Minter Whitepaper

April 05, 2022

Minter is a decentralized digital assets marketplace. It is a single point of access to the largest digital and crypto currencies—BTC, ETH, BIP, USDC, and thousands more—allowing one to buy, sell, send, and spend them right inside a wallet. Minter is built around the concepts of the Internet of Money (IoM) and decentralized finance (DeFi), meaning each user can manage their funds as they see fit without middlemen or trusted third parties such as financial institutions.

Unlike in other networks and protocols, all functionality is implemented at the core level of blockchain, making it possible to reach high operational speed, independence from external services, and maximum compatibility among components within a single ecosystem.

Major Functionality and Advantages

- Transactions complete in 5 seconds with final blocks (no need to wait several blocks for confirmation)
- Any liquid coins and tokens swappable for one another (*)
- Liquidity pools with a 0.3% fee (0.2% goes straight to providers, 0.1% goes towards BIP buyback)
- AMMOB: Automated Market Maker pools with on-chain Order Books (limit orders)
- Low transaction fees fixed in U.S. dollars ($0.01 per trade, $0.03 per swap) and payable in any liquid coin (backed) or token (non-backed) of the network (*)
- Your own tokens and liquidity pools created in just a couple of clicks
- Cross-chain transfers across Minter, Ethereum, BNB Smart Chain, and others

(*) If the coin's reserve drops to the minimum required level of 10,000 BIP or the token has no pools, they cannot participate in such transactions.

Technical Side

Minter is a blockchain powered by the Tendermint engine, running on the Delegated Proof-of-Stake (DPoS) consensus algorithm. Key characteristics:

- Average block time: up to 5 seconds
- Throughput: 10,000 transactions or 1M receivers (multi-send)
- Number of validators: up to 64 (with the capacity to increase, if necessary)
- Number of validator's slots (maximum number of delegators): 1,000
- Base coin: BIP (maximum supply: 10B)
- Dynamic mining: block reward depends on the price of the native coin, which is BIP
- Ability to lock stake for increased rewards

Block Structure (Network Specification)

- Header
- Transactions
- Signatures of >⅔ of validators

The algorithm of generating addresses and the signature scheme have been imported from Ethereum (Cryptographic Signature Scheme: Elliptic Curve Digital Signature Algorithm).

Base coin BIP

BIP is Minter's native utility coin that is mined with each new block and circulated inside the network. The final supply is 10 billion units. The resulting quantity of BIP, however, may be lower due to various types of burning—by balancer, by users, of ticker fees, and for marketing purposes.

Use Cases of BIP

- Delegate and get rewards (portion of block rewards + transaction fees)
- Provide custom coins with reserve, or back them
- Pay all network fees (+30 types of transactions)
- Validate the network (mining, voting power)
- Supply liquidity to pools (for 0.2% of the amount swapped)

The distinctive feature of Minter tokenomics is that transaction costs can be covered in any liquid coin or token. But in the end, they will all be converted into BIP and further distributed among stakeholders or burned whatsoever.

Also, any token that has a pool (trading pair) with BIP can be set as a fee price indicator. For that, validators need to vote for it. In such a case, the current in-pool price will be used to calculate the amount of BIP necessary to pay the fee.

BIPx

For BIP to be used in the world's best decentralized finance (DeFi) services beyond Minter, it will be issued on other blockchains under the BIPx ticker. It has already gone live on Ethereum July 1st, 2021, and arrived at BNB Smart Chain (BSC) September 2nd, 2021.

When you withdraw BIP to another network, it is locked on Minter and released on a given network as BIPx. The reverse operation is similar: BIPx is burned on the external network and unlocked on Minter as BIP. The exchange rate is always 1:1.

Smart contract of BIPX on Ethereum:
0xcafE34BAE6F1b23A6B575303EdCc0578d2188131

Smart contract of BIPX on BNB Smart Chain:
0xf2Ba89A6f9670459ed5AeEfbd8Db52Be912228b8

In short, BIPx is BIP mirrored onto the outer chains. To learn more, read **this article**.

Custom Coins and Tokens

On Minter, there are several types of digital objects, and each has its own features. Any user can create their own coin or token to later be used in their project, business, or community. To maximize functionality and enable flexibility in case of varying scenarios, we divided objects into 2 types:

1. Coins are reserved digital objects constantly backed by the base coin BIP. Coins can be delegated in order to receive network rewards, or converted via reserves and liquidity pools. The coin's price changes depending on the amount of BIP in its reserve. One can buy or sell any amount of the coin without a counterparty—when buying, the coins are burned and the corresponding share of BIP reserve is returned; when selling, vice versa.
2. Tokens are non-reserved digital objects that have no direct backing. They can be additionally minted or burned by the owner, which is good for mirroring external assets as tokens are not tied to the base coin BIP and their exchange is only possible through liquidity pools.

