Cosmos Token Model

DRAFT

Sunny Aggarwal
sunny@tendermint.com

December 2017

1 Introduction

The Cosmos Hub is a Proof of Stake based blockchain that uses Tendermint consensus and serves as a backbone to the Cosmos ecosystem. This paper is a subset of a larger paper that will detail and justify the design decisions used in the cryptoeconomic design of the Cosmos Hub and its Proof of Stake mechanisms. This paper will focus particularly on the Cosmos Hub's token model. The final paper will include details on topics such as slashing conditions, delegation of stake, inflation rate algorithms, and more. This paper assumes familiarity with the Cosmos whitepaper by Jae Kwon and Ethan Buchman. [KB17]

2 Role in the Cosmos Ecosystem

The Cosmos Ecosystem is a partially-ordered network of blockchains called zones that run concurrently and interoperate to create a multi-blockchain ecosystem. It is termed an Internet of Blockchains as much like the traditional Internet which connects otherwise isolated networks, Cosmos connects otherwise isolated blockchain networks. These multiple blockchains can communicate using a protocol called Inter Blockchain Communication (IBC), which can be thought of as the TCP/IP of Cosmos. Much like how Internet Service Providers (ISPs) help route IP packets, Hubs are special blockchains that help zones route IBC packets. The Cosmos Hub is one such hub to which zones can connect to and is secured by an open and globally decentralized set of validators. On the Cosmos Hub, tokens can be held by individual users or by zones themselves. Along with just providing routing for packets, the Cosmos Hub also preserves the global invariance of the total amount of each token across the zones, preventing zones from double spending other zones.

Many ISPs, along with providing Internet connectivity, also offer a variety of additional services such as web hosting. Similarly, the Cosmos Hub also provides hosted consensus. While zones can connect to the Cosmos Hub with their own independent validator sets, zones also have the opportunity to be validated by the Cosmos Hub validators and benefit from the shared security of all the chains operated by the Cosmos Hub validators.

Because the Cosmos Hub is responsible for the operation and consensus of many chains, the security and cryptoeconomic design of the Hub is of paramount importance.

3 Tendermint Consensus

As detailed in the Cosmos whitepaper, the Cosmos Hub uses Tendermint as its consensus algorithm. Tendermint is a byzantine fault tolerant consensus algorithm developed in 2014 to address the speed, scalability, and environmental concerns of Proof of Work. The economics of Cosmos Proof of Stake are heavily dependent on Tendermint consensus due to its design of involving all validators in the production of each block, a substantial difference from Nakamoto consensus. Furthermore, its strict accountability for byzantine faults allows us to punish misbehaving validators and provide economic security for the network. It is expected that the reader is fairly familiar with the details of the Tendermint consensus algorithm. [Kwo14]

The Cosmos Hub uses Tendermint in its public Proof of Stake context. This works in the following method as described by the Tendermint whitepaper:

> “Validators are users with accounts that have coins locked in a bond deposit by posting a bond transaction. We say that a validator has voting power equal to the amount of the bonded coins.”

In such a system, the validator set is open and permissionless, which means that anyone who owns some of the coins in the system can bond their coins and become a validator. In the Cosmos Hub, this staking token is known as an Atom. The limited resource of Atoms acts as a sybil prevention mechanism. An entity can create and distribute their Atoms among many validator nodes but their sum total of their voting power is equivalent to having just a single validator. Because all that determines a validator’s voting power is their bonded stake and not reputation or real world identity, validators can choose to be either anonymous or public.

One of the key innovations of the Tendermint whitepaper was the idea of using validator “security deposits” which can be seized and burned by the protocol in a process known as ”slashing” if a validator is caught creating attributable byzantine faults that harm to the well-functioning of the system thus solving the Nothing-at-Stake problem suffered by first generation Proof of Stake blockchains like NXT and BitShares 1.0. These security deposits are locked in a bonded account and when a staker wishes to unbond their staked tokens, they are put into an “unbonding period” during which proof of malicious activity can be submitted. The details of the slashing conditions which lay out the possible byznatine faults and their respective punishments will be covered in a future paper.

