LEASED PROOF-OF-STAKE

TIM BOS, ROHAN LE PAGE, TRANG TRAN & TAN DO

CONTENTS

Version	Date	Editor	Comments
0.1	15/01/2019	ShareRing team	Initial public release for POS

DISCLAIMER

This document is a technical document setting out the current and future developments of the ShareRing platform and the ShareRing ecosystem. An integral aspect of the ShareRing ecosystem is the issuance and usage of the crypto-token known as the ShareToken.

This document is for information purposes only and is NOT A STATEMENT OF FUTURE INTENT.

Unless expressly specified otherwise, the products, services and innovations detailed in this document are currently under development and are not currently deployed. The Promoters of this document and all persons associated with its publication specifically make no warranties or representations as to the successful development, implementation or deployment of any technologies and innovations, or achievements of any other activities noted in this document. The Promoters of this document and all persons associated with the preparation and/or publication of this document each disclaim to the fullest extent permitted by law any and all warranties implied by law.

No person is entitled to rely on the information detailed in this document or any inferences drawn from this document, including in relation to any interactions with the ShareToken or the technologies mentioned in this document. The Promoters of the document and all persons associated with the preparation and/or publication of this document each disclaim all liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and/or opinions relating to the ShareToken, the ShareRing platform or the ShareRing ecosystem or any information which is made available in connection with any further enquiries, notwithstanding any negligence default or lack of due care and skill.

THE PROMOTERS OF THE DOCUMENT AND ALL PERSONS ASSOCIATED WITH THE PREPARATION AND/OR PUBLICATION OF THIS DOCUMENT TAKE NO RESPONSIBILITY NOR ASSUME ANY RESPONSIBILITY FOR ANY ERRORS THAT MAY BE CONTAINED IN THE DOCUMENT.

All information contained in this document is derived from data obtained from sources believed by the Promoters of the document and all persons associated with the preparation and/ or publication of this document to be reliable and is given in good faith. No warranties or guarantees, or representations are made by the Promoters of the document and all persons associated with the preparation and/or publication of this document with regard to the accuracy or completeness correctness or suitability of the information presented.

Nothing in this document should be relied upon and shall not confer rights or remedies upon you or any of your employees, creditors, holders of securities or other equity holders or any other persons whether related to you or not. Any opinions expressed reflect the current judgement of the Promoters of this document. The opinions reflected in this document may change without notice and the opinions do not necessarily correspond to the opinions of the Promoters of the document and/or any persons associated with the preparation and/or publication of this document. The Promoters of this document do not have any obligation to amend, modify or update this document or to otherwise notify any reader or recipient of this document in the event that any matter related or stated in this document or any opinion, projection, forecast or estimate detailed in this document changes or subsequently becomes inaccurate.

The Promoters of the document and all persons associated with the preparation and/or publication of this document do not have any responsibility or liability to any personal recipient (whether by reason of negligence, negligent misstatement or otherwise, arising from any statement, opinion or information expressed or implied arising out of contained in or derived from or omission from this document. Neither the Promoters nor its advisers have independently verified any of the information, including the forecasts, prospects and projections contained in this paper. The Promoters of the document and all persons associated with the preparation and/or publication of this document do not accept any liability that may arise out of any information contained or implied in this document.

Each recipient of this document is to rely solely on its/his/her knowledge, investigation, judgement and assessment of the matters which are the subject of this document and any information which is made available in connection with any further enquiries and such recipient must satisfy itself/himself/herself as to the accuracy and completeness of such matter.

While the Promoters of the document and all persons associated with the preparation and/or publication of this document have attempted to ensure that statements of facts made in this document are accurate, all estimates, projections, forecasts, prospects, expressions of opinion and other subjective judgements contained in this document are based on assumptions considered to be reasonable as at the date of this document in which they are contained and must not be construed as a representation that the matters referred to in this document will occur.

Problems can occur and as such all recipients who act upon the contents of this document do so at their own risk and fully assume the responsibility for such action to the exclusion of the Promoters of the document and all persons associated with the preparation and/or publication of this document. Any plans, projections or forecasts mentioned in this document may not be achieved due to multiple risk factors including without limitation defects in technology development, legal and regulatory exposure, market volatility, sector volatility, corporate actions or the unavailability of complete and accurate information.

