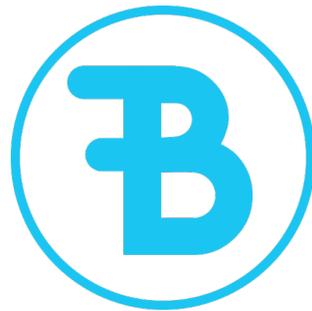# Whitepaper

A trustless Stablecoin based on Binance-chain

BiDao

A whitepaper of the BiDao
CDP and Stablecoin system

Bidao UG
Germany
26. July 2019

Contents

Abstract

The BiDao Cryptocurrency (BID) utilizes a completely decentralized proof-of-stake Blockchain with an additional collateral-backed value token which is 100% stable in value quite in contrast to for example Bitcoin, Binance Coin or Ethereum [1] which experience huge fluctuation. As Settlement Layer the BiDao system utilizes the Binance-chain. This means that you can also freely interact with all crypto assets that are running on Binance-chain. In future, BiDao will be also integrated with other Blockchains like Ethereum, Tezos, and EOS. This way BiDao becomes the one-stop-shop for Decentralized Finance (Defi) applications.

1 Executive Summary

What is BiDao?

BiDao is a new blockchain system [2] that creates a trustless stablecoin and a new decentralized financial tool that allows leveraged trading in a trustless setup. Moreover, BiDao is a one-stop-shop for DeFi applications.

The Problem

At the moment there is no trustless stablecoin that is blockchain-agnostic and allows different crypto assets as collaterals. The only similar system is MakerDAO, but MakerDAO is completely dependent on the Ethereum Blockchain and therefore not able to interact frictionless with other crypto assets. The decentralized finance (Defi) market is growing each day and users are looking for new tools that can be used in the new decentralized financial world.

The Solution

BiDao is building a new blockchain system that is dedicated to DeFi. In the beginning, BiDao will be completely integrated with the Binance Blockchain and BNB will be used as the collateral. In the future also other Blockchains will be integrated into the BiDao ecosystem. Our goal is to create a blockchain-agnostic ecosystem for Defi applications.

Fundraising

To finance the implementation and marketing of the BiDao platform a fundraise will be conducted. During fundraising, the BID Token will be sold. The BID Token is a BEP-2 compliant Token that is running on the Binance Blockchain.

2 Market Analysis

One major problem of most cryptocurrencies is that their prices are highly volatile. To reach mass-adoption a trustless stablecoin will be needed. Many applications will only become possible, once a trustless and blockchain agnostic stablecoin is established. At the moment there are many centralized stablecoins like Tether and others. All these stablecoins share the same weaknesses - you cannot trust them.

Moreover, these stablecoins are often very intransparent and in general, difficult to monitor. Decentralized stablecoins like Maker-DAI are just useable on a single platform and too complicated for casual users. It is needed to create an easy-to-use and trustless stablecoin - exactly this is the goal of BiDao. Moreover Blockchain interoperability becomes more and more important. Blockchains like EOS, Tron, Cosmos and Tezos gain more popularity each month. So it is key to create a DeFi ecosystem that is able to communicate with all these different Blockchains and their assets. Stablecoins and DeFi are already big markets. The market cap of Stablecoins is about 4 billion USD and about 450 million USD are currently locked in DeFi applications.

3 Technology

3.1 Binance-chain as Settlement Layer

Instead of using ETH as collateral and Ethereum as the settlement layer, BiDao uses BNB (Binance coin) as collateral and the Binance-chain as Settlement Layer. Using BNB instead of ETH as collateral has multiple advantages for the Users.

