The BitShares Blockchain

BitShares Blockchain Foundation
officially approved spokesperson of the BitShares Blockchain
www.bitshares.foundation
info@bitshares.foundation

***Abstract*—The BitShares Blockchain is an industrial-grade decentralized platform built for high-performance financial smart contracts. It represents the first decentralized autonomous community that lets its core token holder decide on its future direction and products.**

1 Introduction

The BitShares Blockchain, as it exists today, was launched on 13th October 2015 with its community being established already in 2013. It implements an industrial-grade decentralized platform built for high-performance smart contracts with focus on the financial technologies sector.

Furthermore, BitShares represents the first decentralized autonomous cooperation that lets holders of its core native token BTS decide on its future direction and governance aspects. For sake of clarity and to avoid confusion with other smart contracting platforms, the BitShares Blockchain implements its contracts in form of operations . Even though the BitShares Blockchain comes with over 50 already implemented operations which deserve to be presented, this document focuses on the description of the BitShares Blockchain as a platform, its architecture as well as its governance system using the core native token BTS.

2 Architecture

The BitShares Blockchain constitutes the following components which are described individually.

2.1 Transactions

When users want to interact with any Blockchain, they construct so called *transactions* and transmit to the network (see section 2.3). These present messages that contain instructions about what particular *operation(s)* a user wants to use. A common operation is the simple *transfer* operation that comes with transfer-specific instructions that provides the necessary information for this action, such as the sender, receiver, the amount to transfer as well as an optional encrypted memo. To allow multiple operations to take place subsequently, multiple operations can be bundled into a single transaction.
To identify against the system, transactions are cryptographically signed by the users. These signatures *authenticate* a user and provide *authorization* for the operations in the transaction.

2.2 Blockchain

The Blockchain serves as a journal (e.g. a ledger) of user-signed instructions that become a binding agreement as soon as they are included into a block. After inclusion into a block, the agreements are stored indefinitely by means of a hash-linked-list (the Blockchain). From this ordered sequence of transactions, a *current state* (think: account balances) can be determined by processing all transactions consecutively starting at the very first block. As we will see later, the software will ensure that instructions that are stored in the Blockchain have been successfully authenticated and validated. For validating and processing of operations, a common set of rules define the consequences of particular actions, which are part of the of the blockchain protocol (see section 2.5).

2.3 Networking

A blockchain merely defines a means of storage and can be used in a non-distributed, single-participant fashion as well as in a distributed internet-based mesh network often referred to as Peer-2-Peer (P2P) network. In the latter case, multiple parties are connected with each other in a way that incoming transactions are forwarded to every other connected participant. A transaction ultimately reaches a so called *block producer*. A block producer verifies incoming transactions against a hard-coded protocol and bundles them into a single block that is added to the existing blockchain. At this point, a transaction is considered confirmed and executed. The effects of an executed operation on the current state are defined in the blockchain protocol (see section 2.5).

2.4 Consensus

Consensus is the process by which a community comes to a universally recognized, unambiguous agreement on a piece of information. In the context of blockchains, consensus means agreement about the validity rules for transactions (i.e. the blockchain protocol - see section 2.5), and the order in which they have been observed by the blockchain. This ultimately results in an agreement about the *current state* that is build deterministically from those validity rules and the sequence of transactions.

The most commonly known consensus scheme is Proof-of-Work (PoW). Most dominant disadvantage is the heavy power consumption and the scalability in terms of transactions per second and confirmation times. The BitShares Blockchain makes use of an algorithm called Delegated Proof of Stake (DPoS) that was developed specifically to replace the wasteful 'mining' process, increase throughput and reduce reaction times of the

blockchain. It is a tremendous improvement when it comes to consumption of electricity.

DPoS allows to generate a new block at fixed rate (block production/confirmation time) with minimal computational requirements. This means that the blockchain can process more transactions in significantly less time and at almost no cost when compared to PoW-based Blockchains[1]. Block production is performed by a set of so called *witnesses* (block producers) that take turns. After every turn, the order of block producers is randomized in a deterministic manner such that all parties agree on the new order.