The document may refer to a number of hyperlinks to websites of entities mentioned in this document, however. the inclusion of a hyperlink does not imply that the Promoters of the document and/or any persons associated with the preparation and/or publication of this document endorses, recommends or approves any material on the linked page or accessible from it. Such linked websites must be accessed entirely at the recipient's own risk. The Promoters of the document and/or any persons associated with the preparation and/or publication of this document do not accept any risk or liability whatsoever to any such material, nor for consequences of its use.

This document IS NOT DIRECTED TO, or intended for distribution to or used by, any person or entity who is a citizen or resident of or located in any state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation. In particular, this document is not an offer to any residents or domiciles of the United States of America or Singapore.

This document is only available on https://sharering.network and may not be distributed, reproduced or passed on to any other person or published, in part or in whole, for any purpose without the prior written consent of the Promoters. The manner of distribution this document may be restricted by law or regulation in certain jurisdictions. Persons who possess this document must observe all such restrictions.

By accessing this document, the recipient agrees to be bound by the above limitations detailed in this disclaimer.

ABSTRACT

A consensus algorithm is a vital part of any Blockchain and is fundamental to a distributed network. Proof-of-Work, the first consensus algorithm developed by Nakamoto Satoshi, is used by the two most popular blockchain platforms, Bitcoin and Etherum. The algorithm guarantees a unique view across the network by proposing a mathematically complex problem to all participants. Solving the problem successfully first rewards the winner the right to mine a new block. This results in a block reward.

Since its inception, Proof-of-Work has laid the path for many other consensus mechanisms now in circulation. In this document, we describe Leased Proof-of-Stake, a variation used in the ShareLedger distributed ledger. Also addressed is the implementation and technical variances the ShareLedger consensus algorithm provides.

TERMINOLOGIES

This section introduces the key terms used in the subsequent sections in this document. It also gives short explanations to such terms and can act as a summary for future references.

TOKENS:

- *Bonded tokens:* SHR tokens that are locked for MasterNode/Validator holders. Holders of 'Bonded tokens' can participate in the block proposal process.
- The remaining tokens are *standard tokens.*
- When tokens are switched from *bonded* to *standard tokens,* they become *'unbonding'* tokens for at least the UNBONDING_TIME blocks to prevent Token Holders withdrawing tokens after performing any malicious acts. In this case, we have chosen 3 weeks as the UNBONDING_TIME value. More at Slashing.
- Tokens that are being converted from Bonded to a standard Tokens will show a status of *undonding*.

VALIDATOR/MASTERNODE: is a single address which is able to propose a block. A limited number of addresses, with an initial balance of bonded SHR token above 2 Million bonded tokens can hold a MasterNode/Validator (note: This is expected to increase over time) this is defined as MIN_MASTER_NODE_TOKEN. The initial value of MIN_MASTER_NODE_TOKEN is 2000000 (2 million) SHR at genesis. This amount is subject to change without notice.

- Each Validator/Masternode has its own commission rate for providing a token staking service. This commision rate is defined by the Masternode holder.
- The maximum number of MasterNodes is defined on genesis.json

POOL: maintains the latest status of ShareLedger's staking feature including

- Total of available SHR tokens
- Total of bonded SHR tokens = reserve of bonded tokens
- Total of unbonded SHR tokens = number of tokens not associated with any validator
- Total of unbonding SHR tokens = number of tokens moving from bonded to unbonded
- Total of loose unbonded SHR tokens = reserve of unbonded tokens held with validators

DELEGATION: represents the bonding relationship between any address (delegator) and the validator, including:

- The amount of SHR Token (at any address) staked at a validator
- (Possible) the block height that the bonded token updated for statistical purpose.

VOTING POWER: of a validator is proportional to the amount of bonded SHR tokens it holds. In ShareLedger, the voting power depends on the bonded token of each validator.

PROPOSER: is the Validator selected to propose/forge a block at a certain block height.