3.1.1 BNB vs. ETH

- ETH is primarily used to pay for code execution on the Ethereum Blockchain. The drawback of this is that ETH is not used as a store of value. Instead of that BNB, it the primary coin of Binance Exchange and Binance DEX. BNB is the base pair for multiple other cryptocurrencies on Binance Exchange and Binance DEX. Moreover, BNB is burned regularly, which makes it more attractive for users to hold.
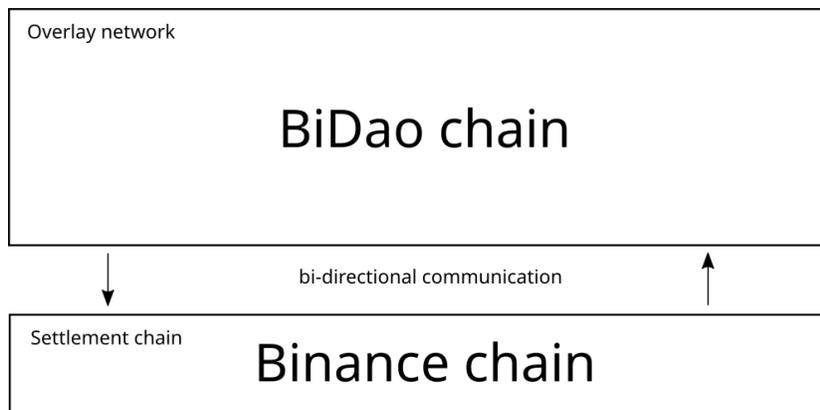
Figure 1: Binance chain as Settlement Layer

- The core focus of Binance-chain is to be a fast and reliable settlement layer. Binance-chain allows the easy and fast creation of digital Tokens and allows to integrate different Tokens. Ethereum and it's Turing complete programming languages like Solidiy and Vyper allow Ethereum Developers to create all kinds of smart contracts, but the drawback is that the Ethereum chain becomes slow, needs lots of memory and is not able to scale.

- Sidechains can be easily deployed to allow smart-contract functionality for Binance-chain. The smart-contract functionality can be easily outsourced to side-chains and Binance-chain is used as a Settlement Layer.

3.2 The BiDao chain

BiDao uses a delegated Byzantine Fault Tolerance (dBFT) [3] consensus mechanism and can support thousands of transactions. The BID Token is used as the native Staking token. The Staking reward is set at around 3% annually. Because of dBFT Staking is extremely convenient. Just leave your BID untouched and your wallet will automatically start staking. The highest priority for the BiDao chain is to communicate with other Blockchains like Binance-chain and Ethereum. This way the BiDao system has access to many different crypto assets.

3.2.1 The BiDao clients

There will be many different BiDao clients. We will concentrate on creating a stable client written in the Haskell Programming language. Haskell is a Programming Language that belongs to the so-called Functional Paradigm of Programming. A big advantage of Functional Programming is that programs can be easily verified with HOL Theorem Provers. One such prover is Isabelle.

3.3 Three Token Architecture

There are 3 Tokens within the BiDao system. One Token is needed as the stablecoin. Another Token is needed for staking, governance and payment of fees. And of course, BNB is used as the collateral.

- **BAI as stablecoin:** The stablecoin of the BiDao system is called BAI. The target price of BAI is 1 USD. This means that 1 BAI can be sold for 1 USD on exchanges. The target price is reached through in-built game theory [4], that incentivizes participants to keep the value of 1 BAI to 1 USD.

- **BID as staking and governance coin:** BID is used as the staking and governance coin within the system. BID holders play an important role in governing the BiDao system. Moreover BID can be staked and used for paying the fees within the BiDao system.

- **BNB as collateral:** As shown is Section 3.1, BNB is perfectly suitable as collateral within a CDP system. BNB has all the important characteristics to be used as collateral.

3.4 The Stablecoin BAI

Once the Stablecoin (BAI) has been generated it can be used exactly like Bitcoin or Ethereum. Which means that it can be transferred between account or simply held in the Wallet. The Target Price for one BAI is 1 USD which means that it is 1:1 pegged to the US Dollar. This value is guaranteed due to the fact that in the case of a price drop of the Binance Coin the insufficiently backed contracts are liquidated and with this, the target price of the BAI can be maintained.

BID
Governance
+
Staking

BNB
Collateral

BAI
Stablecoin
1 BAI = 1USD

Figure 2: 3 Tokens of Bidao

3.5 The Stability Mechanism of BAI

In this section, it will be described how the BAI stablecoin can be stabilized. The goal is that 1 BAI equals 1 USD. For the following it is important to understand the Target Price and the Stability Fee.

Target Price: The Target Price of 1 BAI equals 1 USD. This means that the equilibrium state of the system is that all participants value 1 BAI equal to 1 USD. This can be achieved by the Bidao stability mechanism.