They share some common parameters:

- Name
- Ticker
- Version (in case of re-creation)

- Initial issuance
- Maximum supply

Reserved Coins

Each custom coin is backed by BIP. That is how the instant liquidity principle is maintained, meaning any coin can be swapped for any other coin in any volume. Such an approach ensures free conversion, under which the BIP reserve flows from a coin sold into a coin bought.

To calculate the number of BIP that the user has to get after selling a custom coin, the following formula is used:

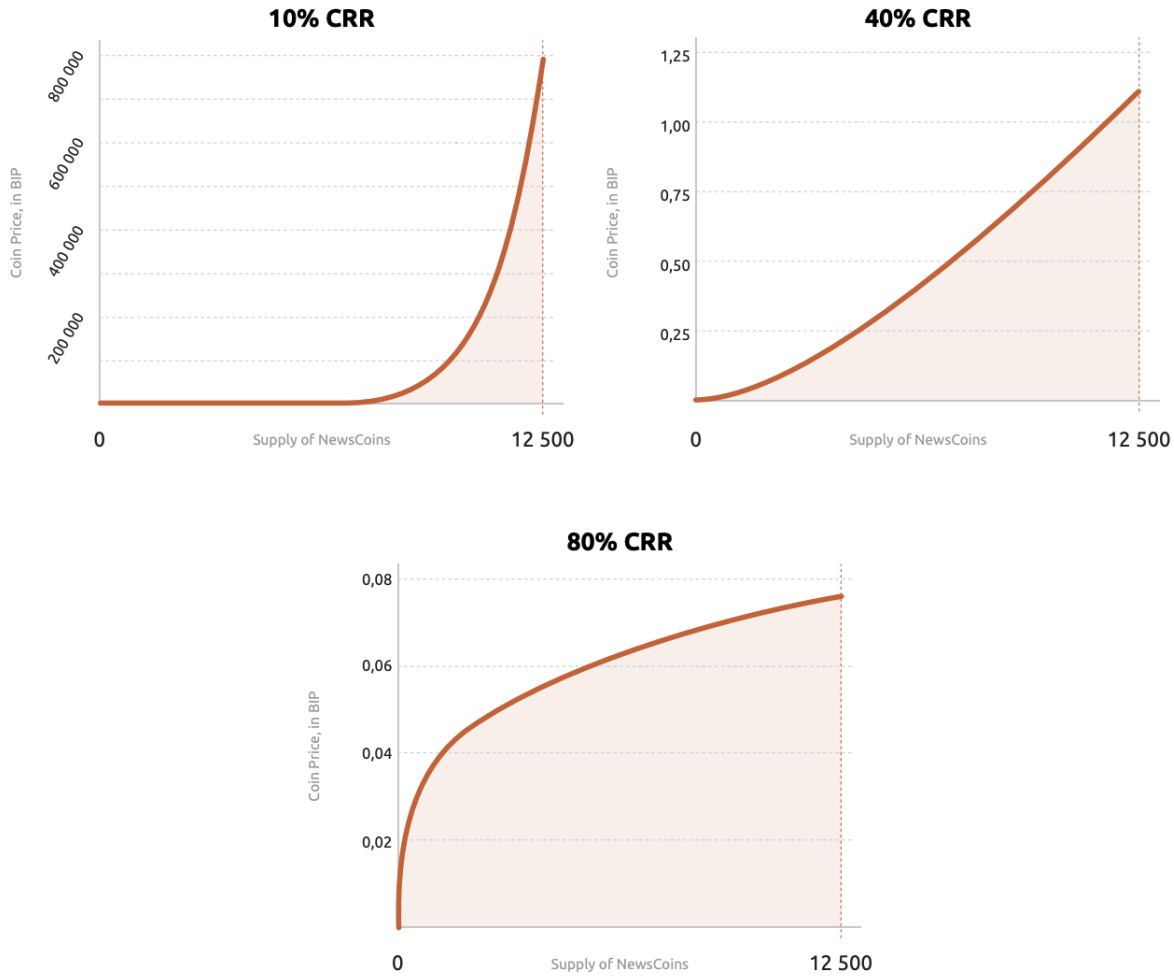
$$reserve * (1 - (1 - sellAmount / supply) ^ (100 / crr))$$

If it is needed to calculate the current price of a custom coin, the sellAmount value is usually set to 1.