2.5 Protocol

The most essential part of blockchain technologies is here referred to as blockchain protocol. It defines the behavior of the entire system including consequences and side-effects when processing transactions. Users utilize particular features by crafting a transaction that contains a particular letter-of-interest (also referred to as *operation*).

Since the Blockchain, as a storage, only stores incremental changes (e.g. transfers), the final balance of each account together with other information needs to be tracked separately in the *current state*.

It is important to note that the protocol is deterministic in the sense that the very same state is generated when applying the same sequence of operations (as provided by the blockchain). This makes blockchain technologies tamper proof and auditable.

In BitShares, over 50 operations are available (as of early 2018). Each of them hooks into the Blockchain protocol at least three times:

- **Validation**: During validation, the raw instructions (also referred to as *payload*) are checked for consistency. E.g., in case of a transfer, we ensure that the amount to transfer is positive.
- **Evaluation**: In the evaluation step, the operation-specific instruction is validated against the current state of the blockchain. In case of a transfer, we here ensure that the amount to be transferred is available in the account of the sender.
- **Application**: This step takes action in the sense that it modifies the current state. In the case of a transfer, we here reduce the account balance of the sender and increase the account balance of the receiver according to the amount of tokens transferred.

Example: Transfer operation Consider a simple *transfer* operation that sends funds from one account to another. Here, the protocol defines the validation rules such that negative amounts are prevented. The evaluation ensures that the sender cannot transfer more than what is in his account balance. When applying a transfer from Alice to Bob, Alice is credited the transferred amount while Bob receives the amount. Here, *transfer* refers to the operation *type*, while the sender, receiver, and amount refers to the operation-specific instructions. Obviously, different operation types come with different instructions.

[1] https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

2.6 Extensibility

The Software behind the BitShares Blockchain is extensively modularized and implements its operations independently of each other. This allows for adding new features once the corresponding code, which the implements validation, evaluation and application methods, reaches maturity. In a sense, operations on the BitShares Blockchain are *smart-contracts* and allows for extending the range of functions of the system. In contrast to other smart-contracting platforms, however, the BitShares Blockchain requires new features to be vetted by the core developers and approved by the BTS holders before they can be installed by means of a network-wide protocol upgrade. As a consequence the platform is considered much more solid as new features require to go through multiple stages of quality assurance. These protocol upgrades are well coordinated and already happened 28 times (Q3/2018) in the past.

2.7 Performance and Scalability

The BitShares Blockchain publicly demonstrated sustaining over 3,000 (three thousand) *transactions* per second and over 22,000 *operations* per second on a distributed test network. This technology can easily scale to over 100,000 (hundred thousand) or more transactions per second with relatively straightforward improvements to server capacity and communication protocols.
To achieve this industry-leading performance, BitShares has borrowed lessons learned from the LMAX Exchange[2], which is able to process 6 million transactions per second. Among these lessons are the following key points:

- Keep everything in memory.
- Keep the core business logic in a single thread.
- Keep cryptographic operations (hashes and signatures) out of the core business logic.
- Divide validation into state-dependent and state-independent checks.
- Use an object oriented data model.

By following these simple rules, BitShares is theoretically able to process >10,000 (ten thousand) transactions per second without any significant effort devoted to optimization. To put things into perspective[3], at peak times, the Ethereum and Bitcoin Blockchain jointly process roughly 0.7% of the peak capacity of the BitShares Blockchain (Q1/2018) as prove from distributed stress testing.

3 Identity

BitShares makes use of human-readable account names that have to be registered together with public-keys in the blockchain prior to its usage. Thus, the blockchain acts as a name-to-public-key resolver similar to the traditional domain name service (DNS). These named accounts enable users to easily remember and communicate their account information instead of using error-prone *addresses*. Depending on individual needs, applications making use of the BitShares Blockchain can create environments

[2] https://martinfowler.com/articles/lmax.html
[3] http://blocktivity.info/

which have full KYC (Know Your Customer) support through so called *whitelisting* which enables a maximum of control or transparency when so desired.