Stability Fee: The Stability Fee is an internal parameter of the Bidao system. The Stability Fee can be changed by a quorum of the BID Tokenholders. The Stability Fee is a fee that has to be paid in order to close the CDP and withdraw the collateral.

In the following we will look at different market scenarios and how the BAI stablecoin can be stabilized in each situation. At first, we have to analyze the different situations that could occur. Basically, there are 3 cases:

- The market values 1 BAI equal to 1 USD,
- the market values 1 BAI < 1 USD and
- the market values 1 BAI > 1 USD.

It can be seen that in case 1, BAI is stable and meets the Target Price. In this case, nothing has to be done in order to stabilize BAI. In order to understand the stability mechanism, we have to look at the cases in which BAI deviates from the Target price (1 USD).

7

Case 2 (1 BAI < 1 USD): In this case 1 BAI is worth less than 1 USD. In order to understand this outcome, we have to look at the market dynamics. Let us consider that 1 BAI = 0.95 USD. This means that BAI is 5% below the Target Price and therefore a way to increase the price of BAI by 5% has to be found. In open and free markets there are only 2 options to increase the market value of an asset: increase demand and/or lower the supply of the asset. In order to increase the demand for BAI, the Stability Fee can be increased. If the Stability Fee is increased, open CDPs become more expensive and some users will close open CDPs. In order to close CDPs, BAI stablecoins have to be repaid, which means that the demand for BAI stablecoins increases. Moreover, the supply of BAI stablecoins decreases because users are paying back their debt in order to withdraw their collateral. Hence, in order to re-stabilize BAI, BID Tokenholders will vote for Stability Fee increases until 1 BAI = 1 USD.

Case 3 (1 BAI > 1 USD): In this case 1 BAI is worth more than 1 USD. Let us consider that 1 BAI = 1.05 USD. This means that BAI is 5% above the Target Price. In order to re-stabilize in this case, the supply of BAI has to be increased and the demand for BAI has to be decreased. This can be achieved by lowering the Stability Fee. If the Stability Fee is lower, it becomes more attractive for users to open CDPs, because open CDPs become cheaper. This way more BAI will be generated by opening CDPs and moreover the demand for BAI on the market will decrease, because less users need to buy BAI on the open market in order to close their CDPs. So in this case BID Tokenholders will vote for Stability Fee decreases until 1 BAI = 1 USD.

It can be seen that the game-theoretical equilibrium of this system is that 1 BAI equals 1 USD. If the market price deviates from the Target Price, there is an incentive for market participants to re-stabilize the value of BAI.

3.6   Fees on the BiDao Platform

2 Percent of the borrowed BID Tokens are withheld and 100% of which are distributed among the BiDao Token Holders and therefore acts as a usage fee on the platform.
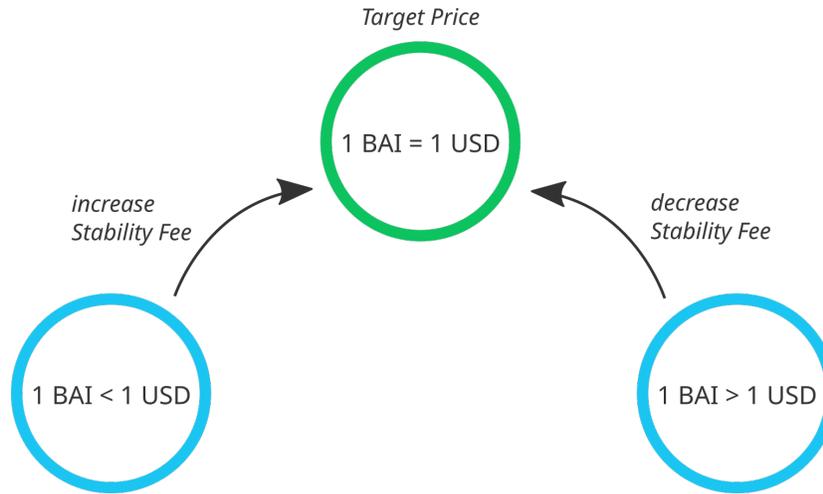
Figure 3: Stability of BAI