4 Token Economics and Incentives

Let us examine some of the fundamental economics and incentives of blockchain systems. To do so, let us first define the two primary classes of actors in a blockchain network, the keepers and the users. The term keepers refers to a class of actors that act as the operators and maintainers of a blockchain network. In the context of blockchain consensus, keepers refers to miners in a Proof of Work setting and stakers in a Proof of Stake setting. The users of a blockchain network are the people who are deriving some utility from the network. In any public blockchain, the keepers of the chain are essentially offering the service of providing consensus to the users of the blockchain, and in order for them to do this, they need to be incentivized.

In order to explore incentivization, let us first set up some basic premises of the concept of value. Blockchain ecosystem tokens can be considered a type of commodity. In classical economics, commodities have two identified types of value: use value and exchange value. Use value is defined the “want satisfying power” of a commodity. It is based on the utility of the commodity. Meanwhile, the exchange value of a commodity is defined as “the amount of goods and services which we may obtain in the market in exchange for a particular thing”. We may commonly think of this as the price of the commodity.

We can define the economic security of a blockchain consensus system as the amount of money needed to be spent in order to attack the system, which is proportional to the exchange value of the commodity needed to be consumed in order to pull off the attack. In Proof of Work, the commodity needed to be spent is electricity, and thus the economic security is the number of joules needed to attack times the exchange value (price) of joules. Similarly, in Proof of Stake, the economic security is based on the number of staking tokens needed to have more than 33% of stake times the exchange value of the staking token.

For many different reasons, the exchange value of a commodity might be greater than the use value of the commodity. Trying to reason about and predict the exchange value of Atoms is very difficult, especially due to the lack of market data before launch. However, interestingly, the exchange value is effectively lower bounded by the use value of the commodity. Thus, we can use this lower bound in order to reason about the economic properties of our system.

In most Proof of Work blockchains, the miners are paid by the users through transaction fees and sometimes block rewards which need to be paid in some token that has exchange value. In these Proof of Work blockchains, there is usually a native token whose primary purpose is to pay transaction fees in the network. In some cases, this same token also has some other desired utility as well. For example, in Bitcoin, the token is used to pay transaction fees but also acts as a generic monetary currency. But at the very minimum, the use value of the token is its utility in affording you to use the blockchain due to its necessity in paying transaction fees. Because this token has a use value, this gives it a lower bounded exchange value, thus allowing it be used to compensate miners for their role in providing consensus.

5 Atoms: The Staking Token

The naive approach to creating a Proof of Stake blockchain is to try and extend this single token model and use it for both fees and staking. Because the single token already has some minimum exchange value enforced by its use value, it provides economic security to the Proof of Stake by making sure there is real economic value at stake. This is done by many Proof of Stake systems. For example, when switching to Casper, Ethereum plans to use its existing fee token, Ether, as its staking token. While there is some merit to the conceptual simplicity of this model, it does lead to potential risks and issues.

In the single token model, the single token has utility beyond mere staking, thus there will be a reasonably liquid amount of tokens that are not staked. This more utility that the token has beyond staking, the more liquidity of that token is required for those purposes, meaning a larger percentage of the tokens will not be staked. This weakens the security of the system as it makes it easier to stealthily obtain enough tokens required to attack the system.

For example, in a Proof of Work network, because electricity and computational power have so many alternate utilities other than mining, the vast majority of these resources are not used for mining and thus are ”unaccounted for”. For a Proof of Work blockchain using an ASIC-resistant hashing, it would be possible for a large government to suddenly shift a lot of its electric and computational resources to mining to attack the system. However, because SHA-256 ASICs have little utility beyond Bitcoin mining (which is largely dominated by ASICs), it is reasonable to assume that close to all existing SHA-256 ASICs are already currently mining, and thus it is highly unlikely that any entity could suddenly start mining and have over 50% of the hashrate. Any attempt to try to mass produce or buy up a majority of ASICs would take time and would also likely send detectable signals into ASIC markets, allowing governance mechanisms to be able to preemptively respond i.e. changing the hash function.

