Bisq DAO Overview

Introduction

Bisq enables users to exchange bitcoin for other assets in a fully decentralized manner. We have designed a Decentralized Autonomous Organization (DAO) [1] to achieve a decentralized management and funding model for Bisq.

We introduce a token (BSQ) into the Bisq ecosystem to enable a value exchange between those who use the platform for trading and those who enable the project by their work.

The token is represented on the Bitcoin blockchain as a custom form of *colored coin* [2]. Around this token, the architecture of a new governance model is built, which is evolved through each user's voluntary participation in the network.

In a nutshell

Bisq

Bisq is open source software that allows users to exchange Bitcoin for fiat currencies as well as alternative cryptocurrencies in a decentralized and privacy-protecting way. It is a desktop application utilizing a custom P2P network for connecting users on the network.

A dedicated trade protocol secures the transaction between the peers. The security is based on a combination of 3 key aspects:

- 2-of-3 multisignature (2 traders and arbitrator are the key holders)

- Security deposit

- Arbitration system

The funds are either in sole control of the user (on their local wallet) or locked up in the multisig

address. Bisq never has access to or control over users' funds. A user does not need to register, and there is no central entity or server collecting user data.

Bisq DAO and the BSQ token

Bisq is organized and administered by the Bisq Decentralized Autonomous Organisation (DAO).

BSQ tokens provide 3 main functions:

- Payment to contributors
- Used as voting "chips" for governance
- Discounted trade fee can be paid in BSQ

Contributors file requests for compensation, and in a monthly voting phase, stakeholders decide if the request gets accepted. If it gets accepted, a contributor has the right to issue new BSQ. Voting is also used to change parameters of the DAO itself.

The users of the platform can choose to use BSQ or BTC for paying the trading fee. If they use BSQ, users get a considerable discount (initially about 90%). The BSQ from the fee payment will be invalidated (taken out of circulation) and can be seen as a distribution to all stakeholders.

All those aspects are achieved in a fully decentralized way by the network of Bisq applications utilizing the Bisq DAO protocol, the Bitcoin blockchain and the Bisq P2P network.

The project is designed as a community project. Bisq was developed without any external funding but with personal savings, donations and altruistic contributions.

Motivation

Being true to Bitcoin's permissionless global nature, Bisq aims to be borderless and fully decentralized. One of the core values of Bisq is the protection of the user's privacy. In order to protect contributors and users from arbitrary interventions and violations of basic human rights for privacy [3], security of the network must be attained through a method of decentralization. Organic growth of a network requires a **solid and sustainable funding model** which is aligned with its core values.

Two more core functions of the Bisq DAO are **project management** and **governance**. We follow a meritocratic approach, so those who contribute the most will get the most influence. The Bisq DAO provides the security to **open and decentralize the arbitration system**, as well as all other aspects

of the project that are currently not fully decentralized.

Governance

The core principle of Bisq DAO is meritocracy. This is based on a belief that the project is best managed and governed by those who contribute the most. This meritocracy is facilitated in an environment that is open and transparent, where users can freely participate.

Voting based on ownership of BSQ as well as on proof of contribution is used for making decisions about changes of the DAO as well as authorizing issuance of new BSQ to contributors for their work in the project.

Management through voting

Stake-based voting

The project is managed initially by the stakeholders through voting. It is important to see these activities as a management tool. We are following a meritocratic approach. Those who have the biggest stake in the project and those who have contributed most should have the most influence. They are usually the ones who are best informed and incentivized to make the best decisions.

As voting by stake will have limitations and risks (ex. whale buys a lot of tokens and makes bad decisions), the project is intended to shift the main influence for voting from stake to reputation in a later phase.

Reputation-based voting

Reputation is derived from all the payments a contributor has received. The more a contributor has earned, the more value they have added to the project and the more experience and knowledge they have gained. Thus, they should have more influence in the decision-making process.

Reputation will not be implemented initially, but is planned for a later phase. The data is available and verifiable from the very first payment to a contributor (the BSQ issuance for contribution is a Bitcoin transaction in the blockchain). So, there will inherently be reputation from the beginning, though Bisq will not make this explicitly visible and will initially not make use of it.

The balance between the weight of reputation and stake for the voting process is intended to be about 70% reputation and 30% stake, but will be decided by DAO voting by the stakeholders.

Voting by reputation will require a certain amount of stake (to be defined), as well as the quorum for a voting item will stay determined by the BSQ stake. Reputation will also have an aging factor to

prevent contributors who become inactive from wielding too much influence.

Incentives

BSQ incentivizes users to become contributors who are committed to the development of Bisq by rewarding their work.

