Fantom Proof of Stake FIP-2

Andre Cronje, Alex Kampa, Michael Kong, George Samman

March 15, 2019

Contents

1 Introduction

This document introduces the mechanics, mathematical reasoning and formulae for calculating various aspects of Fantom's Proof of Stake system.

Fantom has designed a system with multiple incentive mechanisms to achieve high throughput, scalability, security and decentralisation.

2 Definitions and Variables

General definitions

$\mathcal{F}$	denotes the network itself
N	the set of nodes in the network
SPV	"Special Purpose Vehicle" - a special smart contract acting as an internal market-maker for FTG tokens, managing the collection of transaction fees and the payment of all rewards
FTM	main network token
FTG	network transaction token (gas)
E	set of event blocks in $\mathcal{F}$
$E(d)$	set of all event blocks validated on day d, their number being $\|E(d)\|$

Account Categories

$\mathcal{U}$		set of all user accounts in the network
$\mathcal{A}$	$\subset \mathcal{U}$	user accounts with a positive FTM token balance
$\mathcal{A}'$	$\subset \mathcal{U}$	user accounts with a positive FTG token balance
$\mathcal{C}$	$\subset \mathcal{A}$	accounts that have staked for validation (some of which may not actually be validators)
$\mathcal{V}$	$\subset \mathcal{C}$	validating accounts, corresponding to the set of the network's validating nodes

Network "constants" subject to on-chain governance decisions

F	$3.175e9$	total supply of FTM tokens
δ	30	period in days for determining Proof of Importance
λ	90	period in days after which validator staking must be renewed, to ensure activity
ε	1	minimum number of tokens that can be staked by an account for any purpose
θ	30%	impact of Proof of Importance for rewards
ξ	50%	impact of Proof of Importance for transaction staking
ϕ	30%	SPV commission on transaction fees
μ	15%	validator commission on delegated tokens

Tokens held and staked

Unless otherwise specified, any mention of *tokens* refers to FTM tokens.

t_i		number of FTM tokens held by account $i \in \mathcal{A}$
t_i^x	$> \varepsilon$	transaction-staked tokens by account i
$t_i^d(c)$	$> \varepsilon$	tokens delegated by account i to account $c \in \mathcal{C}$
$t^d(c)$		total of tokens delegated to account $c \in \mathcal{C}$
t_i^d		total of tokens delegated by account i to accounts in $\mathcal{C}$
t_i^s		validation-staked tokens by account i
T_{min}^s	0.1%	minimum tokens staked by $v \in \mathcal{V}$, as a percentage of F
T_{max}^s	0.4%	maximum tokens staked by $v \in \mathcal{V}$, as a percentage of F
M	15	delegation multiplier - maximum ratio of delegated versus staked tokens

The sum of tokens staked or delegated by an account $i \in \mathcal{A}$ cannot exceed the amount of tokens held:

$$t_i^x + t_i^s + \sum_{c \in \mathcal{C}} t_i^d(c) \leq t_i \tag{1}$$

The following limits apply for token staked for validation by $c \in \mathcal{C}$:

$$T_{min}^s * F \leq f_c^s \leq T_{max}^s * F \tag{2}$$

The total amount of tokens delegated to an account $c \in \mathcal{C}$ is:

$$t^i(c) = \sum_{i \in \mathcal{A}} t_i^d(c) \tag{3}$$

The total amount of tokens delegated by an account $i \in \mathcal{A}$ is:

$$t_i^d = \sum_{c \in \mathcal{C}} t_i^d(c) \tag{4}$$

The sum of tokens delegated to an account $c \in \mathcal{C}$ cannot exceed a fixed multiple of tokens staked by that account:

$$t^i(c) \leq M * f_c^s \tag{5}$$

Finally, there is a limit on the amount of tokens that can be transaction-staked or delegated:

$$t_i^d \leq Q * f_i \qquad t_i^x \leq Q * f_i \tag{6}$$

Weight in $\mathcal{F}$

The weight of an account $i \in \mathcal{A}$ is equal to its token holding t_i.