The coins can be converted both through reserves and liquidity pools (if any).

CRR

The CRR (Constant Reserve Ratio) value determines the degree of liquidity—i.e., how much each coin in the total supply is reserved. The higher the CRR, the bigger the backing, the more resistance to fluctuations. For example, with a CRR of 100%, the coin's price will always remain the same.



For more examples of coins with different CRRs and an in-depth description of the instant and absolute liquidity mechanism, check out this **document**.

Non-Reserved Tokens

Unlike coins, tokens have no BIP reserve and are, in fact, “empty.” This leads to a number of restrictions (e.g., tokens cannot be delegated), but makes it possible to:

- Mint (owner)
- Burn (anyone)

One of the main application areas for tokens is mirroring from other networks. For example, a popular stablecoin USDT can be freely moved from Ethereum to Minter and the other way around. For that, the USDTE token was issued on the Minter network, which, when moved between the chains, is frozen on one network and released on the other.

Within the Minter network, tokens can be swapped via liquidity pools they participate in.

Coins versus Tokens

Function	Coins	Tokens
Reservation	in BIP	—
Min reserve	10000 BIP	—
Name	up to 64 letters long	up to 64 letters long
Symbol	3 to 10 symbols long	3 to 10 symbols long
Initial amount	Yes	Yes
Max supply	Yes	Yes
CRR	10 - 100%	—
Mintable (by owner)	—	Yes
Burnable (by any address)	—	Yes
Swap (reserves)	Yes	—
Swap (pools)	Yes	Yes
Creation of liquidity pools	Yes	Yes
Delegate and receive rewards	Yes	—
Ticker symbol fees	10 - 100000 USD	10 - 100000 USD
Pay fees	Yes	Yes
Re-creation	Yes	Yes

Minter HUB

Minter Hub is a bridge interconnecting different blockchains that is responsible for cross-chain transfers, lock control, and token mint and burn. Minter Hub is Minter's sidechain, whose first release connects Minter with Ethereum and BNB Smart Chain.

Executing user commands, Minter Hub acts as a custodian and operator of tokens across chains mentioned above. For example, using the bridge, one may send the USDT token from the Ethereum network to Minter, or BNB from BNB Smart Chain to Ethereum.

This way, Minter makes it possible to hold, transfer, and swap the majority of popular digital assets —ETH, stablecoins (USDT, USDC, and more), wrapped BTC, tokenized assets (stocks, gold, indexes, and more), DeFi tokens, and others.

You may find the list of tokens available to be transferred cross-chain here: https://explorer.minter.network/coins/cross-chain

Minter Hub is based on Cosmos SDK and maintained by 16 oracles (validators of the network) and the PoS consensus, meaning that voting on blocks is collateralized with stakes. To connect with the Ethereum and BNB Smart Chain networks, Minter Hub uses a modified Peggy solution developed by the Cosmos team.

The project's code is open-source and can be accessed in a public repository: **https://github.com/MinterTeam/minter-hub**

HUB is a token staked by Minter Hub oracles. Its main features are:

- Validation of the Minter Hub network (up to 1% on all cross-chain transfers)
- Voting on DAO-related issues
- Reduction of fees charged for making cross-chain transfers
- Provision of liquidity to the pools (0.2–0.3% on the amount swapped)

By staking HUB, validators receive up to 1% of cross-chain transfers made by users as a fee. The transaction cost can go to as low as 0.4%, provided the sender holds HUB tokens on their balance.

For more detail on HUB's use cases and its broader tokenomics, **read here**.

Liquidity Pools

A liquidity pool is a trading pair of coins/tokens with locked-up funds of liquidity providers that guarantee exchangeability. Buying or selling through a liquidity pool, a trader uses funds that have been locked into it. The process is carried out using Automated Market Maker (AMM).

Mechanism

Under the AMM mechanism, a coin or token is added into a pool when it is bought, and withdrawn from it when it is sold. AMM automatically determines the price of a token by balancing the quantities of both tokens in a given pair. There is a constant that is calculated using the following formula:

$$x * y = k$$

where x is the quantity of the first coin; y, quantity of the second coin; and k, their product. This constant represents the size of a pool and is measured in units. It cannot decrease when buy/sell deals are made within a pool. On the contrary, with each swap, it increases because of the 0.2-percent fee; the size of the pool itself increases as well. The bigger the pool gets due to the fees, the bigger earnings the liquidity providers make.

