[DRAFT]
LOKA: A Bitcoin Liquid Mining Protocol That Makes Mining Financing More Accessible and The Bitcoin Network More Secure

Andy Fajar Handika
andy@lokamining.com

28 May 2024

Abstract

Loka is a new kind of protocol that strengthens the Bitcoin network by democratizing both the access and rewards of Bitcoin mining.

Currently, Bitcoin mining is controlled predominantly by centralized corporations or at least mining operations with deep pockets. One of the main reasons for this is that Bitcoin mining is capital-intensive in terms of the hardware needed and the recurring cost of paying for energy to power operations. These issues will only become more pronounced as the competition for hash rate intensifies.

Overtime, this trend can lead to consolidation of mining power and present potential chokepoints or bottlenecks to the Bitcoin Network. In fact, we are already seeing the consolidation of Bitcoin's Mining activities.

Loka solves this problem by providing a fully-collateralized win-win solution for both smaller-scale miners and investors looking to get access to bitcoin without having to pay market premiums. Best of all, is that the Loka protocol leverages the interoperability of Chain-key Bitcoin (ckBTC),[1] a 1:1 bitcoin-backed token on the Internet Computer Protocol. The resulting smart contracts make Loka composable and customizable, opening a number of interesting use cases such mining contracts that are mintable (and tradable) as non-fungible tokens (NFTs). Contract-holders can also use the contracts for things like collateral to take out loans.

Ordinary Bitcoin miners also benefit from the collateralized contract arrangement because it removes some of the volatility and risk associated with mining bitcoin and instead gives stable and consistent liquidity to manage and grow their operations.

[1] ckBTC- ckBTC is a multi-chain bitcoin twin, trustlessly created by chain-key cryptography and Internet Computer smart contracts that directly hold raw bitcoin.

Loka's architecture means that the mining contract agreements can be created and executed in a decentralized, trustless, and non-custodial way. This is different from previous attempts in the mining market to create "cloud mining" arrangements. Instead, the backbone of Loka is fully-collateralized contracts that are designed to protect both the investor and the miner, all while eliminating the need for a trusted third-party or middleman.

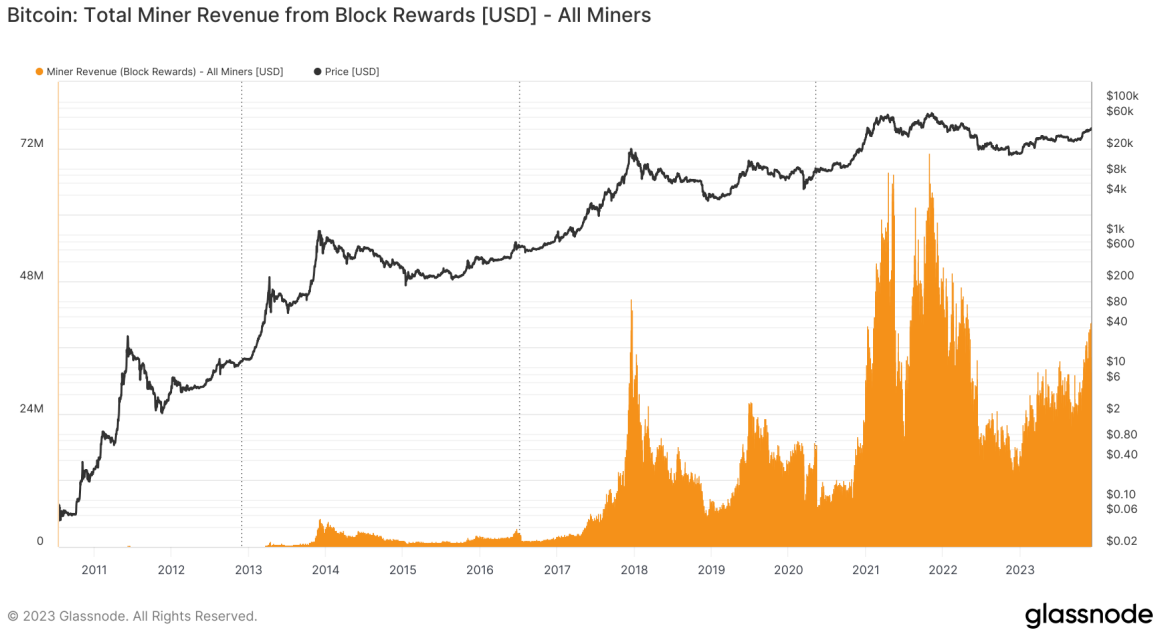
Summary

- High capital and technical requirements create entry barriers that prevent average people from entering the Bitcoin mining industry.
- On the capital side, small-to-medium-size Bitcoin miners have limited access to capital for scaling up their operations
- Cloud mining is one common alternative financing route for miners. While there are a few legitimate cloud mining companies there are also a number of scams and fraudulent actors.
- The profitability of Bitcoin mining varies from miner to miner and largely depends on different operational costs and energy expenses.

1. Introduction: Loka Solves a Growing Problem of Centralization in Bitcoin Mining

1.1. Bitcoin Mining Competitive Landscape

Bitcoin miners play a crucial role in the overall functioning, health, and resilience of the Bitcoin Network. For their efforts, which take the form of dedicated computing power, they share in over $10 billion in block rewards each year. This lucrative aspect has turned Bitcoin mining into a highly centralized, multibillion-dollar industry.



Bitcoin mining is capital intensive because it requires recurring hardware costs and recurring energy costs. Bitcoin mining uses industry-specific, highly specialized data process hardware called ASICs that require routine upgrades and replacements to stay competitive.

Additionally, Bitcoin miners also require access to electricity to run their data processing machines. The only way that Bitcoin mining is profitable in the near term is if miners move to markets and locations that are able to produce energy very cheaply in order to maintain profit margins.

The combination of hardware and energy costs means most miners have to look for outside capital to grow and sustain operations. So far, two popular options for raising money for mining operations include creating a large company, or creating a more distributed system of pooling resources such as cloud mining. To date, both options require increased centralization that can lead to issues such as too much control, or fraudulent actors (as was the case with a number of cloud miners).

Bitcoin was first envisioned as a peer-to-peer digital cash network. In order for Bitcoin to stay completely decentralized and outside of the control of a handful of corporations, the mining power (the backbone of overall network security) has to stay accessible to everyone. One way to keep Bitcoin mining permissionless is to create a mechanism to match people with the technical knowledge needed to operate a Bitcoin mine with people looking for pre-market exposure to Bitcoin.

Cloud mining is a popular method of alternative financing for miners looking to raise a lot of capital but do not want to create publicly-traded companies. Cloud mining is essentially a profit-sharing scheme between investors and Bitcoin miners and/or mining operators. This approach solves liquidity issues for miners by enabling them to scale faster or by getting their initial investment paid back upfront.

