees that the users of the platform are anonymous and its functioning is independent of centralized entities. The BigShortBets platform consists of a set of two segments:

- ^ Anonymous Social Information Platform
- ^ Decentralized Futures Market - DAO Market

#### 3.1 Social Information Platform

Performing a market operation requires a certain stimulus - acquiring knowledge, finding a promising trend, or examining market sentiment. It is possible to do this effectively in conditions where censorship does not affect the formation of artificial information bubbles. Various events involving common social media platforms prove that entities are able to effectively limit the reach or even block the content creator. On issues as sensitive as finance, power, politics, and documentation - censorship is particularly evident. For this reason, an anonymous platform is created that will be a place of expression for everyone, where each member is accountable to the rest of the community.

##### 3.1.1 Description

Information exchange requires a secure infrastructure and uncensored interaction between users. One of the pillars of the project is anonymity, and the platform guarantees its preservation by logging in using the MetaMask wallet. According to the "zero-knowledge" policy, the only information constituting the identity of the account on the platform is the wallet address. No personal data is required and stored. To ensure the best experience of using BigShortBets, the information platform segment has known mechanisms of interaction between users used in the popular social - media.

##### 3.1.2 Features

1. Timeline - it presents the latest information published by users using "Baits". "Bait" is a single post and information carrier. It can contain both a description in text form, as well as audio, video and images as attachments. Timeline information is sorted by an algorithm, but can also be sorted and searched using a custom filter. "Baits" can be filtered in terms of content, hashtags and the user's reputation level.
2. Profile - each user, by registering on the platform, generates his profile, which is a page representing the activities related to the account. Creating a profile does not involve providing any data. This is a completely anonymous solution. The user has the option of fully personalizing his profile by changing the name, editing the description, adding an avatar and a background photo. Users also have the option to create and promote their own hashtags. The above tools are designed to make your profile stand out in an anonymous space.

3. Groups - an inseparable element of a thriving social platform. BigShortBets allows you to create groups and their full personalization - own hashtags, hermetic or open groups, emojis, ranks, etc. All this to create the best environment for connecting and sharing information. Groups will be encrypted and anonymized in line with our security policy.
4. Messages - a big part of a well-functioning community is the possibility of mutual private communication. The term "privacy" is crucial here. The idea we support requires tools that allow for safe communication of users and exchange of files/data. As part of the BigShortBets platform, we will offer an anonymous messenger that utilizes keys stored in the MetaMask wallet. Chat will allow for the encrypted exchange of all content (text, audio, video, documents, etc.).
5. Content - as a multi-level platform that solves the problem of anonymity, BigShortBets introduces a whole list of functionalities that will not only guarantee security, but also give you a complete user experience. The first level is the encryption of Bait (posts), the next one is the ability to anonymously upload and publish audio files (.wmv), pictures (.jpeg) or documents (pdf.; doc.). At a later stage, the function of transferring video files as well as live-streaming will be enabled. Everything anonymously.

### 3.1.3 Information Market

Nowadays, information can be worth more than capital or work. Good news can bring significant economic benefits and be the subject of a transaction between two parties. The idea behind the BigShortBets platform is not only to integrate the society, conduct uncensored discussions, but also to trade information within this community in a secure and anonymous manner.

### 3.1.4 Paid Bait

Bait are the carrier of information appearing on the timeline - they contain content and optional attachments. Bait can take the form of free community-exchanged posts or paid posts. The latter are to allow creators to earn money on their knowledge, research and analysis. The creation of paid content will be possible, inter alia, in the following forms:

- ^ subscription (e.g. 5 BIGSB / month),
- ^ one-off payment from one user (e.g. 1 x 100 BIGSB),
- ^ one-off payment from multiple users (e.g. 100 x 1 BIGSB).

Users will be able to access this content in a way that suits them best. A special smart contract acting as a transaction broker will be responsible for securing the transaction.

An important function from the point of view of users creating and sharing content is the possibility of supporting them on the basis of patronage. Users will be able to donate any amount to their favorite creators in exchange for unique benefits. Such a model will enable all creators focused on the subscription model, to transfer the entire process of collecting and settling funds paid by fans

into one ergonomic and decentralized place. As a result, the creator-recipient relationship remains unwavering, and only they are involved in the transaction. The lack of an intermediary (e.g. PayPal, payment gateways) minimizes the risk of blocking funds, or simply limits the costs of commissions and handling fees that are necessary to incur.