There are 3 price stages:

1. Current price (before the exchange is made)
2. Price at the time of exchange

3. Final price (after the exchange is made)

The current prices are calculated based on the total volume of coins/tokens in the pool:

$$Price\ of\ 1\ token\ A = in\text{-}pool\ volume\ of\ B\ /\ in\text{-}pool\ volume\ of\ A$$

$$Price\ of\ 1\ token\ B = in\text{-}pool\ volume\ of\ A\ /\ in\text{-}pool\ volume\ of\ B$$

For each individual swap, the price at the time of exchange depends on the current liquidity in the pool and the volume swapped. Knowing the quantity of token A bought/sold, we can calculate how many tokens B will be needed for an exchange to go through:

$$B = (K\ /\ (X - A) - Y)\ /\ (1 - Fee\ /\ 100)$$

where K is the pool's constant; X, the pool's volume expressed in token A; Y, the pool's volume expressed in token B; Fee, the commission payment (0.3%). Therefore, the price at the time of exchange:

$$Price\ A = B\ /\ A$$

$$Price\ B = A\ /\ B$$

Once swapped, tokens A bought are withdrawn from the pool:

$$X\_new = X - A$$

while tokens B sold are added into it:

$$Y\_new = Y + B$$

We may now apply the formulas mentioned above using the new pool parameters (X_new and Y_new) in order to find out the post-transaction price:

$$New\_Price\ A = Y\_new\ /\ X\_new$$

$$New\_Price\ B = X\_new\ /\ Y\_new$$

Liquidity Providers

For a trader to be able to buy and sell through a pool, that pool needs to be liquid. The liquidity is supplied by LPs who get a .2% reward on the amount swapped. These fees are automatically added into a pool, enriching it.

To supply into an existing pool, a provider needs to make a corresponding transaction sending both coins/tokens into liquidity at the same ratio (50% each). This is a basic rule that allows for keeping proportions without impacting the price. It means that by supplying, an LP increases the pool's volume, its liquidity, but does not influence the price.

If a pool that you need has not been created yet, you can create it yourself by making a corresponding transaction. For that, you just need to specify the volumes of both coins/tokens that will form initial liquidity and thus, prices.

LP Tokens

Once a provider has added liquidity into a pool, they get LP tokens—which are minted at the time of transaction—in return and their share of total liquidity in the pool is fixed. To remove liquidity, a provider needs to hold LP tokens—which will now be burned—on their balance. At the same time, the corresponding share of liquidity will return at a 50:50 ratio, depending on the current proportion of in-pool token volumes.

LP tokens are strictly tied to a pool that issued them and look like this: LP-*, where * is a numerical identifier of a pool, e.g., LP-1. The quantity of issuance is calculated using this formula:

$$\sqrt{(X * Y)}$$

To prevent some attacks that may lead to an abnormal price of minimal pool shares for minor liquidity providers, 1,000 units of LP tokens are forever “locked” upon pool creation. It is an insignificant amount for almost any pair of tokens. It substantially increases, however, the cost of an attack mentioned above.

In addition to their direct purpose, LP tokens can also be:

- Sent to any address (then receiver address will be able to claim liquidity back from the pool)
- Added into your own pools with any other coins and tokens, meaning any LP token can be freely traded on the Minter network

Such opportunities allow users to trade in shares of pools. One can both buy someone’s share of a particular pool and sell their own.

Routing

If the user needs to swap two tokens that do not have a common pool for direct exchange, the conversion can take place through a chain of pools (up to 5 tokens). This means that when token A is swapped for token E and there is a chain allowing them to “connect,” the route will look like this:

$$A \dashrightarrow B \dashrightarrow C \dashrightarrow D \dashrightarrow E$$

In the example above, token A is swapped for token E through a chain of up to 4 liquidity pools. In the meantime, for each link in the chain, pool and transaction fees will each be paid:

$$Base + (PoolsCount - 1) * Delta$$

In this formula, the base fee is summed with the multiplier based on the number of pools in the chain.