3.7 Proof of Stake

The BID is a stake-able Token which means that its holders able to generate Passive income on top of the Fees of the Platform just by holding their coins. To Stake the BID Token all you need to do is download the BiDao wallet for your device, transfer your assets to it and after a maturity period of 12 hours you automatically receive a staking reward. On top of this, it's not necessary to keep your wallet open all the time like with POS cryptocurrencies. This way you don't need a powerful computing system or exorbitant amounts of electricity to earn your reward. With BiDao your receive a staking reward of about 3% which is much more than the Bank would pay you and there is no limit to the amount of BiDao you're able to stake

3.8 BiDao Governance

The BID Token is used as the governance Token. By owning more BID, the voting power of a certain address increases. This means that addresses with more BID have more voting power than addresses with less BID. We refer to the voting power ϕ of a certain User $\nu \, as \, \phi_\nu$. The total voting power Φ can then be calculated by $\sum_{\nu \in V} \phi_\nu$.

Theorem 3.1 *Let ϕ_ν be the voting power ϕ of a certain User ν, then the total voting power is $\Phi = \sum_{\nu \in V} \phi_\nu$.*
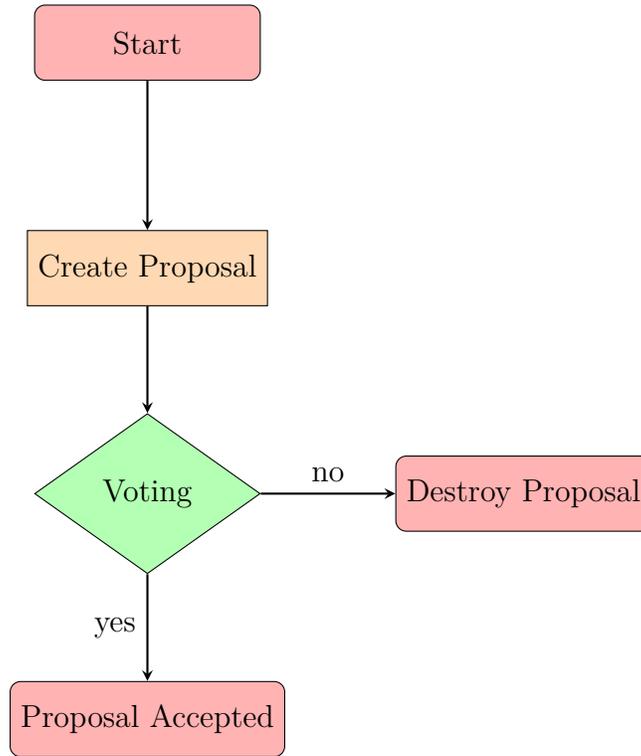
9

Figure 4: Process of Proposal governance

A BidDao Proposal can be proposed by any user who holds some BID. BidDao Proposals can change internal parameters of the BidDao system, like the Stability Fee. After a BidDao Proposal is accepted by the majority of Tokenholders, the Proposal becomes active and changes internal system parameters that have been defined within the proposal. Let V_1 be all the users that voted for Proposal 1. Proposal 1 will be only accepted if $\sum_{\nu \in V_1} \phi_\nu > \frac{\sum_{\nu \in V} \phi_\nu}{2}$

Theorem 3.2 *Let V_1 be the set of Users who voted for Proposal 1, then the Proposal will only be accepted if $\sum_{\nu \in V_1} \phi_\nu > \frac{\sum_{\nu \in V} \phi_\nu}{2}$.*

3.9 Collateralized Debt Position Smart Contracts

BiDao employs similar smart contracts to the MakerDao system. Instead of using ETH (Ethereum) as collateral, the BNB coin will be used as collateral. Moreover a faster and more specialized Blockchain architecture is used. The system uses Binanechain as settlement layer and builds upon this layer an additional Blockchain system that handles the Smart Contract process management. Everybody, who has collateral assets can use them to generate BAI in the BiDao smart contract environment. CDPs have been introduced to the cryptocurrency market by the MakerDAO team. CDP stands for Collateralized Debt Position. This means that a CDP holds collateral assets that have been deposited by a user and permit this user to generate the BAI stablecoin that is pegged to USD. Generating BAI also generates debt in the system. This debt locks the collateral in the smart contract system until the debtor pays back an equivalent amount of BAI. After the equivalent amount of BAI is paid back, the debtor is able to withdraw the collateral. To keep the system secure, the debt is always over-collateralized. This means that the value of the collateral is higher than the value of the open debt position.