### 3.1.5 Reputation system and ranking

A platform that aims to anonymize and protect users by implementing a "zero-knowledge" protocol places certain demands on the community. You need a system that reflects the credibility of users. The solution adopted on the BigShortBets platform is a system of gaining a reputation, which transparently shows the level of trust in the user and is a reflection of his behavior on the platform.

Reputation affects the ranking of Bait, as well as the "power" of comments and likes, making it a measure of voting power. It also impacts the positioning of the Bait on the timeline. Trust in the user helps to motivate ranks, which are 6. Each rank is the sum of the profile activity ratings made by other users. Determines whether the profile is reliable or not. The ranks are positioned as follows:

- ^ Troll - <-1 to -0.6
- ^ Fishy - <-0.6 to -0.3
- ^ Unranked - <-0.3 to 0.3
- ^ Active - <0.3 to 0.7
- ^ Trusted - <0.7 to 0.9
- ^ Honorable - <0.9 to 1

The underlying system on which reputation is built is binomial distribution. Using the Wilson Score model, the system calculates the exact reputation value. Our formula allows you to determine your reputation value by taking a lower band. Reputation is at the bottom of the Wilson Score. If the reputation value is 50 percent, then the user has 96 percent more efficiency than 50 percent. Efficiency in this case means the probability that the user's reputation is above the lower band determined by the formula. The lower band is where the reputation value has the highest similarity, and therefore this number is displayed as the user's reputation value, rather than anything else.

### 3.1.6 Security, Encryption and Anonymization

#### Security

Each market participant expects security and guarantees that the transaction is genuine. Due to the nature of DeFi solutions, a trusted third party is a smart contract. The security issue is similar in the case of any transaction made on the BigShortBets platform. Creating any commercial offer and leading to transactions between platform participants, in effect, will mean interactions with a smart contract that will secure the transfer of information and funds in this specific event.

## Content Encryption

### Private Keys

"Application keys" refer to a pair of Curve25519[?] ] keys assigned to a BigShortBets user on the first login. Their purpose is to provide encryption capabilities without exposing wallet keys.

Application private key is not persisted in BigShortBets database. They belong to the user and remain his secret key, enabling encrypted peer-to-peer communication between users, with BigShortBets platform acting as a middle-man unaware of the content.

### Application private key storage

### Mobile Client

Mobile devices with Android platform allows the user to store application keys in local KeyStore.

### Web Client

Since web client is available only via Tor Browser, there is no secure storage that could be used to persist application keys. A workaround for this issue, is to re-generate users' application keys when they are needed to perform an operation. For convenience, application keys are stored in browser memory (non-persistent) for the duration of the session.

The challenge was to regenerate application keys without storing or providing the seed by the user. The solution is described below:

1. A random seed number of 256bits is generated using browsers Crypto API
2. The user is asked to sign the seed (converted into the hex format) using his Metamask wallet.
3. The first 32 bytes of this signature are used as de facto seed for curve25519 keypair generation. The library used is curve25519-js[ ]
4. Web application sends the following information to the BigShortBets service:

- ^ unsigned\_app\_private\_key\_seed    It is the random seed number from step one, converted into string hex format
- ^ app\_public\_key\_signature    public component of application keys signed with Metamask wallet to confirm the owner of the wallet approves generated keys
- ^ nonce\_signature    one-time password signed with Metamask wallet



```
{  
  "nonce_signature": "0xb109051afab6de0318f73cb79dea6ef81caa189864ba07bbd1616f6864f1172353a  
  "unsigned_app_private_key_seed": "0xe4234c93f3bda43e674d094e1dac79d378bd67764b0ff8f3f9fd7ba  
  "app_public_key": "0x33e6125c33bb7d66161a877a98b4543d83bc34c97204b431244ed39a89900676",  
  "app_public_key_signature": "0x15ed44a6f0139082e668d33f4c51ada1ffb0f531102a40909a640a044487  
}
```

The user account and his application keys are initiated and stored in memory (non-persistent) until the user has closed the browser. Since they are not stored in the browser between sessions, nor in the systems' database, they need to be recovered on the next user session. The recovery is based on the seed from step 1 and goes as follows:

1. User signs in with his Metamask signature of one-time password (nonce)
2. User receives his random seed number stored in BigShortBets database. The seed is not available to anyone other than the used it belongs to.
3. When the user activates a feature utilizing encryption, then is asked to sign the random seed number with Metamask wallet.
4. Signed seed is used to generate application keys the same way it was done in step 3 of account initialization.