LEASED PROOF-OF-STAKE

Proof-of-Stake (POS) is a consensus algorithm generally seen as a replacement for Proof-of-Work (POW) algorithm. The latter uses high energy consumption and computing resources to form a block. The former has been developed as a cheaper and more efficient alternative. Unlike POW, where all nodes in the network race to be the first hash the problem solver, POS selects the block validator (or proposer) upfront based on the number of staked (bonded) tokens. Selected proposer for a block gets the right to propose a block for a specific height and then transfers the right to another proposer for the next block.

ShareLedger uses a modified version of POS, namely Leased Proof-of-Stake (LPOS). In LPOS, each validator (Masternode) can receive *delegations* from other token holders (delegators) to increase its staked tokens in return for a share of the block rewards. This is otherwise known as a pool.

The probability of a MasterNode being selected as a Proposer is proportional to its Voting Power, which in turn grows with the number of staked tokens (including delegated or pooled tokens), up to the limits proposed by the Voter Equality System (see below).

PROPOSER SELECTION MECHANISM

Tendermint[1], the underlying consensus algorithm, is responsible for selecting the Proposer for each Block.

ROTATING LEADER ELECTION[2]

Tendermint rotates through the validator set, i.e. block proposers, in a weighted round-robin fashion. The higher the stake (i.e. voting power) that a validator has delegated to them, the more weight that they have, and proportionally more times they will be elected as leaders. To illustrate, if one validator has the same amount of voting power as another validator, they will both be elected by the protocol an equal number of times.

The simplified explanation of how the algorithm works looks like this:

1. Validator weight is established. Initially, all validators are assigned with Weight 0.
2. As each round progresses, each validator's Weight increases an amount equal to its voting power.
3. A validator with highest Weight is elected and is granted its turn to propose a block.

[1] https://tendermint.com/
[2] https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb

4. After the round is completed, the selected validator’s Weight is recalculated and decreases by the total of *Voting Power of all validators.*
5. The loop continues with step 2 above.

For example, let’s consider a set of 3 Validators *(A, B, C)* with respective Voting Power *(1, 2, 3)*.

1. In the beginning, all validators start with Weight of *0.*
2. The first round starts and validators A’s Weight increases by 1. The same goes with validator B and C with the Weight gain 2 and 3 respectively.
3. As the validator with the current highest Weight, validator C is selected as the Proposer.
4. After the round completes, his Weight is reduced by *6* to become *-3.* So the next round starts with the validator set *(A, B, C)* having the respective Weight set *(1, 2, -3).*

For more detailed explanation about how Tendermint selects a Proposer, please consult Tendermit’s document[3].

VOTER EQUALITY SYSTEM

As equality plays a vital role when designing our ShareLedger platform, we have designed a Voting Power calculation algorithm so that there is no notable gap amongst the MasterNodes in terms of Voting Power. This is to avoid a single significant holder of SHR tokens from obtaining an unfair Voting Power, which in turn controls the Block Proposing process of the whole network.

The Voting Power of each node is calculated as follows:

VOTING_POWER = Min(120% x Median(votingPowers), Ceiling((tokens - 2,000,000)))

In which:

- *votingPowers:* all current voting powers of all Masternodes/Validators
- *tokens:* number of tokens that the specific Masternode holds

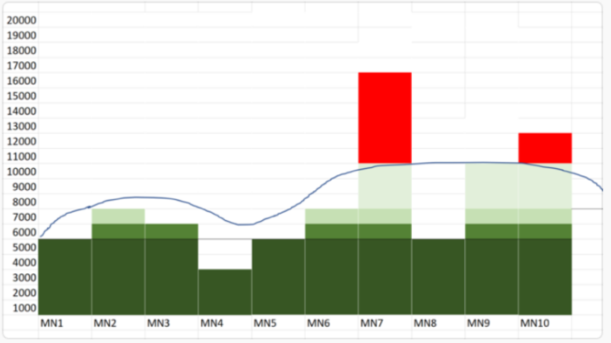
There are several noticeable points from the formula:

- The Voting Power is not linearly proportional to the number of staked tokens. In fact, with Square Root function, the acceleration of Voting Power growth is inversely