3.10 The CDP Process Diagram

In this section, the process of creating and closing a CDP will be described. We will show, how to create a CDP and which steps are needed to set up a CDP. Moreover we will show at which step within the process, the BAI stablecoin will be generated. The basic process can be seen in Figure 1.

3.10.1 The Akteurs

- **Akteur 1: User** The *User* is the person or entity, that is interacting with the CDP.

- **Akteur 2: BID Holder** The *BID Holder* is the person or entity that holds the BID Token. The BID Token is used for paying fees and for governance puroposes within the system.

3.10.2 The Process of creating a CDP

- **Process 1: Create the CDP and deposit the required**

collateral At first the User has to create the CDP. This is done with a single transaction. After that, the User has to deposit the required collateral. After depositing the collateral, the User is able to generate the appropriate amount of BAI.

- **Process 2: Generating BAI** In a follow up transaction, the User is able to generate the BAI stablecoins. The BiDao system then locks the collateral. The collateral stays locked until the debt is paid back by the User.

- **Process 3: Paying the debt and Stability Fee** If the User decides that he wants to unlock the collateral, the User has to pay down the debt and additionaly a Stability Fee. The Stability Fee has to be paid in BID Tokens.

- **Process 4: Withdraw the collateral** After the CDP is debt-free, the User can withdraw all of the collateral, or just parts of the collateral.

4 Fundraise

BiDao is conducting a Tokensale for fundraising. A Tokensale can also be called ICO, which means Initial Coin Offering. During the sale, contributors will be able to buy BID Tokens. The Tokensale is organized in different phases with different goals and prices.

4.1 Why is a Fundraise needed?

Developing a new cryptocurrency and blockchain system is very labour intensive. A professional team of highly skilled developers is needed to create a new blockchain system. We are only satisfied with the optimal solution, therefore a fundraise is needed to fund the development of BiDao. Moreover, the BiDao system can only work optimally if the BID Token can be distributed amongst many different people. This is the case, because the Bidao governance mechanism is more resistant against voting cartels and manipulation, the fairer the BID Tokens are distributed. By "fairer" we specifically mean, that single entities are not able to manipulate the output of votings. The best way to achieve a fair Token distribution is to conduct a Tokensale and allow as many people as possible to participate in the sale.
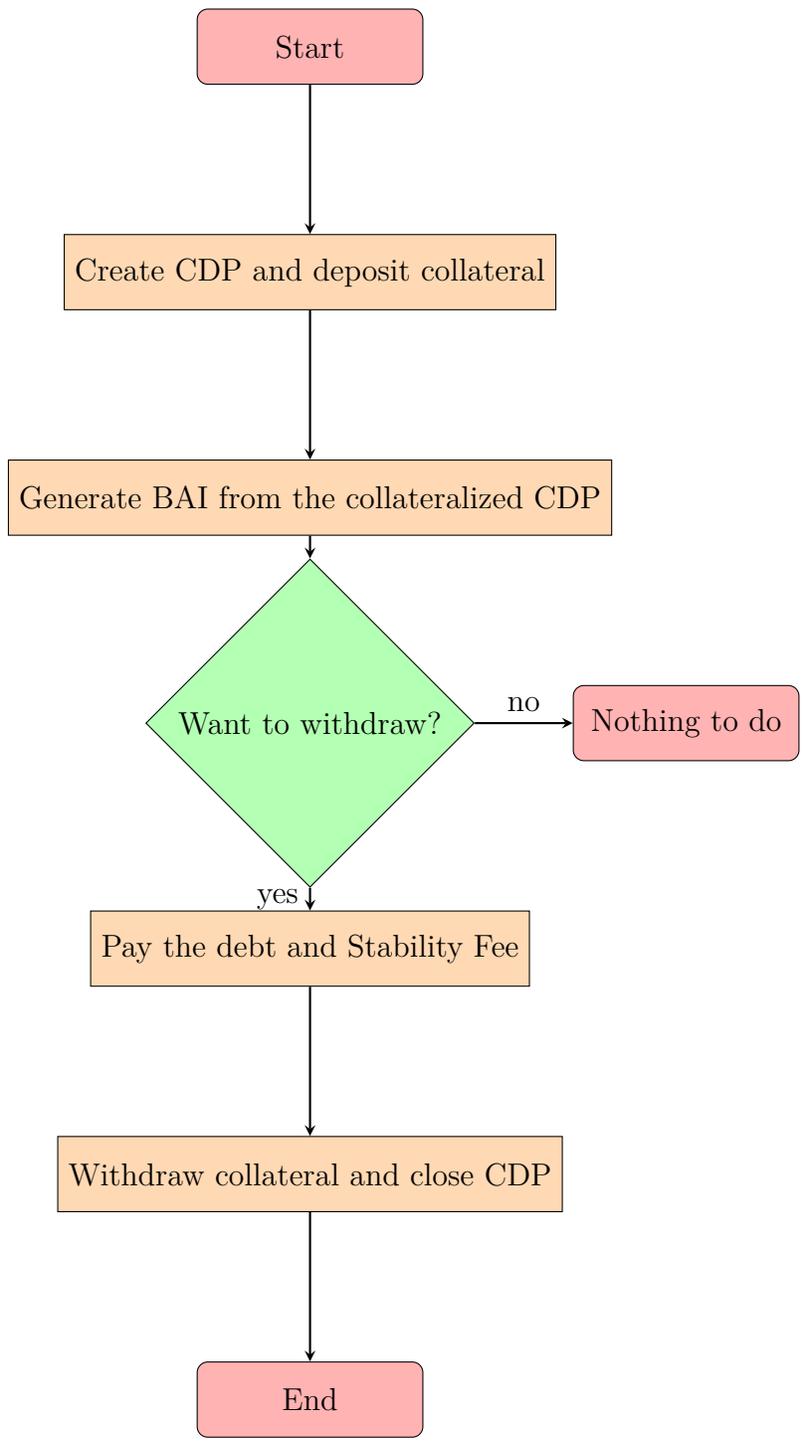
Figure 5: Process of CDP creation