#### Chat messages end-to-end encryption

Chat messages are end-to-end encrypted with AES-based algorithm "secret-box" from libsodium library. Web implementation uses "tweet-nacl" port. Every message has its own unique symmetric key, as well as nonce. Symmetric key is encrypted as a part of the message using Diffie-Hellman shared key encryption, together with another nonce. That provides both hardness from decipher attempts and ability to perform fast AES encryption on large messages. That approach guarantees identity of the interlocutor and prevents from accessing content of the whole conversation, even if symmetric key is compromised for a single message .

## Messages Encryption

Figure 1: Message encryption diagram

1. Generate a random symmetric key for AES256/secretbox of 32 bytes
2. Generate a random nonce of 24 bytes
3. Generate the shared key using Diffie-Hellman key exchange. Current user provides his private key and his interlocutors public key. Shared key length is 32 bytes
4. Symmetric key from step 1 is wrapped in a `box[]`
5. Message header is constructed by concatenating nonce and boxed symmetric key, then converting to Base64. Message header has 96 bytes.
6. Generate another random nonce of 24 bytes
7. Encrypt message content using the new nonce from step 6 and the symmetric key from step 1. Message is wrapped into a secret `box[]`. The length of the message is a function of the content length and can be expressed with a formula:
8. Wrapped message is converted into Base64 and concatenated with message header from step 5.

### Decrypting a message

1. Decode first 96 bytes of Base64 message to unsigned bytes(8-bit unsigned integer values). This is the Message Header. The first 24 bytes are box nonce, the rest is encrypted key.
2. Generate the shared key using Diffie-Hellman key exchange. Current user provides his private key and his interlocutors public key.
3. Open the box! Using shared key and box nonce to obtain the Key.
4. Decode the rest of the message from Base64 to unsigned bytes(8-bit unsigned integer values). The first 24 bytes are secretbox nonce, the rest is encrypted content.
5. Open the secretbox! Using the Key and secretbox nonce.
6. Text content can be read by encoding the resulting bytes to UTF8.

+ Encoding and decoding between bytes, Base64 String and UTF8 is performed by [? ]

### 3.2 Decentralized Futures Platform - DAO Market

The world of smart contracts has brought us completely new possibilities of thinking about money. Central institutions - banks and stock exchanges - seem to be no longer needed, even for very complex operations such as asset swaps or loans. A purely decentralized contract mechanism would allow people to gain exposure to the assets they wish to speculate in a completely uncensored and uncontrolled manner. We propose a simple model that we believe will provide all of the above features.

### 3.2.1 Decentralized Futures Contracts

Decentralized futures contracts are contracts that have a mechanism to follow the price of a given pair of assets (e.g. quarterly or perpetual settlement). In the case of BigShortBets, it refers to assets equivalent to assets on a conventional exchange, but decentralized and digital. In this case, the popular NDX / USD (Nasdaq) pair will be listed e.g. as NDX / USDC, in stable tokens. The BigShortBets futures system also has a trading engine that monitors the contracts in terms of time, quantity and owner. There is no Hedging Fund that is managed by any company or owned by developers. Liquidation of loss positions is especially tight, designed to prevent any manipulation. The whole system is mathematically hermetic, it should be remembered that it is primarily a closed circuit, so the amount of security is always equal to the sum of collateral posted by market users and the total sum of contracts is always zero.

### 3.2.2 How it works?

Our model will reflect the 17th century Amsterdam stock exchange, but with the use of an internal blockchain network. You will need 2 sides with mutual bets for each transaction. In order to buy, someone has to sell, and vice versa. There must be two sides in the deal that contain opposing bets to form a pair of "Bets". The block will have pairs of "Bets" with account ID and bet information. Nodes play an important role in placing bets. The Node will be responsible for verifying whether it is possible to execute the called transaction and whether it is real (the way the nodes work is described below in the "BigShortBets DAO" chapter). A special library will aggregate information for validation in the network. All this will be done using smart contracts without the participation of external people. The only input for users will be to create an asset pair. This will make it impossible to manipulate and interfere with accounting, excluding the human factor from the game system. The only way to have an impact on the environment will be to participate in the game by trading contracts on the platform. The platform only provides certain rules of the game, does not produce any contracts, and does not "print" money. The rules will clearly define how value flows between the platform participants and the conditions under which it can be forced to flow (liquidation). These rules will be transparent and written in smart contracts supporting the platform.