[3] https://github.com/tendermint/tendermint/blob/master/docs/spec/reactors/consensus/proposer-selection.md

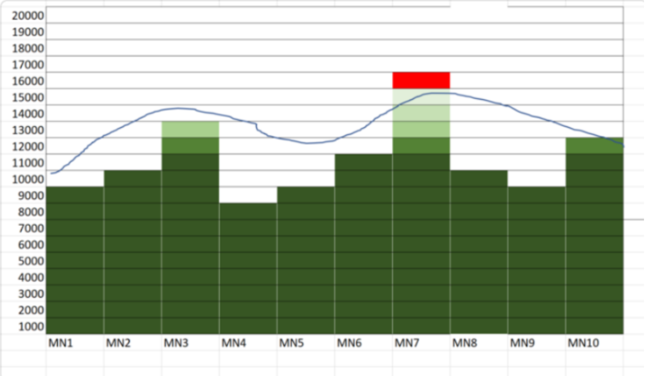
proportional to the increase in the number of staked tokens. That means your Voting Power gain slows down when you stake more tokens.

- The voting power of each node is capped at 120% of the median value of all voting power.



Scenario 1: A MasterNode (MN7) staking a large number of tokens to himself than others.

For example, look at the above diagram. The various shades of green colour indicate the increase of Voting Power equivalent to that number of staked tokens. Deeper green means significant power growth while light green shows a lesser rise. The red colour means no gain in term of Voting Power for staked tokens above the median. In the diagram, Masternode 7 (MN7) notices that it would not be financially beneficial for him to continue staking to himself. He decided to try other options.



Scenario 2: A Masternode (MN7) staking tokens to himself and other nodes

In this new diagram, the MN7 decides to stake his tokens to other Masternodes. Doing so helps the network to raise the median value, which in turn helps MN7 to raise his Voting Power.

With Voter Equality System, Masternodes in the network are incentivized to not only stake to their own nodes but also to other nodes. This helps bring all validators in the networks to the same level of Voting Power achieving a stable Gini Coefficient with times. In other words, the network is less likely to be controlled by a group of major token holders and more likely to distribute equally the right of proposing blocks across all validators.

BLOCK REWARDING

For each successfully proposed block, the Proposer is rewarded with a fixed amount of SHR tokens (REWARD_PER_BLOCK). The reward together with the total transaction fee of such block is distributed proportionally to the contribution of the Validator and Delegators. So, the total earning a validator can receive for each successfully proposed block is:

BLOCK_EARNING = REWARD_PER_BLOCK + TOTAL TRANSACTION FEES

The Validator, then, keeps a fixed percentage of SHR token as the commission for providing block forging services. Each validator has its own commission rate.

Initially, a pool of tokens is reserved to issue rewarding tokens to validators. REWARD_PER_BLOCK remains constant across blocks. The collected transaction fees can be used to purchase SHR tokens on the market to re-distribute to validators at later phases. This increases token liquidity and creates token demand on the market.

SLASHING

If a Validator were to act maliciously to gain more rewards by deliberately making blocks on all available chains, he enacts the *nothing-at-stake*[4] scenario. This is resolved by *Slashing* to disincentivise any Validator who attempts to publish two votes at any block height.

We maintain an additional *Treasury* account and deduce a SLASHING_PERCENTAGE of the bonded tokens from the violator's account to the *Treasury* account.

GENESIS

Every block is preceded by a block except the first one, the Genesis block. The Genesis block is defined by a file, *genesis.json* in which several other parameters of Shareledger are also included such as the number of total bonded tokens, length of unbonding tokens and number of validators at genesis. It is expected to have at least 30 validators at the beginning of Shareledger.

[4] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-the-nothing-at-stake-problem-and-how-can-it-be-fixed

CONCLUSION

Leased Proof-of-Stake, a variant of POS, is the consensus algorithm used in Shareledger. The algorithm provides the ability for all token holders, regardless of any amount, to participate in Shareledger and gain financial profits proportional to their staked tokens. Shareledger also utilizes Voter Equality System to maintain a fair allocation of staked tokens among validators as well as to avoid any attacks resulting from a significant hold of tokens.