But the way that most cloud mining operations are set up also makes them easy to cover fraudulent activities. It's estimated that more than 90% of cloud mining platforms in the market are scams or fraudulent operations. There are legitimate companies, but investors are still exposed to regulation and centralized party risks.

In fact, several companies with publicly known founders and executives have turned out to be elaborate Ponzi schemes, such as Bitclub Network,[2] HashOcean,[3] Hashflare,[4] and others.[5] These platforms typically operate by asking people to invest money, promising high returns in the future, and using their perceived credibility to gain trust (essentially saying, 'just trust us').

This is where Loka comes in. But what's different about Loka compared to other distributed mining operations that have come before is that the protocol is decentralized, non-custodial, and completely permissionless.

1.2. The Economics and Profitability of Bitcoin Mining

By September 2023, it's estimated that around 10% of the total Bitcoin supply, equating to about $50 billion, is in wallets controlled by miners.

While measuring the amount of Bitcoin controlled by miners is pretty straightforward, calculating the profitability of Bitcoin mining is a bit more complex. Like any other industry, there are several factors that determine profitability.

One of the standardized methods of calculating mining profits involves using the market Hashprice Index, a function of four inputs: network difficulty[6], Bitcoin's price, block subsidy[7], and transaction fees.

Bitcoin's hashprice changes every time a new block is added to Bitcoin's blockchain. By breaking down the hash cost it's possible to determine that each miner faces different costs based on their hardware and electricity use.

The total hashprice is based on:

a. Network difficulty
b. Bitcoin price

---

[2] A Bloomberg article explaining Bitclub Network fraud charges.
[3] A Cointelegraph article about investigations into Hash Ocean.
[4] A Cointelegraph article about arrests at Hash Flare:
[5] News story about other cloud mining fraud: https://bravenewcoin.com/insights/cloud-mining-scams
[6] Network difficulty: A measure of how difficult it is to find a new block compared to the easiest it can ever be. This difficulty adjusts approximately every two weeks to ensure that the time between block discoveries remains around 10 minutes, regardless of the number of miners and their computing power.
[7] Block subsidy, also called a block reward is the amount of new bitcoins created and awarded to miners with each new block they successfully add to the blockchain. This subsidy, which started at 50 bitcoins per block, is halved approximately every four years in an event known as the "halving," reducing the rate at which new bitcoins are created and thus contributing to its scarcity.

c. Block subsidy
d. Transaction fees

The hashprice is expressed in relation to its baseline energy production, which is 1 Terrahash/day.

But to determine overall mining profitability, hashcost also needs to be calculated.

The total cost of Hash (hashcost) can be broken down into two main variables:

1. Hardware hashcost, which includes:
    a. Hardware depreciation cost
    b. Operational cost including labor costs
    c. Installation/setup cost and margin buffer, amortized
2. Energy hashcost, determined by:
    a. Hardware efficiency (J/Terrahash) of the mining machines
    b. Energy cost per kWh ($) of the energy used in the mining operations

The profitability of Bitcoin mining operations on any given day is the result of the difference between By hashprice and hashcost.

2. Key Benefits of the Loka Protocol

The Loka Protocol makes Bitcoin mining more accessible by lowering the barrier of entry for miners looking for liquidity to grow or sustain smaller-scale operations. At the same time, Loka allows more people from all over the world to participate in the running and upkeep of the truly permissionless and decentralized Bitcoin Network.

Mining contracts are at the heart of the Loka Protocol. Once created between miners, investors, and insurers, the contracts, which are minted as NFTs, can also be used for other kinds of applications within the DeFi space.

Some example use cases using the tokenized mining contracts include:

- The creation of self-paying loans using the contracts as collateral
- The creation of contract-backed Bitcoin stablecoin
- Mining contract based options trading based on bull and bear cases and outlooks

From the miner's perspective, Loka-enabled mining contracts take some of the challenge and volatility out of operating a mine, and can make it possible for miners to hold the bitcoin they produce long term while also enabling miners to meet operation costs such as equipment upgrades and ongoing energy costs.

Data shows that Bitcoin miners prefer to hold the Bitcoin they mine and sell at a profit during favorable market conditions.[8] By selling part of their hashrate, miners can create cash flow and implement more strategic financial planning.

---

[8] Data from on-chain analytics firm, Glassnode, showing the hold and sell behavior of Bitcoin miners: https://studio.glassnode.com/metrics?a=BTC&category=Miners&m=distribution.BalanceMinersSum&pScl=log&s=1383264000&u=1700672399&zoom=

Additionally, by selling hashrate using the Loka Protocol, Bitcoin miners are able to access capital efficient financing to fund or grow operations and hedge against price risk in the future.

Here are some of the main features enabled by the Loka Protocol and the Bitcoin Network:

2.1. Cross-Border Energy Markets

Loka capitalizes on regional energy cost differences and encourages energy arbitrage, enhancing global energy market efficiency. By utilizing Bitcoin's capacity as a form of 'battery,'[9] Loka optimizes energy utilization and facilitates democratized energy trading across borders.

2.2. Fully Decentralized Mining Pool

Loka offers a truly decentralized mining pool where anyone may provide liquidity to pay miners upfront on their hash rates regardless of any blocks found or not. Liquidity providers may stake their Bitcoin and get native yield from the mining pool fees. This scenario also enables miners to reduce their fees to almost zero percent.

2.3. Bitcoin Liquid Staking with Native Yield

Loka unlocked the native yield from their Bitcoin holdings by providing liquidity to miners. This real yield came from the fees of the mining pool, essentially the delta between what paid to miners and what received from the Bitcoin network.

2.4. Over-Collateralized Mining Contract

Each contract is overcollateralized with Bitcoin in a 110% ratio (more on this below) using on-chain non-custodial escrow,[10] removing centralized party risks. If miners fail to deliver the hash rate that produces Bitcoin rewards, the collateral is released to contract buyers.

2.5. Tokenized Fractional Mining Contract

By fractionalization and tokenization the Loka protocol enables trading of mining contracts like other digital assets. This means that investors can quickly and easily buy or sell Loka-powered mining contracts on secondary markets.

The liquidity of the tokenized contracts has a significant advantage, providing flexibility and ease of access that traditional mining contracts do not offer. For example, the contracts can be fractionalized, investors have the freedom to decide the amount they wish to invest in each mining contract, making it inclusive for investors of all types.

---

[9] The blog post that first outlined the concept of Bitcoin as a battery.
[10] Non-custodial escrow: refers to an arrangement where a third-party escrow service facilitates a transaction without holding the buyer's or seller's funds themselves. Instead, the transaction is secured using smart contracts or multi-signature wallets on the blockchain, ensuring that funds are only released when certain agreed-upon conditions are met, thereby reducing the need for trust between parties.