Figure 2: Market structure

### 3.2.3 Peer-To-Peer Bets

Settlement of decentralized futures contracts will be performed using specially designed oracles. They will be responsible for sending information about the prices of the given assets to the platform, and the positions will be settled on the basis of these prices (e.g. quarterly, weekly, etc.). The above technology can also be used to create any plants. It is possible to place bets on weather forecasts, sports bets or even in uencer bets (e.g. number of views over a certain period of time) - sky is the limit . The only requirement will be to create an appropriate oracle that will download the necessary data from the appropriate platform (API) and on their basis will settle the bet between users. The above solution gives unlimited possibilities and defines the next steps in the development of the platform.

### 3.2.4 Arbitrage

The BigShortBets platform will support arbitrage on typical terms of trading in instruments between the traditional markets and the DAO Market. In its development, the platform includes support for arbitrators, also in terms of API for placing orders. Instruments synthetically created by users on the BigShortBets platform will have the same specificity as traditional instruments and will allow arbitrage to be made by every market participant. Equal access to arbitration tools will make them (arbitrators) compete with each other by the difference in margin, which in the end results in smaller and smaller price differences compared to traditional markets (smaller spread). Trading on the DAO market, which we propose, is not based on a mathematical formula taking into account the size of the pool and the number of tokens (such a system is offered by all popular DEX exchanges, e.g. Uniswap, Pancakeswap), but on real P2P trading with locked liquidity. The total liquidity of the platform is the total value of all the Bets at any given moment locked through the duration of the trade - until the position is closed. This solution enables the execution of orders with a price limit.

NOTE : The platform does not create bets or print money. It only provides tools that users are able to use. Peer-to-peer trading is characterized by the lack of a viable intermediary (third party). As a result, it marginalizes the role of the platform to enable transactions created by users.

### 3.2.5 Wallet

The internal wallet acts as a transaction security deposit, and a specific token is sent to the platform within the ERC-20 network. Trading of the deposited tokens will take place using a specially built SideChain. The wallet is individual and corresponds to the wallet address used during registration - it is its internal clone, synchronized with the wallet on the Ethereum network. Such a scheme of operation prevents external access, because only the wallet with a given Ethereum address has access to the corresponding wallet on the BigShortBets side network. The process of logging in and activating the BigShortBets Wallet is integrated with the process of logging in to the Web 3.0 platform. The use of such a solution guarantees the user's safety and prevents unwanted interference by third parties.

### 3.2.6 Transactions

Transactions on the platform will take place within the internal side Ethereum network (SideChain). These transactions will not be charged with ERC-20 gas fees. However, there will be small commissions on the SideChain network, and their amount will depend on the number of BIGSB tokens a user has. The commission tokens on the internal network will be redistributed to all BIGSB token hodlers. Appropriate amounts of BIGSB tokens will also be used to reduce the commission for transactions on the BigShortBets Market platform. Both models are designed to reward users with tokens and encourage them to buy and hodl.

Figure 3: Market transaction

The amount of the commission can be represented by the formula:

$$P = y(x)$$

Where:

P - transaction commission

x - base commission of 1 BIGSB

y - multiplier in the range 0.1 - 1

The amount of the multiplier is motivated by the levels of the number of BIGSB tokens held, presented in the table:

Table 1: Commission multiplier

[Example] - user A makes transactions on the BigShortBets platform, and his wallet has 80 BigSB. He will pay a commission of 1 BIGSB for the transaction. User B - who is the other party to this transaction, will also pay a commission, but due to the fact that he has over 10,000 BigSB in his wallet, the commission will be 0.5 BIGSB.

NOTE : If there is not enough BigSB to cover the commission, the system will settle the fee in stable token (e.g. USDC). To reward and promote BigSB token holders, the commission settled in stable tokens will be twice as high as that settled in the native BigShortBets coin, and the income generated from these commissions will be used to operate the token BuyBack program (Read - "Buyback and redistribution").

## 4 BigShortBets Mobile App

The functionality and capabilities of an anonymous information platform as well as a decentralized futures market are the cornerstones of the BigShortBets environment. In today's era, however, accessibility to the tool is no less important, and from there it is a short way to mobile solutions. The BigShortBets mobile app will have all the functionality known from the web browser version.