4.2 Distribution of BID Tokens after Fundraise

Our goal is to evenly distribute the BID Tokens amongst as many users as possible. Because of this, most BID Tokens will be sold during the BID Tokensale.

- **Tokensale (75%):** 75% of all BID Tokens will be sold during the Tokensale. This guarantees that there are no big entities that controle most of the BID in circulation.

- **Founders (5%):** 5% of the BID Tokens will be held by the Founders.

- **Developer Bounties (5%):** 5% of the BID Tokens are reserved for Developer Bounties. Developer Bounties are helpful during the development, because this way developers can be incentiviced to help debugging the platform.

- **Marketing Bounties (13%):** 13% of the BID Tokens are reserved for Marketing Bounties.

- **Advisory Board (2%):** 2% of the BID Tokens will be given to our Advisors. This shows that our Advisors will stay long-term commited to our project.

4.3 How is the Fundraise structured?

The fundraise uses a new model of fundraising - the so-called Power Stake Tokensale PST. This means that the earlier you join, the longer you will be able to stake your BID Tokens. In each phase people are able to buy the BID Tokens. In total, 1.95 billion BID Token will be sold during the Tokensale. Staking is already enabled during the Tokensale, moreover, Tokensale participants will be able to become so-called Powerstakers. The price is 0.01 USD per 1 BID. The earlier you join the Tokensale, the longer you will be able to powerstake. Staking Power is set to 30%. After the Tokensale, the Staking Reward stays 3%.

4.4 How to Powerstake?

Powerstaking is super easy! You just have to keep your BID Tokens in your wallet without transferring them.

List of Figures

References

[1] Chris Dannen. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners.* Apress, Berkely, CA, USA, 1st edition, 2017.

[2] Melanie Swan. *Blockchain: Blueprint for a New Economy.* O'Reilly Media, Inc., 1st edition, 2015.

[3] Wikipedia contributors. Byzantine fault, 2019. [Online; accessed 22-July-2004].

[4] Drew Fudenberg and Jean Tirole. *Game Theory.* MIT Press, Cambridge, MA, 1991. Translated into Chinesse by Renin University Press, Bejing: China.