It is likely that contributors will also be stakeholders. Therefore, their economic incentives are aligned with the success of the project represented in the token value.

Contributors tend to be long-term-oriented if they have the intention to keep working on the project. This provides additional security as compared to pure BSQ stakeholders, who might act with short-term interests against the project's interest (e.g. shorting BSQ).

Economic cycle

Traders who are using BSQ for the fee payment get a considerable discount in return for their support in creating market demand for the tokens. Market value is required in order to enable payment of the contributors who do the work enabling usage of the Bisq platform. A closed economic cycle of value exchange arises from users on the platform to creators of the platform.

The BSQ token

At the core of the Bisq DAO lies the BSQ token.

1 BSQ equals 100 colored satoshis (0.00000100 bitcoin). We apply a context and add special rules (ancestry in the genesis or issuance transaction, etc.), giving BSQ tokens custom properties and a different value than the underlying BTC value. So, we inherit the basic features of Bitcoin and add the rules required for the Bisq DAO. BSQ tokens are tradable over the Bisq exchange like any other altcoin.

Issuance

There are 2 ways of issuing BSQ tokens:

1. Genesis distribution
2. Periodic issuance

Genesis distribution

In the first phase, there will be a genesis issuance of 2,500,000 BSQ tokens, given to the

contributors who have worked on the project thus far. In this way, we distribute the value of the project to all participants in proportion to their contributions. Each contributor will hold a certain percentage of the project's total value. We will use 2.5 of the 25 BTC we received over the past years in our donation address as input for the genesis transaction. So, the starting base capital will be 2.5 BTC. Right after the trading begins, market forces will determine the value of the project.

Periodic issuance

In the second phase of the Bisq DAO implementation, we will introduce a monthly issuance cycle. Any contributor can make a request for payment in BSQ for their work, and if that request gets accepted in the decentralized voting process, the requester has the right to issue new BSQ tokens. With this model, we have an open and decentralized form of token issuance. The amount of the issuance represents the amount of work added to the project in that time period.

There will be 3 periods in each monthly cycle:

1. Contributors publish compensation requests for a specific amount of BSQ

2. Stakeholders vote

3. New BSQ is issued

In the issuance period (which happens directly and automatically after the vote result is completed), the contributor issues new BSQ if their compensation request was accepted in the voting process.

Similar to miners who are issuing new BTC for their work to secure the BTC network, the contributors are issuing themselves new BSQ tokens as reward for their work on the project.

Functions of the BSQ token

BSQ tokens facilitate the following functions in the DAO model:

1. Payment of trading fees

2. Funding contributions to the Bisq project

3. Voting on payments for contributors and changes in the Bisq DAO

4. Decentralization of the arbitration system

5. Security deposit for enabling further decentralization

1. Trading fees

The BSQ token can be used for paying Bisq market trading fees. The trading fee can optionally be paid in bitcoin, but if the user pays with BSQ they get a considerable discount (initially, 90% cheaper).

The function of the token is similar to the concept of *Appcoins* [4], where a token is used for accessing a service. BSQ can be acquired via the Bisq exchange and traded like any other cryptocurrency.

When using BSQ for fee payment, tokens are invalidated – taken out of circulation (creating deflation). This can be seen as a distribution of BSQ value to all stakeholders.

2. Compensation request

In the first period (27 days) a contributor can publish a compensation request in the amount of BSQ expected for the work done. The contributor must deliver work up-front, without any guarantee of payment. The risks this constraint impose on the contributor encourage that contributor to stay in close communication with the Bisq community, and to build reputation over time. In order to avoid spam, publishing a compensation request requires a fee of 10 BSQ. Contribution requests accepted by the stakeholder vote will lead to the issuance of new BSQ, in the amount defined in the compensation request.

3. Voting

Mechanism of voting is enabled through BSQ tokens, which is the key component for governance. Voting requires a fee payment in BSQ (initially 5 BSQ, can be changed in voting) to protect against spam and deter uninformed or uninterested voters.

In a monthly phase, the stakeholders hold a vote to determine whether the requests filed by contributors get accepted. Voting is also used to change parameters of the DAO itself. The voting period lasts 450 blocks (about 3 days).

Voting is conducted on the BTC blockchain and uses stake and time of voting for weighting. The more BSQ staked and the earlier a stakeholder votes, the higher the vote weight.

The time-based weighting is applied in 3 phases:

1. First 150 blocks (about 1 day): 100% weight
2. Next 150 blocks: 50% weight
3. Last 150 blocks: 15% weight

After the voting period, the result of the votes will be calculated by each node.