Let us imagine a hypothetical situation in which a large whale owns 5% of the total supply of Ether in the Serenity Ethereum blockchain with Casper. This whale could single handedly pull off a 33% attack if less than 15% of all Ether was staked. But because Ether has so much utility outside of staking, it will likely be very difficult to get 15% of Ether to be staked, causing an economic security risk.

So instead, Cosmos uses a multi-token model in which the Atom, is used primarily only for staking, and is not intended to be used to pay fees or used as a currency. Essentially the optimal utility of the token should be to stake it. But if this token no longer has use value derived from its function as a fee token, where does it get enough exchange value to give economic security to the system?

The utility of the Atom is that it is necessary for staking and thus gives you the ability to earn the transaction fees and the block rewards of chains validated by the Cosmos Hub validators, which includes the Cosmos Hub itself as well as any hosted chains. Atoms can basically be seen thus as somewhat analogous to ASICs in Proof of Work; it is a piece of virtualized hardware that you need to obtain in order to participate as a keeper in the network. Because partaking as a keeper in consensus allows you the earn transaction fees (paid in a token that has economic value as described above), the value of the staking token thus becomes the expected profit to be earned from the transaction fees and block rewards in the network, which are paid in a fee token. This can be observed in the increase of the price of SHA-256 ASICs as the expected earnings from mining Bitcoin have increased as well.

If you have a certain percentage of the staked Atoms, you have the ability to earn that percentage of the transaction fees and block rewards. You can earn more either if there is an increase in the value of transaction fees going through the network or if you obtain more Atoms, giving you a larger percentage share thus affording you a larger percentage share of the transaction fees and block rewards.

In the Hub, there are block provisions given in Atoms. These are technically analogous to block rewards but serve a different purpose. They are there in order to incentivize Atom holders to stake. Because Atoms are given as block provisions to stakers, there is a continuous inflation rate of Atoms. Atoms holders who do not stake are thus punished through inflation as their percentage share of the total Atom supply decreases as they do not receive any of the newly minted Atoms. This creates a significant incentive for Atom holders to stake their Atoms as there is a continuous transfer of wealth from non-stakers to stakers. The inflation rate targeting mechanism targets an inflation rate based on the percentage of staked Atoms. The inflation of Atoms is a percentage of the total supply, and thus the block provisions per block increases as the total supply of Atoms increases. We use the term provisions rather than reward because the function of the provisions is primarily to punish non-stakers than to reward stakers.

Because of inflation going to only stakers and the lack of alternate designed utility for the Atom, a large majority of the total Atoms will be staked (greater than 66%). This makes it far harder for the situation described at the beginning of this section to occur in which a large whale stakes and gets over 33% of the bonded tokens. If anyone tries to buy the amount of Atoms required to get 33% of the stake on the open market, the market for Atoms would get progressively more illiquid causing the price of each successive Atom more expensive, greatly increasing the cost required to make an attack feasible.

6 Transaction Fees

In a blockchain, transaction fees serve two primary purposes: spam-prevention and a payment to keepers for their work in operating the blockchain. Blocks need to have some sort of scarce resource that limits the amount of work need to validate a block. If you tried to put the entire pending mempool into the next block, someone could spam the mempool causing the block to take too long to validate. In Bitcoin, this scarce resource is the block size and in Ethereum it is the gas limit. Because there is limited space in a block for a limited number of transactions, in order to determine which transactions from the mempool get added into a block, each transaction is accompanied by some sort of transaction fee that gets paid to keepers of the blockchain. The proposer of a block then uses these transaction fees to order the transactions by fee, thereby maximizing their earnings from proposing that block as the transactions with the highest fees get added to the block before the limit is reached. Different transaction use differing amounts of resources, so instead of ordering by absolute amount of transaction fee of a transaction, we instead order by transaction fee per resource i.e. BTC per byte in Bitcoin or "gas price" (ETH per gas) in Ethereum.