2.6. Composability

Each “mining contract” is a yield-bearing primitive asset that generates revenue and is also fully composable[11]. This unlocks a number of use cases such as:

- **Contract collateral**: The ability to borrow stablecoins against a“mining contract” and use the contract as the loan’s collateral
- **Self-repaying loans**: Borrow against BTC to purchase a “mining contract” that generates Bitcoin to repay the loan automatically.
- **Options marketplace**: Buy and sell put option premiums to protect against bitcoin price drops or earn additional rewards when the price increases during the active contract period.
- **BTC-backed stablecoins**: The ability to mint bitcoin-backed stablecoins that are over-collateralized with mining contracts.
- **Native BTC Yield:** Custodian company may offers native yield to their client by converting their BTC into mining contract, effectively enable BTC to become productive asset

2.7. Censorship Resistance

As a protocol rather than a platform, Loka operates without any form of centralized control, ensuring uninterrupted, bias-free functioning. Loka’s frontend operation is provided by a number of discrete entities, which make the system completely decentralized and resistant to censorship, while benefiting from growth incentives including earning tokens native to the Loka protocol.[12]

Frontend operators can either download the web interface provided as a launch kit or opt for creating their own custom user interface and integrate it with other services such as crypto wallets, decentralized apps, or related services, or even select only specific mining contracts that fit their own criteria to display on their interface.

3. Collateral Mechanism

One of the reasons why the Loka can exist as a first-of-its-kind tokenized hasrate protocol is because it is decentralized. Other projects have tried to offer similar products, but they are centralized, which undermines the power of permissionless digital assets and platforms.

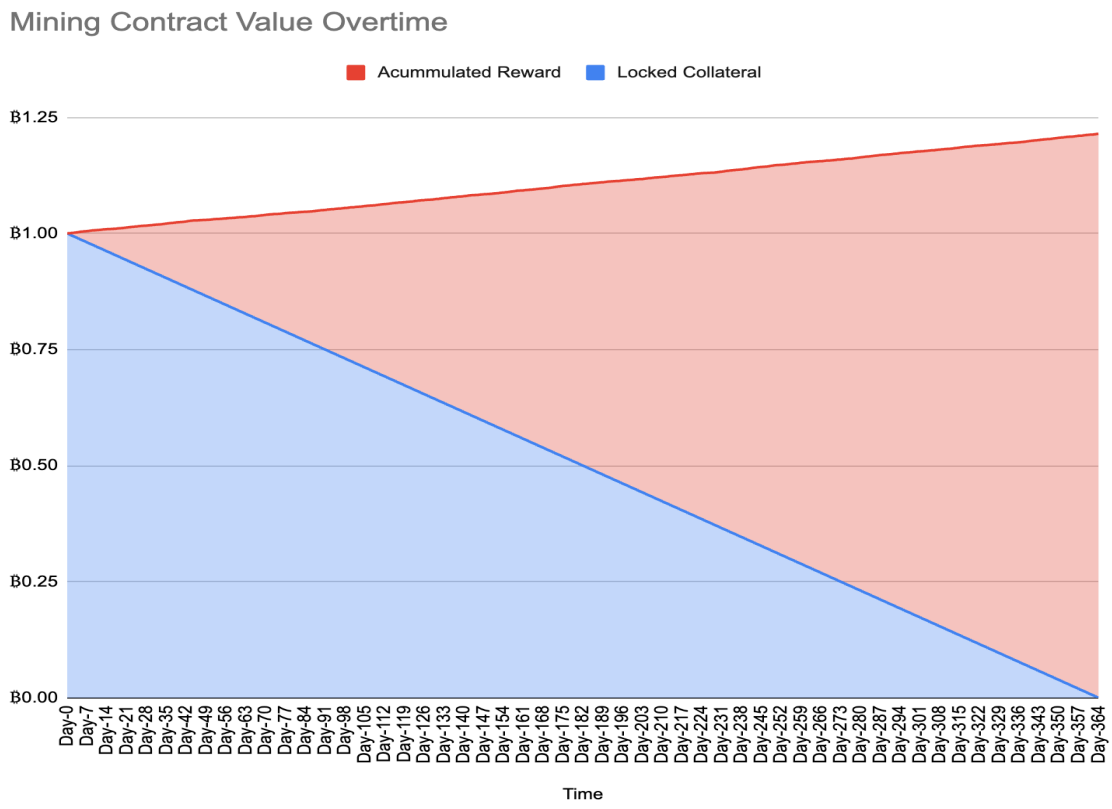
One of the main reasons that Loka can operate in a decentralized manner is because of its collateration method.The underlying principle of collateralization is simple. A mining contract will always have value in Bitcoin as well as the accruing value from mining reward over the life of the contract.

At the beginning of the term, 100% of the value is derived from the collateral locked within the contract itself. Overtime, the collateral is released back to the miner, along with a percentage of any mining rewards earned during the term of the contract. This release

[11] Composable design or composability refers to the concept of modular design and of creating elements that can work across multiple blockchain systems.
[12] Explain native tokens here and/or link to more info

happens along a predetermined timeline so that by the end of the contract, all of the collateral is paid back to the miner or insurer that provided the collateral.

Figure 1: Contract value is composed of accumulated reward & locked collateral (1-year contract)



3.1. Three-Parties Involved in Non-Custodial Escrow

There are three different roles or actors in the protocol's escrow ecosystem:

1. Bitcoin miners – The miners can range in size from small operators to larger, more complex operations. Regardless of size or sophistication, all miners sell their hash rate for upfront return on their capital expenditure. During the escrow period, miners continue to earn a percentage of the mining reward earned by their operation.
2. Investors – Like the miners, the investors can range in size and sophistication. They enter the contract with an expectation that their investment is collateralized by the miners, and that they will earn a percentage of the mining rewards during the lifetime of the contract in exchange for the use of their capital.
3. Insurers -- who provide collateral and lock their Bitcoin in return of upfront fees & share of mining reward.
   Insurers can be a group of people or individual that bear the risk of their locked capital slashed and released to investors if mining operation halts or stopped completely for whatever reason

3.2. Collateral Buffer

Loka's collateral mechanism is designed to protect both sides of a mining contract. Miners get access to liquidity to continue or grow their mining operations, while investors get access to Bitcoin mining rewards without having to pay a market premium.

Here's how the collateral system, with a built in buffer, works:

A miner and an investor enter into a mining contract. Let's say that at the time they enter the contract, the price of bitcoin is $30,000 and the investor wants to invest $3,000 into the mining contract.

The investor would deposit $3,000, and Miner (or their insurer) would also deposit 0.1 BTC (equivalent to $3,000 in USD) as collateral.

Once the contract is executed, the miner will receive 90% of the contract amount (in this case $2,700). The remaining 10% of the amount (in this case $300) is converted to ckBTC[13] and to the miner's 0.1 BTC so that now the contract has 0.11 BTC or $3,300 (equivalent to 110 % of the contract value) locked as collateral.