### 4.1 Security and Connection Anonymization

The mobile app maintains the same high standard of security and anonymity as the web application. The design of the mobile system (Android) allows for safe connection to the TORnet network. For this purpose, the BigShortBets mobile app connects to the network via the Orbot app. This service allows other programs installed on the device to connect to the TOR network. The use of Orbot is necessary for the BigShortBets mobile application to meet all the adopted security criteria. This solution makes the connection to the network highly encrypted and protects user's anonymity.

### 4.2 Access Authorization via Wallet App

Authorizing access to the mobile application is similar to the web application, but in the case of the mobile version, the application keys generated when logging in for the first time remains on the user's device (the user can delete the key at any time and generate a new one - as the owner of the key, he is responsible for it). In the case of the web version, the application requires authorization with MetaMask each time. Android devices use a separate wallet app rather than a browser extension. In order to authorize access to an account on the BigShortBets platform, it will be necessary to have a wallet application (e.g. MetaMask) with a logged in account. Launching the BigShortBets mobile app and attempting to log into the account will launch the wallet application, in which the user will be asked to sign a contract to confirm the account's identity. The private keys used to authorize access are only stored on the user's device.



Figure 4: First BigShortBets Mobile App Login

Figure 5: Every Next BigShortBets Mobile App Login

## 5 BigShortBets DAO

A certain development of the DeFi ideas and technologies is the more and more often used DAO (Decentralized Autonomous Organization) model. The BigShortBets platform fully draws on the assumptions of DAO and will ultimately function without a centralized management, but with a decentralized community. The reputation system based on voting, the implementation of solutions proposed by users is one of the DAO mechanisms on which the platform will utilize. Such a solution is simply to "give power to the people" and this power will in uence BigShortBets events based on the size of the community participation due to the rank held and the number of BIGSB tokens.

### 5.1 BIGSB SideChain and Nodes

One way to implement decentralization in practice is to disperse the SideChain network supporting the BigShortBets, which will be used for transaction processing and information transfer. We decided to implement the proprietary SideChain network due to the necessary criteria that the network must meet. The own SideChain brings with it the independence and integrity of the entire platform, which is extremely important in the case of a project focused on anonymity and privacy. The integration of transactions with an internal SideChain also allows you to minimize commission fees, which can be high on the ERC20 network. This solution is economically advantageous, not only because of avoiding high fees, but because of its design, which rewards active users.

Figure 6: BIGSBnet structure

To maintain the security of users and fairness of transactions, BigShortBets SideChain will initially operate on the "proof of authority" principle. Then it will be transformed into "proof of stake" on clear, predetermined rules. After introducing the "proof of stake" consensus algorithm, platform users will be able to act as a Node in the internal SideChain network. The selection of Nodes will be based on criteria relating to the trust of the platform participants and the number of BIGSB tokens being stacked. This means that other - socially trusted - market participants and platform users will be responsible for the validation of transactions between market participants on the BigShortBets DAO platform.

## 6 BIGSB Token

A decentralized platform that has its own ecosystem needs a reliable carrier of information and transactional data. The use of existing tokens would be dependent on other ecosystems and would bring another risk and cost factor. To avoid these problems, we decided to implement our own token - BIGSB, which is an ERC-20 token and is widely used on the platform. The token was created to give maximum benefit to stacking hodlers.

### 6.1 Utilities:

- ^ Measure of reputation - the number of the BIGSB tokens will have an impact on the vote weight
- ^ Transaction token - each transaction on Social Platform (buy/ sell/ subscriptions) will be made using the BIGSB token.
- ^ Base commission - BIGSB token will be used to settle commissions and bets other than the existing ones, e.g. NASDAQ, S & P500, Crude Oil.

The token is also deflationary in nature and has a clear stacking rewards system. A 1.5 percent fee is deducted from each transaction made, 0.5 percent of which is automatically burned. The remaining 1 percent of the commission is distributed as a reward to all hodlers using a technology similar to RFI. This means that for every transaction made with BIGSB on the blockchain network, the user is automatically rewarded for the BIGSB hodling.

No lock. No limited prize pool. Pure staking.