The Cosmos Hub, having a limited number of types of transaction, will not use gas counting per opcode like most turing-complete blockchains, but rather assigns each transaction type a weight based on its estimated computational and storage costs. For example, because an IBC transaction is more computationally complex than a token transfer within Cosmos, the transaction cost for an IBC Tx will be greater than that for a SendTx.

7 Many Fee Tokens

A novel feature of the Cosmos Hub is that unlike most other public blockchain platforms is that transaction fees can be paid in any whitelisted token. Most other platforms only allow fees to be paid in a single token, such as Ether in Ethereum, Bitcoin in Bitcoin, and GAS in Neo. In line with the "multi-token ecosystem" mindset of Cosmos, the Cosmos Hub, instead of forcing users to use a specific token in order to pay transaction fees in the system, allows users to select from a number of possible tokens. We will discuss how this works and then the benefits of such a system.

Let's delve into how to make this multi-fee token model work and allow for validators to be able to compare transaction fees paid in differing tokens/currencies in order to do transaction ordering. In the Hub, there exists a whitelist of tokens that are allowed to be used to pay fees in. At launch, the first two tokens that will be whitelisted as fee tokens are Atoms and Photons (will expand on Photons in next section). Somewhat contrary to the previous section of this paper, at the Cosmos Hub, Atoms can also technically be used as the fee token of the Cosmos Hub, and will have to be used as such at launch because there are no other tokens in the system. However, as more chains connect into the Cosmos ecosystem, the tokens from these other chains can be added whitelist by the Cosmos validators through governance. The reason for needing to go through governance to add new tokens to the whitelist is that fees are shared amongst validators, and thus it is necessary that there is consensus amongst the validators as to which tokens they are willing to accept as a group. As more chains and tokens join the Cosmos ecosystem, it can be expected that more of these tokens will become whitelisted fee tokens.

In order to allow for validators to compare the transaction fees being paid in different tokens, there needs to be a way to determine the relative value of each token. Trying to get validators to come to consensus on the current market price of each token would require using either a centralized oracle or pulling prices from an on-chain decentralized exchange (which isn't guaranteed to match the prices on off-chain exchanges). So, instead of trying to get all the validators to agree on prices of all the tokens on each block, we let the block's proposer use their view of how much they value each token to order transactions when it's their turn to propose.

Each validators node has a personal config file which lists their personal weighting of how much they value each token. These weights are what the validator will use to determine transaction ordering when it is their turn to be a proposer.

The initial version of the config file contains only the Atom and the Photon.

```
Atom: 1
Photon: 1
```

Each validator can manually adjust these values to their liking (these values were just chosen randomly as an example):

```
Atom: 5
Photon: 3
```

As more tokens get whitelisted, they get added to the config file as such:

```
Atom: 5
Photon: 3
BTC: 0
ETH: 0
```

Then each validator can also adjust these new values as well:

```
Atom: 5
Photon: 3
BTC: 5000
ETH: 0.2
```

Having such a config file allows validators to run a separate process like a cron job that live updates the configuration file based on live market data pulled from their favorite exchange's API (or combining the data of multiple!). If the exchange API is unreachable, the validator can set the config to fallback to the last available values, pull data from an on-chain exchange, or even resort to a backup default config (such as one in which Atoms have a weight of 1 and everything else has a weight of 0).

Let's walk through an example of deciding the order of two transactions using the above config. Let's say we have two SendTx of equal gas cost and the tx fees on them are 0.5 BTC and 13000 ETH respectively. The first one's transaction fee is worth 2500 (5000×0.5) while the second one's is worth 2600 (0.2×13000), and thus the second transaction will have priority to go into the block over the first one.