As explained earlier, this collateral (including the 10% coming from the investor's initial stake) is paid back linearly to the miner over the duration of the mining contract so that by the time the contract expires, the collateral is at zero.

The idea behind the collateral buffer is to prevent miners from walking away from a contract in the event that the price of bitcoin rapidly increases during the contract period. If something like that were to occur, or if there were other disruptions to the mining operation during the contract period (like changes to the energy supply, for example) and miners are no longer able to send hashrate to the Loka Protocol then investors would still get 110% of their investment back.

In order to add an extra layer of security to the life of the mining contract, there is a role for an additional party. A market could develop for contract insurers who insure the loss of the locked collateral in exchange for upfront fees, or a percentage for mining rewards, or some combination of the two.

3.3. Risk Exposures

When a mining contract created, it is essentially exchanging risks and rewards between different actors:

- Price volatility and mining difficulty that previously belonged to miners are transferred to investors along with the future mining reward, in return of upfront liquidity and profit margin from their capital expenditures.

[13] Check out footnote one for a definition of ckBTC.

- Operation risks that previously belonged to miners are transferred to insurer instead of to investor in the form of collateral, in return of upfront fees of the investment

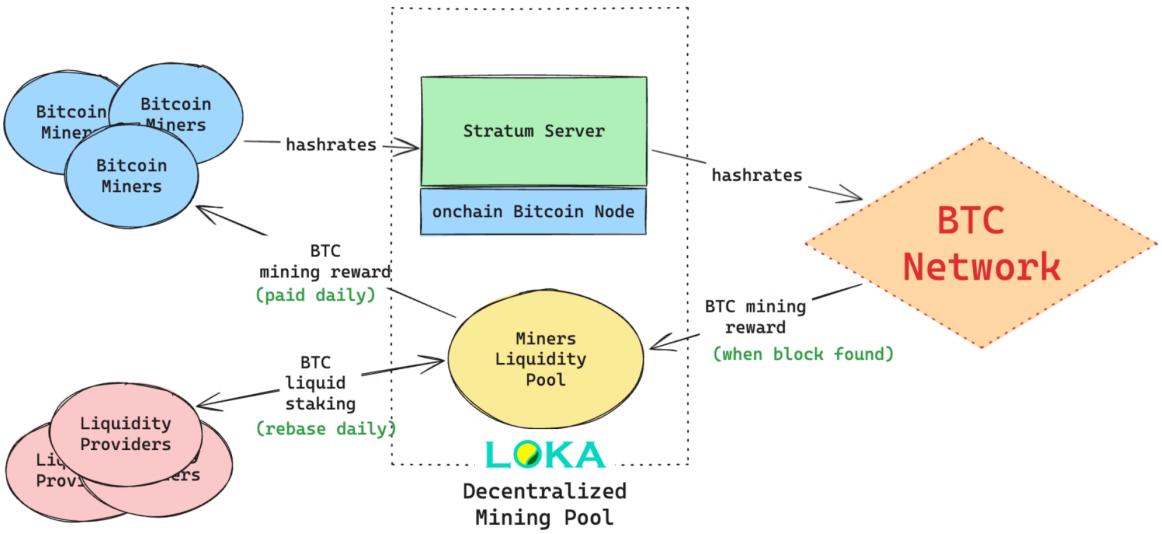
Roles / Risks & Reward	**Reward**	**Price Volatility & Mining Difficulty Risk**	**Operational Risk**
Investor/Contract Holder	Mining reward makes contract value higher than buying Bitcoin at market price	Full exposure	No exposure, worst case 110% BTC value on transaction price gets returned
Insurer/Collateral Provider	Upfront fee + % mining reward (high APY)	Limited exposure on locked collateral	Full exposure, worst scenario is complete loss of locked collateral
Bitcoin Miners	Upfront liquidity + profit margin on investment	Small exposure on the locked collateral buffer	Low exposure, if mining operation stops then the miner doesn't get any collateral buffer release.

Any individual can participate in multiple roles. For example, a miner can also act as an insurer by providing full or partial collateral of the hashrate value exposed to the mining contract. Investors can also participate as an insurer in order to maximize their mining reward and by reducing their investment capital (in the form of fees paid to an insurer) by accepting the underlying exposure of the miner's operational risk.

4. Decentralized Bitcoin Mining Pool Architecture

Mining pools convert lottery mechanisms in Bitcoin mining into pro-rata distribution of mining rewards based on miners' hashrate contributions. Since not every day a mining pool finds a new block, they need liquidity to pay miners upfront even though there's no block found on that day.

Loka's mining pool is decentralizing the liquidity, by enabling retail investors to put their BTC to work and earn native yield from the mining pool fees.



4.1. Stratum Server

This server will receive hashrates from Bitcoin miners and determine the contribution from all miners in the mining pool. No login required.

4.2. Miner Liquidity Pool (MLP)

This is where Bitcoin miners get their daily payment from. Volume of the MLP grows and shrinks according to events that occur in the Mining Pool.

Events	**Effect on Volume**
Liquidity added	increase
Daily payout to miners	decrease
New block found; get coinbase reward + tx fees	increase
Liquidity removed	decrease

4.3. BTC Liquid Staking with rebase mechanism

When Liquidity Providers stake their Bitcoin in the form of ckBTC, they will receive lokBTC, an IOU token that is 1:1 value to the ckBTC.

The total lokBTC supply is mirrored with the Total value locked of ckBTC in the Miner LIquidity Pool and rebased every 24 hours.

5. Forward Hashrate Platform System Architecture

The permissionless and non-custodial elements of the Loka Protocol make it a novel approach to increasing access and diversity in the Bitcoin Mining space.

It's important to note that eventually, Loka will be interoperable with more blockchains, while the infrastructure is built on Internet Computer Protocol (ICP).

The following is a breakdown of the protocol's architecture, including key elements and how they work:

5.1. Stash

Stash is a contract opened by miners that offers their future hashrate from their mining machines by first defining these variables:

- The maturity date or expiration date of when the contract will expire
- Total hash rate to lease in Terrahash/s
- Stash Hashprice per Terrahash in $

Each stash will have default parameters that determine the net profitability for prospective contract buyers/investors, but miners can set their custom parameters, such as:

- The percentage of collateral fee to be paid to the contract insurer
- The transaction fee paid to the insurer

Every 24 hours, the price of total stash will decrease linearly as the mining reward is paid out according to the contract's predetermined schedule.

5.2. Stash Collateral Pool (SCP)

The SCP is an individual pool for each Stash. This is where Insurers (often Miners themselves) store the bitcoin collateral to match the Stash price offer, which is held by the other side of the contract.

The SCP acts as a constraint for the value of the contract because the minted contract can not exceed the value of the 1:1 collateral of the SCP.