Importance in $\mathcal{F}$

The importance is proportional to gas use in the overall network over the most recent period of δ days.

g_i	gas used by account $i \in \mathcal{U}$ during past δ days
$\mathcal{G}$	gas used in the entire network in past δ days
$\hat{g}_i$	importance of $i \in \mathcal{U}$, rebased to be comparable with t_i

We have:

$$G = \sum_{i \in \mathcal{U}} g_i \tag{7}$$

$$\hat{g}_i = \frac{g_i}{\mathcal{G}} F \tag{8}$$

Transacting Power

The transacting power of an account is defined as a weighted average of an account's weight and importance in $\mathcal{F}$. We note that the sum of all the network's transacting power is equal to F.

x_i	transacting power of account $i \in \mathcal{U}$
X	total transacting power of $\mathcal{U}$

We have:

$$x_i = \xi t_i + (1 - \xi)\hat{g}_i \tag{9}$$

$$X = \sum_{i \in \mathcal{U}} x_i = F \tag{10}$$

Network Performance and Transaction Slots

Π	5,000,000,000	Estimated maximum network processing power, in FTG per second
Θ	500,000	Estimated maximum network throughput, in Bytes per second
σ^g		transacting power needed for a slot of 1 FTG per second
σ^b		transacting power needed for a slot of 1 Byte/second of throughput

Given that at most F tokens can be transaction-staked, we have:

$$\sigma^g = \frac{F}{\Pi} \approx 0.635 \tag{11}$$

$$\sigma^b = \frac{F}{\Theta} \approx 6350 \tag{12}$$

Weight in $\mathcal{V}$

Because only a fraction of tokens are staked or delegated for validation, we need to determine a relative weight in order to correctly determine the total validating power of the entire network $\mathcal{F}$.

w_v	tokens staked by, and delegated, to validator $v \in \mathcal{V}$, which represents the weight of this validator
W	total tokens staked by, and delegated to, validators

Thus, we have:

$$w_v = t^s_v + \sum_{i \in \mathcal{A}} t^d_i(v) = t^s_v + t^i(v) \tag{13}$$

$$W = \sum_{v \in \mathcal{V}} w_v \tag{14}$$

Importance in $\mathcal{V}$

The importance in $\mathcal{V}$ proportional to gas use by accounts that have staked or delegated tokens.

h_v	gas use over the past δ days attributable to validator $v \in \mathcal{V}$
$\mathcal{H}$	total gas use over the past δ days attributable to all validators
$\hat{h}_v$	importance of $v \in \mathcal{V}$, rebased to be comparable with w_v

We have:

$$h_v = g_v + \sum_{i \in \mathcal{A}} g_i \frac{t^d_i(v)}{t_i} \tag{15}$$

$$\mathcal{H} = \sum_{v \in \mathcal{V}} h_v \tag{16}$$

$$\hat{h}_v = \frac{h_v}{\mathcal{H}} \mathcal{W} \tag{17}$$

Validator Scores

The validator score will be a number between 0 and 1 representing a composite of three different performance metrics.

s_v	$\in [0,1]$	the total score of validator $v \in \mathcal{V}$
s_v^w	$\in [0,1]$	validating performance score of v
s_v^t	$\in [0,1]$	transaction origination score of v
s_v^p	$\in [0,1]$	processing power score of v

Validating power

The validating power of a validator is defined as a weighted average of a validator's weight and importance, multiplied by its score:

p_v	validating power of validator $v \in \mathcal{V}$
P	total validating power of $\mathcal{V}$