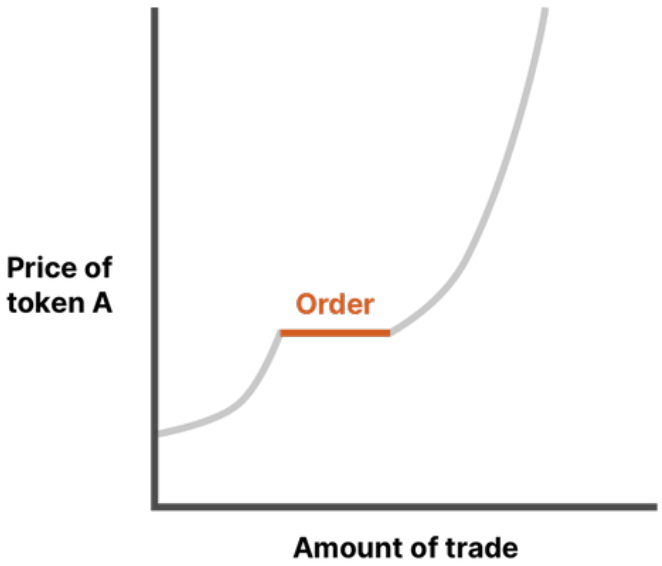
Limit Orders

Minter revolutionizes DeFi protocols with the On-Chain Automated Market Maker with Order Book (AMMOB).

Traders will be able to create fixed-price orders in the AMM liquidity pools without having to give up the benefits of those pools. AMMOB solves three major problems of traditional AMM pools:

1. Traders can buy or sell at a fixed price without giving up the liquidity benefits of AMM pools
2. AMMOB pools are suitable for exchanging stablecoins, for example, USDT for USDC. One will have an opportunity to create an order to buy $1,000,000 worth of USDT for USDC at 1% below the market and later sell it at 1% above
3. An AMMOB pool is more liquid than a traditional AMM one: in some areas, the price curve becomes a straight line

One of the features of this approach is that part of the volume may be automatically filled through a limit order, while the remaining part, via regular AMM inside the pool in question. If we visualize the price curve, it gets horizontal at the moment of the order:



All math and calculations are laid out at the core level of Minter blockchain, so there is no need to depend on any external services, while seamless and fast operations set a new bar for decentralized markets. In just ≈5 seconds (average block time), a swap can be made within a single transaction using both AMM and AMMOB (limit orders).

Let us look at how that happens. Say, a user wants to exchange BIP for USDT. First, the exchange takes place through the standard AMM algorithm using providers' liquidity. After that, part of the volume 'meets' the most profitable limit order.

To calculate the number of tokens that will trigger the execution of a limit order, let us first define the terms below:

T_0 – 1st token of the pool (BIP)
T_1 – 2nd token of the pool (USDT)
Q_0 – quantity of 1st token in the pool
Q_1 – quantity of 2nd token in the pool
Q_{0new} – quantity of 1st token in the pool after deal
Q_{1new} – quantity of 2nd token in the pool after deal
P_{limit} – price needed for a limit order

Let us take a BIP/USDT pool with a liquidity of 440 and 110 tokens, respectively. 1 BIP = 0.25 USDT. According to a limit order, BIP should be sold for the price of 0.5 USDT (at this point, we do not take volumes into account). We need to calculate how many BIPs need to be bought in order for the price to reach 0.5. Let us find T_0.

To begin with, let us find the number of USDTs we will need to spend by putting them into the pool:

$$T_1 = \sqrt{P_{limit} \times Q_0 \times Q_1} - Q_1$$
$$T_1 = \sqrt{0.5 \times 440 \times 110} - 110$$
$$T_1 \approx 45.563$$

Hence, the number of USDT tokens in the pool will now be:

$$Q_{1new} = Q_1 + T_1 = 110 + 45.563 = 155.563$$

Knowing the constant (Q_0 * Q_1), we can calculate how many BIPs will stay in the pool:

$$Q_{0new} = Q_0 \times Q_1 \,/\, (Q_1 + T_1) = 440 \times 110 \,/\, (110 + 45.563) \approx 311.128$$

Hence, the number of BIPs we need to take out from the pool is:

$$T_0 = Q_0 - Q_{0new} = 128.87$$

Checking the price:

$$155.563 \,/\, 311.128 \approx 0.5$$

The full formula that determines the number of BIP tokens needed to reach a given price:

$$T_0 = Q_0 - \frac{Q_0 \times Q_1}{\sqrt{P_{limit} \times Q_0 \times Q_1}}$$

Verifying:

$$T_0 = 440 - \frac{440 \times 110}{\sqrt{0.5 \times 440 \times 110}} \approx 128.87$$

If the deal is not filled via a limit order entirely, the remaining volume will continue to be executed through standard AMM using liquidity supplied by providers. To learn more about AMMOB, you can read this **article** and watch this **video**.