When a contract is minted, the same value from the SCP will be locked in a smart contract, and insurers will be immediately rewarded with the predetermined insurer transaction fee.

Every day, (1/remaining days x locked collateral) part of the collateral will be unlocked and released back into the SCP, along with the collateral fee that was set by miners and outlined in the terms of the contract.

If total value in SCP exceeds the total Stash value, the fees will be distributed proportionally.

5.3. Trove

Trove is the tokenized mining contract minted by the investor from available and collateralised Stash, essentially a fractional Stash that can be purchased by an investor.

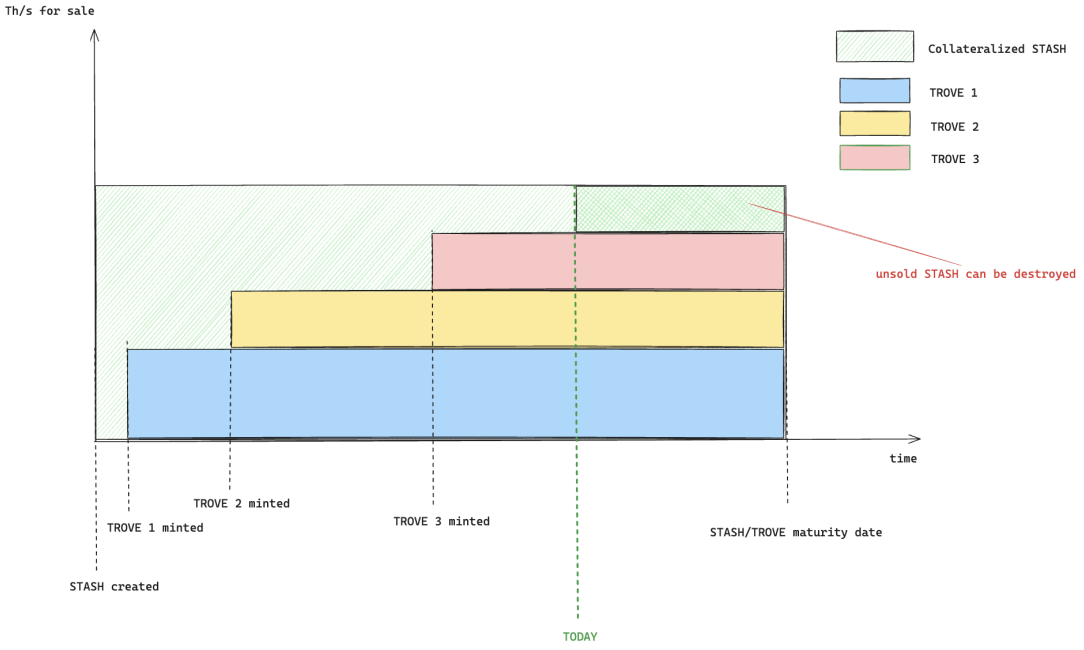
Since Loka allows for fractionalized contract creation, each investor can determine the portion of the Stash they want to mint at will.

All Troves that came from the same Stash will have the same maturity date even though they are minted on a different date.

5.4. Relationship between Stash, SCP, and Trove

Elements	Roles/Actors	Action
Stash	Miners	Create Stash from available hashrate
Stash Collateral Pool	Insurers	Put BTC as collateral to Stash into the associated SCP
Trove	Investors	Mint Trove from available Stash that is already collateralized

Figure 2: Stash & Trove relationship



Stash Creation

Stash can only be created by miners from their available hashrate (defined as hashrate received by the protocol 24 hours in advance of the contract creation).

Trove Minting

Trove can only be minted from collateralized Stash. In the event of a Stash that is not fully collateralized, the maximum value of Trove that can be minted is the same as the value of collateral.

When a Trove is minted, the total transaction value minus fees and collateral buffer will be transferred immediately to the associated Miner.

There's no maximum number of Troves per Stash. Investors can mint Trove in fraction of the Stash, as long as the amount doesn't exceed the available collateral.

Stash Destruction

Since the value of each Stash is decreases by T/h day, miners can destroy portions of unused and unminted Stash
This allows miners to create a new Stash from the available hashrate with a new price, which helps them stay price competitive relative to other miners.

5.5. Hashrate Oracle

The protocol reads the native hashrate sent from the miner to Loka's mining pool.The data will be used as an oracle to determine the ongoing contract outcome.

5.6. Reward payout and collateral release mechanism

Mining reward payout and collateral release occurs every 24 hours.

There are two possible payout scenarios:

a. The miner produced hashrate within or over the contract's threshold during the last 24 hours:
    - 1/(Trove days to maturity) of collateral will be released to the insurer
    - 1/(Trove days to maturity) of collateral buffer will be released to miner
    - 24hr mining reward will be distributed to Trove holders after fee to miner, insurer and the protocol.

b. The miner produced less hashrate than the contract's threshold during the last 24hr:
    - 1/(Trove days to maturity) of collateral + collateral buffer will be released to the Trove holder, essentially 110% of the day contract value.
    - The 24-hour mining reward will be distributed back to miner after fee to insurer and protocol