4. Decentralization of the arbitration system

The Bisq arbitration system (see the [Arbitration and Mediation System](https://docs.google.com/document/d/1DXEVEfk4x1qN6QgIcb2PjZwU4m7W6ib49wCdktMMjLw/) (https://docs.google.com/document/d/1DXEVEfk4x1qN6QgIcb2PjZwU4m7W6ib49wCdktMMjLw/) document for details) is part of the Bisq's security concept , ensuring that users (i.e., traders) fulfill their obligations. To this end, we use a security deposit in BSQ which gets locked up and in case of abuse may be confiscated (by voting).

The locking of the BSQ is made by sending a BSQ transaction to one's own address containing a special `OP_RETURN` "marker" output. The unlocking of the BSQ is also done by sending the locked BSQ in a transaction to one's own address, this time containing another `OP_RETURN` "marker" output signaling unlock intent. After a two-month maturity period, the funds become spendable as normal BSQ. The long maturity period gives enough time for voting in case of a request for confiscation.

As additional protection against abuse by a supermajority of stakeholders we require that the users have to support the decision for confiscation. The confiscation will be deployed as a hardfork which can only become the dominant network if a majority of users agree to update their software. It is expected that this confiscation mechanism will never happen, but having that possibility provides a strong protection against potential abuse scenarios.

5. Security deposits for further decentralization

We also apply the idea of security deposits to other areas of the system not yet fully decentralized, including the privileges to:

- run the default seed nodes;
- run market price provider nodes; and
- operate the project's official social media accounts.

Those who provide these services can request a compensation as contributor.

Q&A

Who owns Bisq?

Bisq is an open source project that develops through the participation of many users and the work of many contributors. The Bisq DAO is a decentralized organization coordinating the value exchange

between those who work on the exchange platform and those who use it. Those contributors and stakeholders are the owners and managers of Bisq.

How are changes to the DAO being made?

The Bisq DAO is work in progress and is constantly changing in order to better the system.

Therefore, it should be made clear that the current vision of the Bisq DAO laid out in the document above is not "set in stone" and may change over time as improvements are made.

We hold a stance that code is NOT law, but rather an expression of intent, that requires adoption and improvements over time.

There is no contract between the BSQ stakeholders and the Bisq DAO. Through a sufficiently high level of decentralization and a strong network, there will be some natural continuity and stability. Radical changes to the system should become harder over time.

Bisq users have an inherent influence by agreeing to update to or rejecting newer versions and rules.

Are forks a risk?

As the project is open-source, the barrier for a fork (a possibly changed copy) is likely to be much lower compared to traditional commercial projects.

The risk of forking provides a strong incentive not to act contrary to the interests of the users, stakeholders and contributors. Successful forks will not happen easily because they are dependent on network effects. The technical complexity of the project will be another counterweight to avoid the risk of a fork that can happen through purely commercial interests.

Is there protection against majority attacks?

It is possible for the main stakeholders to abuse their power in detriment to the interests of minority stakeholders (a.k.a. a majority attack). For example, a majority could vote to add new rules for confiscating or invalidating the tokens of the minority stakeholders. Such decisions constitute a hard fork, i.e. a change to the system that is not backward compatible.

The established network will not accept transactions on the hard fork. This means that a malicious fork would have the difficult task of starting a network of traders from scratch, in particular since they have to compete against the old network. Second, the token value on the new fork would be

essentially zero, and the attackers would presumably lose a lot of wealth. The attackers need to get their token value back and this would take decades, given a token yield of a few percent.

In short, we see no economic incentive for a majority attack on the Bisq DAO.

More details and technical specification

More detailed description and technical specifications can be found in the Bisq DAO specification.

Conclusion

The Bisq DAO model is decentralized, open and self-managed by the voting process. Anyone can assume the role of a trader, contributor, stakeholder or voter.

Governance will be minimal in the beginning but is expected to evolve over time to more sophisticated models. Voting on all important parameters of the DAO and on the acceptance of contribution requests are just the first steps. The voting process can be used to improve the governance model itself, so the DAO achieves autonomy.

---

1. V. Buterin, "Bootstrapping a decentralized autonomous corporation: Part I," https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/, September 2013.

2. Bitcoin wiki, "Colored coins," https://en.bitcoin.it/wiki/Colored_Coins, November 2015.

3. Wikipedia, "Right to privacy," https://en.wikipedia.org/wiki/Right_to_privacy, May 2017.

4. F. Ehrsam, "Blockchain tokens and the dawn of the decentralized business model," https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f, August 2016.