### 6.2 Tokenomics

#### 6.2.1 Supply

- ^ Total supply: 100,000,000 BIGSB
- ^ Sales: 80,000,000 BIGSB
- ^ Liquidity: 10,000,000 BIGSB
- ^ Project reserve: 10,000,000 BIGSB



### 6.2.2 Deflation and staking

A 1.5 percent commission is deducted from each transaction with BIGSB on the Ethereum network:

- 0.5 percent is automatically burned, which in turn reduces the number of BIGSB tokens in circulation
- 1 percent is divided proportionally among all BIGSB hodlers

In addition, 100 percent of commission on transactions made within the SideChain network (chapter - Transactions) is proportionally distributed to hodlers depending on the number of tokens held.

### 6.2.3 BuyBack and Redistribution

The commission on the platform will be paid in stablecoins or BIGSB tokens. In both cases, this commission will be stored on a dedicated wallet address for further distribution as a DAO incentive for users contributing to the platform. Stablecoins charged as a commission will be used to buy tokens from the market (BuyBack), and then, together with BIGSB tokens collected as a commission, will be redistributed to platform users in an amount proportional to the amount of BIGSB held in the wallet.

## 6.3 Investment Rounds

PHASE I - 10,000,000 BIGSB:

1. Local Pre-Sale \$0.65 - 4,000,000
2. International Pre-Sale \$0.95 - 2,500,000
3. Public Sale \$1 - 1,500,000

PHASE II-VIII - 70,000,000 BIGSB:

1. PHASE II min. \$2 - 6-month lock 10,000,000 BIGSB
2. PHASE III min. \$2.1 - 7 months lock 10,000,000 BIGSB
3. PHASE IV min. \$2.2 - 8 months lock 10,000,000 BIGSB
4. PHASE V min. \$2.3 - 9 months lock 10,000,000 BIGSB
5. PHASE VI min. \$2.4 - 10 months lock 10,000,000 BIGSB
6. PHASE VII min. \$2.6 - 11-month lock 10,000,000 BIGSB
7. PHASE VIII min. \$3 - 12-month lock 10,000,000 BIGSB



## 6.4 Revenue Model

The creators and founders of the platform do not receive payments and rewards in the form of redistributed BIGSB tokens. For the use of the core team, 10% of the entire supply of tokens (i.e. 10/100 million BIGSB on the listing date) is blocked under the smart contract. The team is not able to pay out these funds due to the construction of the contract, and the income to keep it working is generated from staking rewards. If the assumptions of the tokenomy show that 1% of the rewards generated from commission is distributed among users, it means that 0.1% goes to the project reserve. Importantly, the smart contract holding tokens is constructed in such a way that the content of the wallet is always blocked by 10% of the entire supply, also after many burning processes. The platform, basing its form and the idea of operation on the DAO system, will redistribute all revenues from fees to the hodlers that contribute directly or indirectly to the ecosystem.

## 7 BigShortBets Team

Team BigShortBets is a mix of different characters, views on the world and life, which have one thing in common - a common fight for the possibility of free expression of their thoughts, words and actions. BigShortBets is made up of a group of several dozen programmers and specialists, which is constantly growing (If you want to join our team and think that you have competences that may be useful to us - write to [coreteam@bigshortbets.com](mailto:coreteam@bigshortbets.com)). Each team member is also an investor in a private dimension. No person working on BigShortBets receives BigSB tokens as part of remuneration, and if he has them, it is due to a personal purchase decision. BigShortBets partly comes from the trading community, because the CEO of the project - Rafał Zaorski - is also the initiator of the Trading Jam Session foundation.

## 8 Risks

Due to the nature of the platform, we are trying to create an independent and safe tool, but the indirect compulsion to use specific technological solutions, as well as the uncertain legal status of the world of cryptocurrencies, carry risks.

### 8.1 Regulatory Risks

Cryptocurrency regulation is an ongoing process. High dynamics of regulation and the frequent lack of understanding of the idea of cryptocurrencies on the part of regulators shake the cryptocurrency market. Despite the technological potential and the growing society supporting this idea, the future is unknown in the context of legislation and certain events limiting the tool utility. Another topic is the risks relates to the transaction brokers regulations. Tool has proprietary solutions, but due to technological standards, use of currency wallets (e.g. MetaMask, TrustWallet) is obligatory. Currently, these solutions are decentralized, but they also face the issue of potential regulations on cryptocurrencies and De-Fi services in the future, so their policy in a few years may be different from what is known today and, for example, may be forced to verify identity.