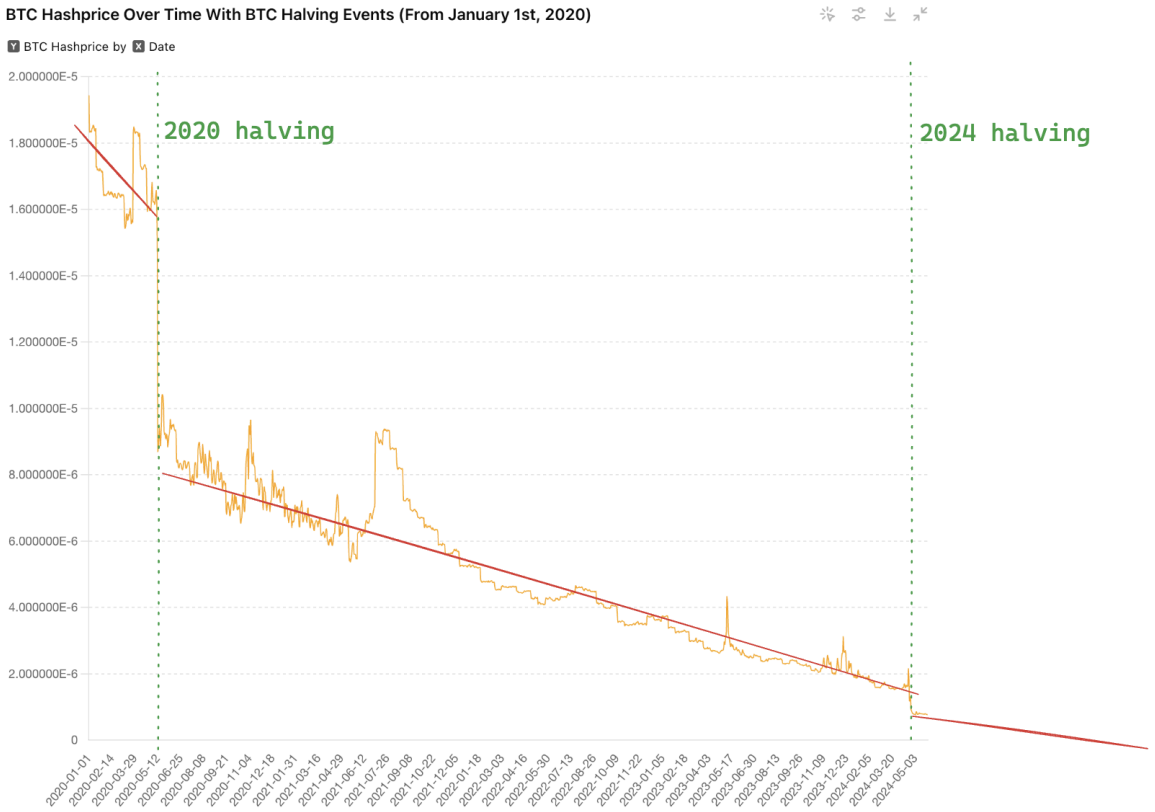
6. Contract Profitability

From the perspective of investors, buying a forward hashrate contract is similar to purchasing Bitcoin at lower than market price, considering for certain aspects:

6.1. Hashprice Projectability

Luxor coined the term of hashprice, which is a function of network difficulty and mining reward per Terra/hash per day. Due to Moore's law that dictates that hardware price tends to decline, this means that the total hashrates contributing to the Bitcoin network that positively correlates network difficulty also tends to increase.

Figure 3: Hashprice Projectability



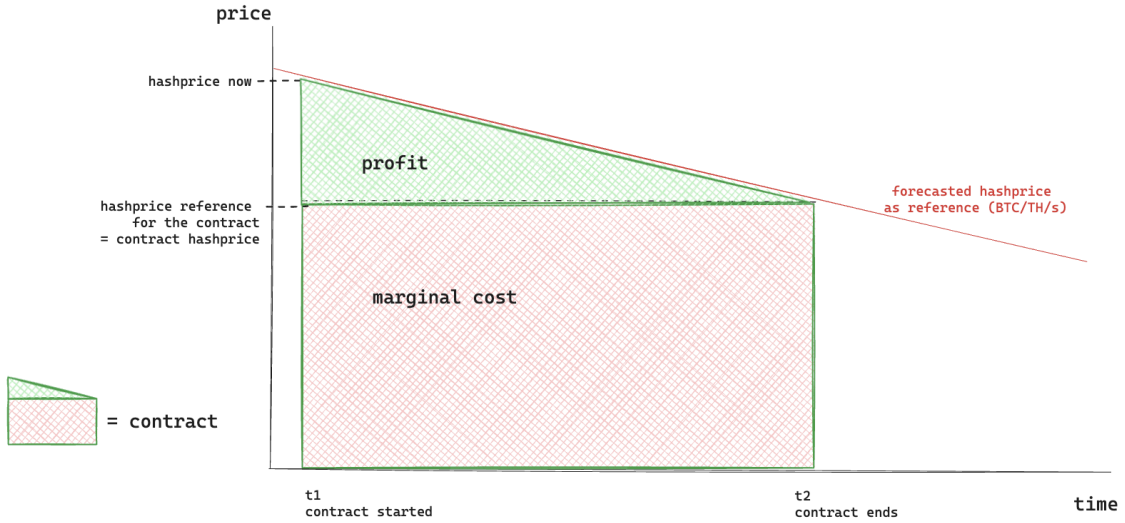
This means that hashprice is always decreasing overtime with predictable rates in between each halvings. The projected hashrate is used by the protocol as the main reference for parties to determine the hashprice of the contract.

6.2. Forward Contract Price & Profitability

When miners use the forecasted hashprice at maturity date to set the contract price, the investor pays for the total amount of hashprice x contract days x hashrate quantity.

The delta between current hashprice and the agreed hashprice are the widest on the first day of the contract, and keep decreasing until it touches on the maturity date – provided if the forecast is 100% accurate.

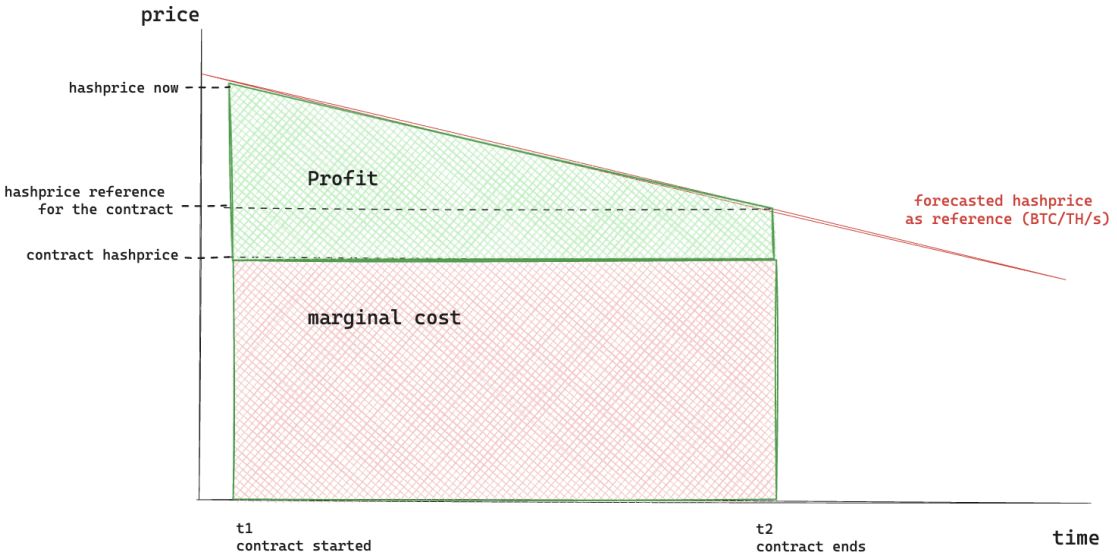
The investor profit is represented by the green triangle.