3.1 Permissions

The BitShares Blockchain designs permissions around accounts, rather than around cryptography, making it easier to use. Every account can be controlled by weighted combination of other accounts and/or keys. This creates a hierarchical structure that reflects how permissions are organized in real life, and makes multi-user control over funds easier for users. Hence, BitShares does technically not have multi-signature accounts, but has multi-account permissions. That said, each public/private key pair is assigned a weight, and a threshold is defined for the authority (see definition below). In order for a transaction to be valid, enough entities must sign so that the sum of their weights meets or exceeds the threshold.

3.2 Authorities

The BitShares Blockchain employs a first of its kind hierarchical private key system to facilitate regular keys and backup keys. Regular (*active*) keys are for day-to-day usage, while a separate backup (*owner*) key can be used to recover access to an account in case of loss of the regular keys. Ideally the owner key is meant to be stored offline, and only used when the account's keys need to be changed or to recover a lost key. Most software that supports the BitShares Blockchain also facilitates the use of a Master Password that encrypts the client's keys locally.

3.3 Encrypted Memos

An account on the BitShares Blockchain has a so called *memo* public key associated with it that allows for initiating encrypted communications between two parties by means of a *shared secret*[4] obtain via the Elliptic-curve Diffie-Hellman Algorithm. This allows to attach encrypted messages to transfers that only sender and receiver can decrypt.

3.4 Referral Program

Furthermore, the BitShares Blockchain has an integrated one-level referral system. Basically, everyone interacting on the BitShares blockchain needs to deduct a transaction fee. From that fee (currently) 20% go into the Working Budget (for future funding of development etc.) and the other 80% go into the referral program from where, the registrar (who pays the registration fee and assisted the registration process) as well as the referrer (who brought the user to the registrar) receive a reward. To opt-out of the referral program, an account can be upgraded to a so called *Life-Time Member* (LTM) which replaces registrar and referrer for the original user to receive a 80% refund on his fees.

[4] A shared secret is a term known from cryptography and describes a piece of data, known only to the parties involved in a specific secure communication. The secret can be a password, a passphrase, a big number or any data as long as it is randomly chosen.

3.5 Fees

Similar to most other Blockchains, interacting with the BitShares Blockchains comes with a fee for using its features (i.e. operations). Each operation comes with its own fee. However, any other token that is registered on the BitShares Blockchain, next to the core native BTS token, can be used as fee, if the governor of the other token chooses to support that.

4 BTS - The Utility Token

The core native token of the BitShares Blockchain, BTS, serves as a utility token and offers governance properties to its holders. Governance describes the progress of governing the Blockchains many variable aspects in a way it it can adapt to future changes more easily.

4.1 Governance

On the BitShares Blockchain, decisions are made by the holders of BTS core native token weighted by the amount of BTS owned. In order to improve voting participation and simplify the life of BTS holders, voters can either vote directly or delegate voting power to so called *proxies*. This is similar to a representative democracy, where selected persons decide the course of action. Those leaders have to account for their actions and can be unelected by the core token holders. Unwanted actions includes censoring, favoring, or simply failure to produce blocks in a timely manner. However, the difference to a democracy is that voters in the community have their vote weighted by the amount of BTS that they own in their account.

At any time, voters have to decide on the following aspects of the BitShares Blockchain.

Members for Block Production (Witnesses) Block production in BitShares is arranged through DPoS which requires block producers to run for witness and campaign for sufficient votes from BTS holders before they can produce blocks on the blockchain and consequently get rewarded per produced block. Given the governance system and quick re-tallying of votes, a misbehaving block producer can be dismissed within hours. Next to the actual selection of block producers, the voters also have a say over how many block producers should exist.

Members for Blockchain Governance (Committee) The Committee comprises a board that has control over a few blockchain parameters such as block size, block time, witness reward, and over 30 others. Additionally, the committee can change the fee schedule which defines the minimum fee for each operation offered by the system. Voters can cast a vote for how many members the committee should constitute as well as vote for a particular set of members.

Project Funding (Workers) Last but not least, the voters have control over who receives funding from the Working Budget of the Blockchain. A worker applies for project funding and needs to campaign for sufficient votes before being rewarded. Similar to block producers and committee members, the rigorous

voting system allows almost immediate removal by BTS holders and proxies.