The fee for any and all swaps remains unchanged at .3%. Liquidity providers get the greater portion (.2%) of that amount regardless of whether the deal is closed using their funds or limit orders. It generates additional returns for providers, making liquidity provision more attractive.

AMMOB Fees

- $0.08 for placing an order
- $0.01 for canceling
- $0.03 for an executed market order
- 0.3% of the volume filled (0.2% is the LPs' reward while 0.1% is used towards BIP buyback)

Fees

The cost of all transactions on the network is determined by validators when +2/3 of the total voting power is in favor. Apart from the base coin, any other coin or token can be used to calculate the fee—its BIP worth will be estimated using liquidity pools built on top of AMM.

That being said, if USDC were to be picked as a fee estimation coin, it would need to have a liquidity pool in BIP, and the fee would be calculated as follows:

$$reserveBIP - (reserveUSDC * reserveBIP) / (amountUSDC * 0.998 + reserveUSDC)$$

The fees can also be paid in any coin of the network provided it has a reserve or a direct trading pair against BIP. If the coin can be swapped both ways, the blockchain will choose the most profitable direction and inform the sender about it in the tags of the processed transaction.

Rewards for validated blocks along with transaction fees are distributed among the addresses of the team, DAO, and validators who in turn further distribute them to their delegators and charge a fee declared at the start.

The exception are fees for minting coins and tokens, which are burned by being sent to the zeroth address thereby reducing BIP supply.

Validation

The Minter Blockchain is based on Tendermint, which relies on a set of validators that are responsible for committing new blocks in the blockchain. These validators participate in the consensus protocol by broadcasting votes which contain cryptographic signatures signed by each validator's private key.

Validator candidates can bond their own coins and have coins "delegated," or staked, to them by token holders. The number of delegator slots in one node = 1,000. If the stake has been squeezed out of the 1,000 slots, user's coins get waitlisted. If that happens, they will need to delegate more coins, or unbond their stake entirely, or move their stake to another validator, or wait until the minimum stake drops to the level they are comfortable with and additionally delegate any amount big enough for their stake to outnumber the one currently ranked last.

Nodes start validating if they get into a list of active validators; for that, they need to reach a certain level of aggregate stake (validator's own coins + coins others have delegated to it). The number of active validating nodes is limited by 64 slots.

The rewards validators receive are proportional to their stakes. They include fees validators charge to their delegators, which range from 1 to 100%.

Requirements

Minimal requirements for running Validator Node are:

- 4GB RAM
- 200GB SSD
- x64 2.0 GHz 4 vCPUs

SSDs are preferable for high transaction throughput.

Recommended:

- 4GB RAM
- 200GB SSD
- x64 3.4 GHz 8 vCPUs
- HSM

Fines

If the validator misbehaves, its bonded stake will be slashed along with its delegators' stakes. The severity of the punishment depends on the type of fault.

There are 2 main faults that can result in the slashing of funds of a validator and its delegators:

- **Double-signing** : If someone on chain A reports that a validator has signed two blocks at the same height on chain A and chain B, this validator will get slashed on chain A for 5% of stake (own + that of its delegators);
- **Unavailability** : If a validator's signature has not been included in 12 of the last 24 blocks, this validator will be turned off and banned for 24 hours (meaning it will not be receiving rewards).

Delegation

Delegation (bonding) is a transaction that ties user's coins to a validator. It is worth noting that the coins are not sent to the validator, but kept in the user's wallet in a locked state instead.

Unbonding is an operation reverse to delegation. When delegating, you "freeze" the coins at the validator's stake; when unbonding, you "unfreeze" them back into your wallet. Upon sending an unbond transaction, the coins become available on the user's balance once again in 518,400 blocks (~30 days)—the time during which a delegator is not receiving any rewards at all. There is also a stake transfer transaction, which is processed in around 7 days.

By delegating coins, users increase a validator's stake affecting its power within the network and receive rewards for block validation (block rewards + transaction fees). The earnings are distributed proportionally to every delegator's stake, minus the fee specified by the validator.