Since the price is determined by the elasticity of the supply-demand and the dynamic of actual hashprice, profitability will be different on each different contract price:

A. Contract Hashprice < Forecasted Hashprice at Maturity

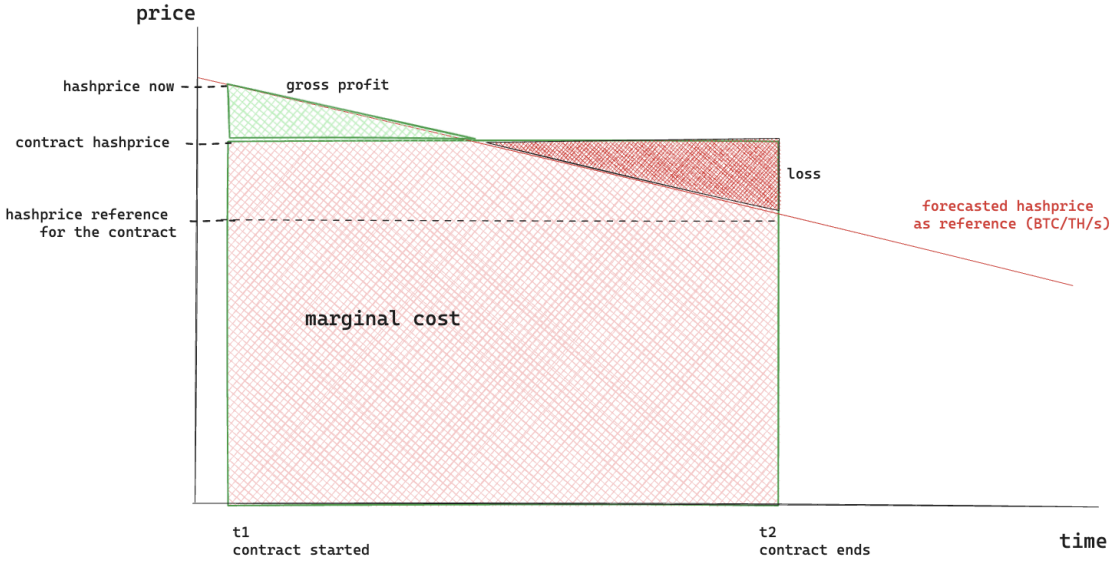
When hashprice on contract maturity is less than the actual hashprice (provided if the forecast is 100% accurate), the profitability area is wider because the investor's marginal cost is smaller.



B. Contract Hashprice > Forecasted Hashprice at Maturity

When hashprice on contract maturity is higher than the actual hashprice (provided if the forecast is 100% accurate), investors are profitable at the beginning of the contract, but will bear loss after the actual hashprice declines below the contract hashprice.

The actual profit is the delta between loss at the end and (gross) profit at the beginning of the contract.



7. General Flow

To summarize each actor's roles and responsibilities within in the protocol ecosystem:

7.1. Miner

The flow starts with Miners opening a Stash with corresponding collateral pool. The protocol will suggest the forecasted hashprice on the maturity date based on the historical price and performance as the default hashprice of the Stash. Miner can adjust this price accordingly.

When a Trove is minted from this Stash, this will trigger the protocol to start activating the contract and Trove will start receiving the mining reward according to the contract parameters.

7.2. Collateral Provider

Collateral provider(s) put money in the Stash collateral pool, and became insurers.

If collateral pool value > total hash rate price, then fees, and rewards will be paid on a pro rata based on percentage of pool share at the moment when the contract minted.

7.3. Investor

One feature of the Loka Protocol is the ability to fractionalize the hashrate provided by Miners in the Stash which enables investors to purchase only a fraction of the hashrate available in the form of Trove.

Investors mint the Trove from available Stash and become Trove holders by paying dollars in stablecoin or equal denominations.

When a Trove is minted, miners will instantly get the liquidity, minus the fee to the insurer and protocol.

7.4. Ongoing contract

The protocol releases mining rewards and collateral every 24 hrs until Trove expires.

8. ICP & ckBTC

Loka protocol is built on the ICP network.

8.1. Why ICP?

The Loka Protocol is strategically built on the Internet Computer Protocol (ICP) network for several key reasons:

- Decentralization and security
  ICP provides a robust and decentralized infrastructure, which is essential for maintaining the security and integrity of Loka's operations as it will be transitioning into DAO in the near future
- Scalability
  ICP's architecture is designed to handle large-scale computations and data storage efficiently, making it an ideal platform for Loka's expansive data and transaction requirements.
- Interoperability & Gasless Transaction
  With ICP, Loka can seamlessly interact with other blockchain networks and technologies, enhancing its functionality and user experience. Users can just use BTC for transaction fee, without having to fund their wallet with ICP native token.
- Technology
  Only ICP is able to control BTC addresses which no human will ever get access to using smart contracts. ICP has the ability to be a decentralized BTC wallet custodian.

8.2. Why ckBTC?

ckBTC is a multi-chain bitcoin twin, trustlessly created by chain-key cryptography and Internet Computer smart contracts that directly hold raw bitcoin. ckBTC can be transferred with 1-2 second finality and negligible fees. No bridge, no intermediaries, and completely non-custodial.

This is crucial for Loka in order to deliver the mining reward and to be fully decentralized.

The private keys for the native Bitcoin address are held by the tECDSA subnet (29 nodes on ICP). Each node has a private key share. Together, they do a threshold signature to enable the movement of Bitcoin.

The private key shares are rotated every 10 hours-(ish) and the protocol handles the key rotations/distribution.The protocol also handles which nodes are assigned to the tECDSA subnet, and the protocol can add/remove nodes as needed.

The IC protocol reads the balance in the deposit address using the Bitcoin light node on chain on ICP, and then mints ckBTC to the designated address on ICP side.

Unwrapping back to native BTC is as simple as sending your ckBTC back to the smart contract, and then it initiates a Bitcoin transaction back to a destination address of your choosing. The smart contract handles all of the UTXO management needed, and generally batches unwrap transactions every five to ten minutes.

To convert BTC to ckBTC it takes 13 confirmations (2 hours) and to convert back to native BTC takes five to ten minutes until the transaction out hits the mempool.

9. Challenges and Roadmap

We acknowledge that there are some challenges for this protocol that we need to tackle:

9.1. Mining pool: Centralized Weak Link

A mining pool is required to convert lottery mechanisms to pro-rata share distribution of mining reward on their hashrate.

But mining pools as an entity have exposure to centralized party risk such as liquidity crisis[14] and the centralization of the mining hashrate[15] as well.

To achieve a truly decentralized and trustless bitcoin mining protocol; a top priority for the Loka Protocol will be to build an open source mining pool that is run by the community and has their own incentive mechanism.

The Challenge: Market Size Feasibility

Due to the nature of the mining pool, we need a certain scale of hashrate contributed from the miners as the participants. To reach an ideal 90%+ possibility of getting block reward every day, a mining pool needs to aggregate at least 0.7% of the total hashrate in the world.

[14] About the liquidity challenges facing mining pools.
[15] Dangers of the centralization of the Bitcoin mining hashrate.

Approach to the Challenge: Building in Phases

Instead of immediately building a Bitcoin mining pool, we jumpstart the go to market strategy with a mining pool aggregator where we redirect the miners hashrates to existing mining pools. Miners can connect to our stratum server and earn extra reward tokens on top of their Bitcoin reward.

Once we accumulate 0.1% total hashrates, we will immediately switch to send hash rates directly to the Bitcoin network.