Thus, we have:

$$p_v = s_v[\theta q_v + (1-\theta)w_v] \tag{18}$$

$$P = \sum_{v \in \mathcal{V}} p_v \tag{19}$$

Rewards

Z	996,341,176	total available block rewards of FTM, for distribution by the SPV during the first 1460 days after mainnet launch
F_s		FTM tokens held by the SPV
F_c	$F - F_s$	total circulating supply
$B(d)$		total transaction fees paid by network users on day d
$R^v(d)$	$\phi * B(d)$	total transaction rewards retained by the SPV on day d
$R^x(d)$	$(1 - \phi) * B(d)$	total transaction rewards to be distributed on day d
$R^b(d)$		total block rewards to be distributed on day d
$R(d)$	$R^x(d) + R^b(d)$	total rewards to be distributed on day d
$R_v(d)$	$R(d) * (p_v/P)$	total daily rewards attributable to validator $v \in \mathcal{V}$ on day d, that will be paid out to the validator and to all user accounts who have delegated tokens to that validator
$D_i^v(d)$		total daily delegation rewards received by $i \in \mathcal{A}$ attributable to validator $v \in \mathcal{V}$ on day d (exclusive of validator rewards)
$D_i(d)$	$\sum_{v \in \mathcal{V}} D_i^v(d)$	total delegation rewards received by i from all validators on day d
$D^v(d)$	$\sum_{i \in \mathcal{A}} D_i^v(d)$	total delegation rewards received by all delegators attributable to validator v
$I_v(d)$		daily validator rewards received by $v \in \mathcal{V}$ on day d (exclusive of delegation rewards)

Block rewards will be distributed over 1460 days (4 years less one day) after launch, corresponding to $Z/1460$ per day during that period:

$$R_b(d) = \begin{cases} 682{,}425.46, & \text{during 1460 days after mainnet launch.} \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

Validating index

The number of votes that a given block has for $v \in \mathcal{V}$.

Validating threshold

2/3 of validating power is needed to confirm an event block to finality.

3 Overview of Token Staking and Delegation

FTM tokens will have multiple uses in the Fantom system, one of these being the right to stake and delegate them. When staking or delegating, a user's weight will be determined not only by the number of FTM tokens held, but also by his "importance" to the network as measured by the gas spend within a 30 day period.

The three possibilities are:

Transaction staking This provides users with a guaranteed transaction volume on the network ("transaction slots").

Validation staking By setting up a sufficiently powerful and well-connected computer, staking a certain minimum amount of tokens, and if necessary, attracting sufficient token delegation from other users, users can become network validators. This gives them a share of block rewards and of transaction fees generated by the network, as well as a share of fee income in proportion to tokens delegated to them.

Validation delegation Users can delegate all or part of their tokens to a validator to gain a share of block rewards and transaction fees generated by the network.

In addition, FTM holders will also be able to participate in on-chain voting, but that is outside the scope of this paper.

4 Delegating Staking

Users will be able delegate a portion of their tokens to validating nodes. Validators will not be able to spend delegated tokens, which will remain secured in the user's own address. Validators will receive a fixed proportion of the validator fees attributable to delegators. They will therefore compete based on their performance and not on fees. Higher performing node, with more reliable uptimes, will earn higher returns. Delegators will be incentivised to choose nodes that have a high validator score, i.e. are reliable and high performing.

Delegators can delegate their tokens for a maximum period of days, after which they need to re-delegate. The requirements to delegate are minimal:

- **Security deposit** None
- **Minimum number of tokens to delegate** 1
- **Minimum lock period** None
- **Maximum number of validators a user can delegate to** None
- **Maximum number of tokens that can be delegated to a validator**: 15 times the number of tokens the validator is staking

Fantom aims to promote and develop software that makes it convenient to delegate to validators through a straightforward UI.

5 Validation Rewards

5.1 Validator Rewards Overview

Validators will receive block and transaction rewards for the tokens they have staked, as well as a percentage of the rewards attributable to the tokens that have been delegated to them. These rewards will also depend in part on their score. It will therefore be in the interest of every validator to maintain a top score, in order to maximise its income and attract delegators.

What validators have staked is at risk at every single message they send. Delegated tokens are not at risk, but they may lose their payout or receive a lower payout if a validator does not perform.

Rewards will be computed daily, and yesterday's rewards will be distributed today.

5.2 Validator Score

The validator score is a number between 0 and 1 which measures the quality of a validator. It will determined by the sum of a validator's "validation performance",number of "originating transactions" and processing power. These are mechanisms designed to incentives node participation for originating and validating transactions. Nodes that fail to do both lead to a decrease in throughput and security, while increasing time to finality.