Unique Minter blockchain mechanisms allow users to delegate not only the base coin which is BIP, but also any other custom coin. The value of a specific amount of the coin in delegation (its BIP equivalent) is calculated differently than its price when selling or buying instantly. The formula:

$$bipValue = (reserve - CalculateSaleReturn(nonLockedSupply)) * value /$$

$$totalDelegatedValue$$

The nonLockedSupply value comprises coins in the following states: FreeFloat, Unbond, and WaitList.

Delegation Rewards

With dynamic mining introduced in Minter 3, the number of BIPs generated per block depends on the price of BIP.

For example, when the supply of coins on the market exceeds the demand, BIP's price drops. To make this less impactful, we introduce a block reward balancer that reacts by reducing block rewards when the BIP price falls, helping to avoid further BIP surplus. At the same time, when the BIP price goes up, the balancer increases the rewards to maximize staking outcome.

With dynamic mining, the block reward depends on the price of BIP. The greater the price, the greater the reward, and vice versa. There are, however, two different delegation schemes, under which delegator block rewards are reset and then accumulated until a pre-specified value is reached. A 'pre-specified value' here refers to the amount of BIP in a block. This one is re-calculated every 24 hours at a pre-determined time (12:00 p.m. UTC).

The user has an option to choose either of the delegation schemes:

- Regular delegation (no stake lock) — the reset feature enabled
- Delegation with stake lock-up period of 3 years — the reset feature disabled, rewards multiplier = x3

Under both schemes, rewards are automatically delegated, increasing stake and future rewards. If the user has a BIP stake, the rewards will be re-delegated to the same slot. If the stake is in a custom coin, an additional slot will be created for rewards in BIP from the same validator.

Regular Delegation

Regular delegation is a standard scheme, under which you can get your stake back in 518,400 blocks after unbonding. During that time, the amount withdrawn won't be generating any new rewards.

To delegators, a rule of 'one-by-one unbonds' will apply. This means that it will be impossible to make the next unbond transaction while the previous one is still in progress (518,400 blocks).

Block reward calculation formula:

$$Price\ ^{\wedge}\ (1/4) * 350,$$

where

- Price : BIP/USDTE rate
- ^ (1/4) : power function with a proper fraction. Its graph is a curve
- 350 : scale

Block Reward Reset

When block reward is reset, the number of BIPs in a block goes to 0. The reset occurs if there's a sharp, 10-percent drop in the price of BIP:

$$100 - Price\_new / Price\_old * 100,$$

where

- Price_new : self-explanatory
- Price_old : price as of the previous snapshot

Return to the pre-specified value happens if the criteria below are met:

1. The following snapshot does not record another 10-percent drop
2. Each drop-free snapshot adds 10 BIP to the block reward (for example, in order to return to the pre-specified reward of 100 BIP, you'll need 10 days with no price drops)

Burning by Balancer

When block reward is reset, the BIPs that haven't yet been distributed to the pre-specified value are burned via being sent to the 0th address. For example, if the block reward has been reset while the pre-specified value = 100 BIP, then that 100 BIP is burned. The next snapshot sees the addition of 10 BIP, the difference between that and the pre-specified 100 BIP is 90 BIP, so the 90 BIP gets burned as well.

Delegation with a 3Y Lockup

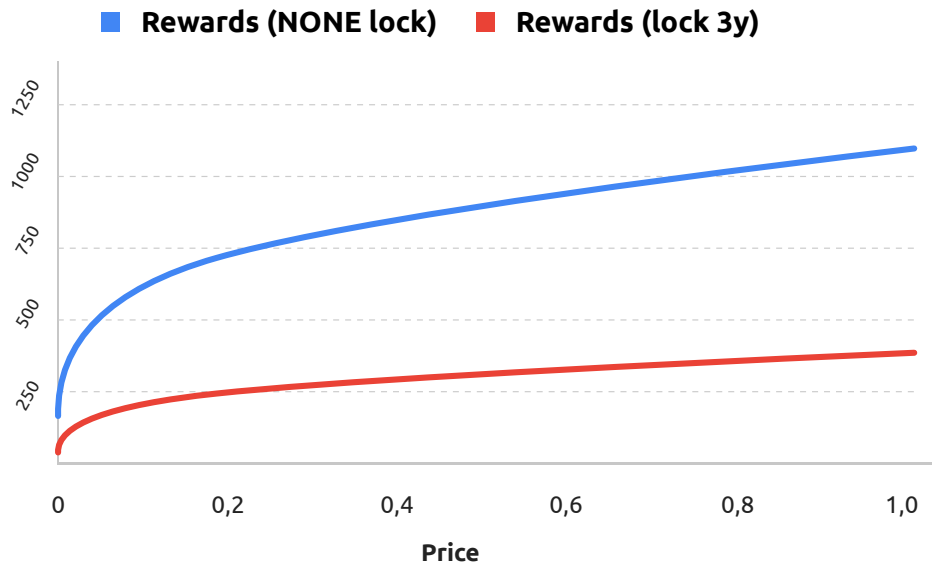
Unlike the standard scheme, the three-year lock means:

- unbond is not allowed until the period is over
- reset (i.e., accumulation of block rewards until a pre-specified value) is not allowed, hence the stake is protected against the absence of rewards
- 3x more rewards

The lock applies to the entire address.

Block reward calculation formula:

$$Price \wedge (1/4) * 350 * 3$$



On top of block rewards, validators (and by proxy, their delegators) share fees charged for every transaction made on Minter Network—except those for minting tickers, they are burned. All rewards are accumulated and proportionally (based on stake value) paid out once per 720 blocks (approximately 1 hour) to all active validators (and by proxy, their delegators) in BIP, the network's native digital coin. No separate transactions are sent for that, and the following taxes are deducted:

1. 10% to the DAO (Decentralized Autonomous Organization) fund
2. 10% to the dev team

The taxes are applied to the base amount of block rewards, and not their threefold product. The validator fees are also calculated using base rewards from stakes.

Other Features

Checks

Minter Check is like an ordinary bank check. Each user of the network can issue their own with any amount of coins and pass it to another person. The check can be redeemed by one recipient or more, they can also be time-limited (expiring on a certain block height) and password-protected.

MultiSends

A MultiSend transaction is used for sending coins to multiple addresses. MultisendData can contain only 100 items. Therefore, this type of transaction has a limit of 100 recipient addresses.

MultiSigs

A MultiSig (multi-signature) address is the one that requires several signatures for a transaction to be confirmed. ‘MultiSig’ implies that more than one user has access to the address.

To generate such an address, one has to specify two wallets or more. Each wallet is assigned its own weight, and all weights are summed in the corresponding field. ‘Threshold’ refers to a minimum value of weights necessary to send a transaction. For example, address Mx1234...5678 with the weight of 2 belongs to Alice, and address Mx8765...4321 with the weight of 1 belongs to Bob.

- if the threshold is set to 1, then both Alice and Bob can transact as they see fit;
- if the threshold is set to 2, then Alice will be able to transact, while Bob will not because his weight is less than 2. For Bob to be able to send a transaction, he will need Alice’s signature;
- if the threshold is set to 3, then neither Alice nor Bob will be able to spend funds from a MultiSig independently. They will need each other’s signature;
- if the threshold is set to 4, then no one will ever be able to manage the MultiSig. All funds sent to it will forever remain there.

Token Lock over a Specific Period

Using a special transaction, any user can lock any token on their balance for the selected number of blocks. This mechanism will be useful for project owners who, for example, want to make LP tokens unavailable for a certain period. Such lock means that the provider will not be able to withdraw liquidity from the pool during this period.

Voting Network-Wide

There are several voting situations on the Minter network. The first is automatic block consensus voting, which is governed by the core of the Tendermint engine. Another 3 are manual: for updating the network, for updating the fees, and for halting the blockchain.

Voting on Updates

With Minter’s new smooth network update algorithm without halting, hard forks have been rendered unnecessary. On the part of validators, the update takes place in several stages:

1. After a new update is released, the validator downloads it and replaces the executable file with a new one. To do this, it only needs to restart the node; that way, the network will not stop since the rest of the validators will continue to function normally;

2. The validator sends a transaction to accept the update, thereby indicating that it has updated the code base of their node to the latest version and is ready to switch the consensus algorithm at the block height which has been approved by +2/3 of the network voting power;

3. The reaching of this agreement indicates that the majority of validators are ready for the update and the blockchain will begin validation according to new algorithms starting at the block height on which all votes have been collected.

Voting on Fees

This feature allows one to monitor the relevance of fees on the network; it is also possible to peg the rate to a custom coin or token—for example, to the USD equivalent.

To perform such a vote, one needs to send a transaction from the address of the validator owner and specify their public key, coin or token for calculating the equivalent in the base BIP coin, and the values of the fields showing the price of a particular transaction and the height at which the changes will occur. The blockchain itself will change them at the specified height in case of securing +⅔ votes of the entire network capacity.