9.2. Two-sided Protocol: Cold Start Problem

As a two-sided protocol, Loka requires active participation from both Bitcoin miners and investors to operate effectively. This cold start problem is a common challenge for two-sided networks, where both sides—supply (miners) and demand (investors)—must be engaged early on to create a functional ecosystem. Without sufficient participants on both sides, the protocol risks low liquidity, insufficient rewards, and a lack of user confidence.

The Challenges: Initial Adoption

- Attracting Miners
  Miners are essential to providing hash rate liquidity, but they may be hesitant to join a new platform without demonstrated benefits or investor interest. Miners need reassurance that their hash rate contributions will yield consistent returns, especially if they're already committed to established mining pools.
- Engaging Investors
  Investors are needed to provide capital by purchasing mining contracts, but they may hesitate to invest without an established track record or active miner participation. Investors need confidence in the security, reliability, and profitability of the contracts available on Loka.

Approach to the Challenges:

Incentive Programs Using MPTS and LPTS

- Initial Reward Boosts for Miners
  Miners will receive Miner Points (MPTS) in addition to their regular mining rewards. These MPTS are granted as additional compensation to early miners, building their interest in the protocol from the start.
- Reward Boosts for Liquidity Providers
  Liquidity providers who stake their BTC to the Protocol will earn Liquidity Provider Points (LPTS). LPTS are distributed as a reward for providing initial liquidity, incentivizing early participation in the protocol's growth.

Airdrop Allocation of $LKMN:

- Both MPTS and LPTS will be used to calculate early participants' allocations in the initial airdrop of $LKMN tokens. These points will represent the contributions of miners and liquidity providers to Loka during its early stages, ensuring that those who support the protocol's launch are rewarded with a proportionate stake in $LKMN governance.
- 1:1 MPTS to LPTS Ratio
  The points system is balanced to reward miners and liquidity providers equally. This 1:1 ratio reinforces the importance of both sides and fairly represents each participant's contribution to the protocol.

Building Network Effects

- Positive Feedback Loop
  Once a critical mass of miners and liquidity providers is reached, the protocol can achieve a self-sustaining cycle: more miners increase hash rate availability, which attracts more liquidity providers seeking returns, which in turn attracts additional miners. This feedback loop strengthens the protocol's liquidity, rewards, and user base.
- Continuous Rewards for Early Participants
  Recognize and incentivize early participants by rewarding MPTS and LPTS through periodic bonuses or additional governance privileges within the DAO. This encourages loyalty among initial miners and liquidity providers, ensuring their sustained engagement as the protocol grows.

By addressing the cold start problem with MPTS and LPTS incentives, initial reward boosts, and balanced rewards distribution, Loka can overcome the early adoption barriers of a two-sided protocol. Establishing trust and engagement from both miners and liquidity providers will be essential to building a resilient, decentralized ecosystem.

10. SNS: Path to Decentralization

The Loka Protocol will gradually shift control from its core team to a decentralized autonomous organization (DAO), empowering the community to participate in governance and drive the protocol's evolution.

Through the Service Nervous System (SNS), Loka will implement a neuron mechanism for time-weighted governance and reward distribution, enabling a secure and community-driven framework. This transition will begin with an SNS sale, allowing participants to acquire $LKMN tokens and establish an initial governance community.

10.1. SNS Sale to Launch Community Governance

- Purpose of the SNS Sale: The SNS sale will allow the community to acquire $LKMN tokens directly, fostering broad token distribution and empowering early supporters to become active participants in governance.
- Token Distribution: The SNS sale will allocate a percentage of $LKMN tokens to participants, creating an initial base of neuron holders and incentivizing active engagement from day one. A portion of tokens may also be reserved for future community initiatives, partnerships, and rewards.
- Fund Allocation: Proceeds from the SNS sale will be allocated to the protocol treasury, funding early development, marketing, and strategic growth. Governance over treasury spending will be managed by $LKMN holders through the neuron system, ensuring that funds are used transparently and align with community priorities.

10.2. Neuron Mechanism for Governance and Rewards

- Neuron Creation
  $LKMN holders can create neurons by locking their tokens in the protocol for a chosen duration. Each neuron represents locked tokens, granting the holder voting power and rewards based on the amount and lock duration.
- Time-Weighted Voting Power
  The voting power of a neuron is determined by a combination of the staked $LKMN amount and the lock duration. This time-weighted model encourages long-term alignment with the protocol's goals, as longer lock periods yield higher voting influence.
- Rewards for Neurons:
  Neurons are eligible for protocol rewards, distributed based on time-weighted voting power. This means that users who lock tokens for longer periods not only have a greater say in governance but also receive a larger share of protocol-generated fees.

10.3. Proposal and Voting Process

- Proposal Creation
  Neuron holders can submit proposals, enabling them to directly influence protocol decisions such as fee structures, treasury allocations, or feature upgrades. Proposals are available for voting by all neurons.
- Voting with Neurons
  Each neuron's vote is weighted according to its voting power, derived from both the locked $LKMN amount and lock duration. The voting process is transparent and on-chain, ensuring a fair decision-making process.
- Cooldown and Neuron Dissolution
  Neurons can be dissolved, returning locked $LKMN to the user after a cooldown period. However, dissolving a neuron immediately reduces its voting power and eligibility for rewards, ensuring stability and preventing abrupt governance changes.

10.4. Decentralized Treasury Management

- Community-Controlled Treasury
  Fees generated from protocol activities are held in a community-managed treasury, which can fund development, marketing, and strategic partnerships. Neurons allow token holders to vote on how funds are allocated, ensuring that treasury spending aligns with community interests.
- Sustainable Treasury Growth
  With a portion of protocol fees regularly added to the treasury, the DAO can continually invest in Loka's expansion and improvement, enhancing the long-term sustainability of the ecosystem.

10.5. Neuron Maturity and Compounding Rewards

- Neuron Maturity
  Neurons accrue rewards over time and reach a "maturity" threshold. Once mature, rewards can either be claimed or reinvested to compound voting power and further increase potential rewards.
- Reward Compounding
  Neuron holders may choose to reinvest their rewards back into their neuron, which increases both its maturity and future voting power. This compounding option incentivizes continuous reinvestment, fostering a loyal and committed governance community.

10.6. Transition Phases to Full Decentralization

- Phase 1
  Core Team Oversight: Initially, the core team will guide Loka's governance, with community members influencing specific proposals. This approach ensures a stable foundation for SNS governance.
- Phase 2
  Mixed Governance: As the community becomes more active and governance stabilizes, $LKMN neuron holders will take greater control, while the core team assumes a support role.
- Phase 3
  Full Community Governance: The final phase sees all governance responsibilities transitioned to the DAO. Neurons will fully control protocol decisions, and the core team will no longer have special privileges, achieving complete decentralization.