There will be several measures of performance:

Validation performance (s_v^w) Given that block finality is reached when an event block has reached the validating threshold of 2/3rds of the network's validating power, we say that a validator effectively participated in a block validation if such validation occurred before the validation threshold was reached. An efficient validator should, on average, effectively participate in validating 2/3rds of all event blocks. Those who consistently do not participate, or participate after the validation threshold is reached, will be penalized, earn fewer block rewards, and will ultimately be pruned from the network.

Originating transactions (s_v^t) Validators will be expected to accept new transactions being submitted to the network and act as originators of such transactions. Those who consistently do not originate transactions will be penalized, receive fewer block rewards, and will ultimately be pruned from the network.

Processing power(s_v^p) The processing power of validators will be measured on a regular basis.

These will be explained in further detail in future iterations of Proof of Stake.

5.3 Block Rewards

Block rewards will be split between validators, according to their validating power, and paid out to validators and delegators.

Each validator will receive its share of the full block reward for its staked tokens, plus a fraction of μ of its delegators' block rewards. Delegators will receive $(1-\mu)$ block rewards based on the validating power of their validator.

5.4 Rewards from Transaction Fees

A fixed proportion ϕ of transaction fees will be retained by the SPV, the rest being distributed to validators and delegators as transaction rewards.

As with block rewards, each validator will receive the full transaction reward for its staked tokens, plus a fraction of μ of its delegators' transaction rewards. Delegators will receive $(1-\mu)$ transaction rewards based on the validating power of their validator.

5.5 Reward Formulae

5.5.1 SPV Rewards

The SPV retains the proportion ϕ of all transactions fees.

5.5.2 Validator Rewards

Validators receive the full rewards corresponding to the validating power of their own staked tokens, as well as a proportion μ of the rewards attributable to their delegators.

$$I_v(d) = R_v(d)\frac{t_v^s + \mu t^i(v)}{w_v} \tag{21}$$

5.5.3 Delegator Rewards

The delegators receive the portion of the rewards corresponding to the validating power of their own staked tokens, as well as a proportion μ of the rewards attributable to their delegators. The total of delegator rewards for validator v is:

$$D^v(d) = R_v(d)\frac{(1-\mu)t^i(v)}{w_v} \tag{22}$$

The reward of delegator i attributable to validator v is:

$$D_i^v(d) = R_v(d)\frac{(1-\mu)t_i^d(v)}{w_v} \tag{23}$$

5.5.4 Average Block Reward Yields

The distribution of block rewards over a 4 year period yields the following average returns across validators and delegators (based solely on block rewards):