Having many tokens be usable as fee tokens heavily reduces the friction involved in using the Cosmos Hub. Because the primary use of the Cosmos is for users to move their tokens from one chain to another chain, users are likely to own the token that will be moved and want to pay fees in that token. In a system with only a singular fee token, it creates a poor user experience because now users would have to obtain the fee token just to make their transactions. This will likely increase the usage of the hub, as the friction in using the hub is greatly reduced. Regarding the complexity of choosing which token to pay with from the tokens the user owns, this choice will likely be dealt with by wallet software or DApps so that the average user does not have to think about it, much like how *amount of fee to pay* is already done so. For some power users (for example frequent governance participants), it does make sense to hold a stock of Atoms or Photons, because using one of these as the fee token will generally be the safest option to getting your transaction in to the chain as fast as possible, as the majority of validators will accept them.

Along with providing a better experience to users, this multiple fee token model also provides a better experience for validators. Unlike other protocols that impose one token as the first class token in the chain, the Cosmos Hub lets validators have a sovereign view on what is valuable. The validator set of Atom holders will inevitable have multiple and diverse preferences about what tokens they find valuable in the cryptocurrency ecosystem, and so we can allow them to accept and be paid in a variety of these different tokens. It is more work on the part of the validators to maintain a relative weighting of different tokens over time, but it is to give them more freedom in how they want to be paid. Any individual validator can always forgo this and stick with a default config file in which everything has a weight of 0, other than one token such as the Atom or Photon.

8 Photon

We've been repeatedly mentioning a token called Photons. But what are these Photons? Photons are a new token being introduced in the Cosmos ecosystem and are designed to act as one of the first multi-chain tokens. Because the Atom is designed as a staking token, the Photon can act as a fee token until more tokens join the Cosmos ecosystem either by directly joining the Hub or through Peg Zones which can bridge over existing tokens like BTC and ETH.

Photons are awarded as block rewards to the Cosmos Hub validators for validating the Hub and also serve to reduce transaction fee costs for users. The Photon block reward is will be a constant 500 Photons per hour, which leads to an inflation rate that asymptotically reaches 0. However, instead of starting from an initial supply of 0 and all the Photons going to Cosmos validators, which wouldn't make for a very distributed initial allocation, there will be an airdrop initial allocation to Atom and Ether holders (through a Hard Spoon). The percentage split going to Atom and Ether holders respectively will be chosen through Cosmos governance.

In Ethereum, a large portion of Ether is stored in smart contracts such as multisigs and not just in externally-controlled accounts. Because of this, in order to allow Ether holders to claim their photons, we would need to fork the entire Ethereum state, including contracts, into an EVM. Luckily, we have a project called Ethermint which allows anyone to spin up an EVM chain running on Tendermint consensus.

This Ethermint Hard Spoon zone with the Ether holders' Photon distribution, in a process that will require approval by governance, will be one of the first zones to connect to the Cosmos Hub, within weeks of the launch. Once this happens, Ether holders can claim their Photons and migrate them to the Hub and then into the rest of the Cosmos ecosystem. Note that the Hard Spoon zone, due to being ”polluted” with the state of the current Ethereum blockchain, is not intended to be used as a normal Ethermint zone for smart contracting purposes but rather as a way for users to claim their Photons. There will be other Ethermint zones connected to the Hub that users can use to build smart contracts and Dapps on top of.

Unlike the Cosmos SDK on which the Cosmos Hub is being built, due to the

EVM currently being designed for only singular fee tokens, it is likely that Photons will be the primary fee token on the **initial** Ethermint zones launched and hosted by the Cosmos Hub validators.

9 Conclusion

Hopefully, this paper helped give a clear sense of the token model of the Cosmos Hub, especially with regards to the incentives and utilities of different tokens in the staking and fees mechanisms. The larger paper which covers more details about many other aspects of the Cosmos Hub cryptoeconomics such as slashing, delegation, inflation, and much more will be released very soon!

References

[Kwo14] Jae Kwon. “Tendermint: Consensus without mining”. In: *Draft v. 0.6, fall* (2014).

[KB17] Jae Kwon and Ethan Buchman. *Cosmos - A Network of Distributed Ledgers*. Mar. 2017. URL: `https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md`.