4.2 Initial Allocation

The way that BitShares, as it exists today, came into existence is well documented in the archives of bitsharestalk.org. The BitShares Blockchain was created on 13th of October 2015 by the community and block producers of BitShares 0.9 who decided to start a new token with a distribution identical to where 0.9 had evolved. It was based on code developed with private resources and given to the world for anyone to use under the MIT license. The previous BitShares 0.9 Blockchain was abandoned by the community who had the option to continue that chain but declined to do so.

In the *genesis block* of the BitShares Blockchain a total of 2,412,042,197.37963 BTS have been distributed to individual keys accordingly. These BTS can still be claimed by proving ownership of the corresponding private key.

The BTS token comes with a limited supply that is different from circulating (liquid) supply. A max supply of 3,600,570,502.10207 BTS has been put in place on the blockchain. This can never change. The difference of initial roughly 1.1B was set aside for future project funding and rewarding block producers, and is only accessible with approval by the BTS holders through the worker system. This so called working budget is also often referred to as *reserves*. It is worth noting that revenues made from transactions fees are not shared with holders of BTS but instead go back into the working budget to further allow future development. There is no reward for holding the core BTS token in any way.

4.3 Supply

In this section, we would like to discuss the actual supply of the core BTS token in more detail. Firstly, we define the *max supply* as that supply that can at most be in circulation, similar to how there will only ever be *up to* 21 million BTC on the Bitcoin Blockchain. Furthermore, the *circulating supply* represents that amount that currently is in circulation and held by participants on the Blockchain. Obviously, the circulating supply will always be smaller than or equal to the max supply. Furthermore, for voting, only the *circulating supply* applies.

4.4 Working Budget

The difference between max supply and circulating supply is called the *Working Budget* and has often in the past been referred to as the *reserves*. The BitShares Blockchain has a daily budget to use for development. This budget has a hard-coded upper limit of

$$\text{Total funds in the } \textit{working budget}/2924.$$

From this daily budget, block production as well as for project funding are made. Of course, the BTS holders have the choice and need to approve BTS tokens leaving the working budget.

Block Production (Witnesses) Block production comes at a cost for running and maintaining equipment. The BitShares Blockchain acknowledges this fact by rewarding block producers in core BTS tokens per produced block. Depending on the valuation of BTS, the committee can modify the amount of BTS rewarded per block. As of Q1/2018, each block is rewarded with 1 BTS. Those BTS are taken from the working budget.

Project Funding (Workers) A certain amount of the daily available tokens can be allocated to make development possible by means of workers. Anyone can set up a worker on the BitShares Blockchain and ask for a daily allowance in BTS. If the BTS holders approve a particular worker, the BTS are transferred from the daily budget. A soft-limit defines the maximum amount of the daily budget that is given to all approved workers. Consequently, those workers that have received more votes from BTS holders will receive their funds first. This means that workers, even if approved, may not be funded if the aforementioned threshold is hit. Furthermore, workers constantly stand under the scrutiny of the BTS holders who can disapprove (i.e. retract their vote, 'fire') workers that do not deliver.

4.5 Transaction Fees & Fee Schedule

Additional to block production and project funding which can drain tokens from the working budget, there are transaction fees paid by users of the BitShares Blockchain that go back into the working budget. As a consequence, the total amount of BTS in the working budget as well as the total in- and out-flow highly varies over time. However, if compared to most proof-of-work-based Blockchains that constantly reward a (more or less) fixed amount of tokens to miners, the BitShares Blockchain has a chance to have the working budget grow and consequently the circulating supply shrink. This is the case if the total transactions fees outweigh the tokens used for block production and project funding.
While, the BTS holders have choices to either increase or decrease the funds used for block production and project funding, the committee has the choice to adapt the transaction fees by means of updating the fee schedule. In contrast to other Blockchains, the BitShares Blockchain comes with fixed fees instead of a fee market[5]. The schedule defines which feature of the Blockchain requires which amount of transaction fee for using it.

4.6 Legality of the BTS token

It is worth noting that the BitShares Blockchain is not a traditional registered entity and has no seat. The core token BTS does not imply any ownership rights. The core token merely serves as a utility for governance, arranging transaction fees and operating other features that are solely implemented on the BitShares Blockchain.

[5] https://arxiv.org/abs/1709.08881