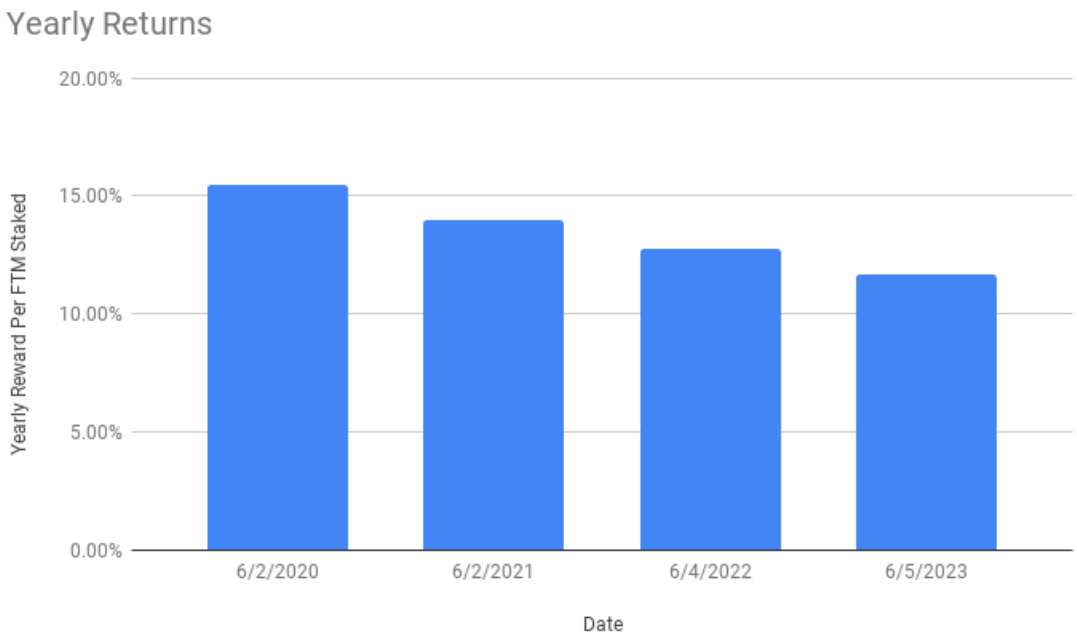

Figure 1: Returns over a four-year period from staking

The returns above are based on the following assumptions:

- Block rewards are distributed daily over 4 years at a fixed amount
- At all times, 70% of the total circulating supply of FTM will be used for validation staking (staked by the validator plus delegated staking)

Fantom's network offers a comparatively high yield to other distributed ledgers using Proof of Stake. The aim of such high yields is to make it attractive to stake and thus secure the network over a long period of time.

After the launch of the mainnet, the foundation will guarantee a floor (measured in USD) in FTM equal to the cost of a validator's hardware up to a certain limit. Although (at the current FTM/USD rate) block rewards alone should cover hardware costs, the guarantee is to ensure that the network encourages high performing, optimal hardware from the beginning. The performance of a given validator can be measured by the network and tied to the coinbase of the validator, with the performance compared to the cost of cloud computing providers such as AWS and Microsoft Azure. The difference between the cost of running a node and block rewards received will be covered by the Foundation, paid directly into the validator's Coinbase. Further details will be released closer to mainnet launch.

6 Transaction-Based Staking

6.1 Introduction

FTM holders can stake a portion of their tokens to secure a guaranteed transaction volume on the network. This is known as "Transaction-based Staking".

Staking tokens gives FTM holders a guaranteed transaction slot consisting of:

- gas, expressed in FTG/second
- data throughput, expressed in Bytes/second

The size of the slot will be proportional to the transacting power of the tokens staked.

6.2 Network Processing Power and Throughput

To estimate the maximum gas that can be spent per second, we start by noting that the best modern desktop processors (such as the Intel Core i9 Extreme Edition) have already reached teraflop speeds - one trillion floating point operations per second.

Every instruction processed by the Fantom Virtual Machine ("FVM") will carry some overhead, as it has to verify signatures and track gas spent.

- Let's assume that only 10% of processing power is available for executing transactions and smart contracts, and that a single multiplication by the FVM costs 100 floating-point operations
- FVM can process one billion multiplications / second (i.e 5 billion gas - utilising Ethereum's gas pricing as a guide)
- $5,000,000,000/21,000 = 238,095$ basic transactions (simple transfers of value from one address to another
- A basic transaction has, on average, a size of 120 bytes
- This would result in a data volume of $230,095 * 120 = 27$ MB / second

A data volume of 27 MB/ second just for new transactions, in addition to consensus protocol traffic, is far too high. This means that if the majority of transactions are relatively simple, the main bottleneck will be network throughput.

The current assumptions are:

- $\mathcal{F}$ can support 5 billion gas / second
- A reasonably high maximum transaction throughput of 0.5MB / second

6.3 Example

In order to be guaranteed one basic transaction per second, whose size is assumed to be 120 Bytes, a user would need to stake tokens with a transacting power corresponding $120 * 6,350 = 762,000$. If that user's gas usage is in line with his token holdings, his transacting power will be roughly equal to his token holdings, so the necessary number of transaction-staked FTM tokens will also be $\approx 762,000$

This corresponds to $762,000/0.635 \approx 1,200,000$ FTG per second, which is quite high.