Lightstreams Governance v0.1

Table of Contents

Introduction

Lightstreams is a blockchain network for building a new generation of applications. Our goal is to transform the way people collaborate with applications that put people in control of their data, money and assets. This document forms the first version of the governance model is open for consultation and will form the basis for the constitution of the network as specified in the Lightstreams White Paper.

At the heart of any Lightstreams application is a system of interconnected smart contracts that control the flow of information between individuals, groups and other applications. Lightstreams' design separates program execution and data storage by hosting smart contracts on an Ethereum-based blockchain and application data on a peer-to-peer storage layer called the Smart Vault.

Lightstreams enhances smart contract write-action behavior with fast confirmation times. Fast confirmation times of smart contract transactions are a crucial factor needed during the saving of application state information so that the user experience feels responsive. For example, Bob purchases a coffee from Alice's store using a Lightstreams app. Alice should immediately receive a confirmation message on her app after Bob clicks the pay on his app.

Today, adoption of peer-to-peer, blockchain-based applications has been limited. Technical limitations have contributed to a lack of adoption including scalability issues, lack of user-friendly key management infrastructure, and upfront transaction costs. Structural weaknesses in the areas of anonymity, immutability and governance are also calling into question the long term sustainability of blockchain networks.

Lightstreams' governance model attempts to address these challenges via its Delegated Proof of Authority (DPoA) consensus and Smart Vault technologies. DPoA consensus include fast transaction throughput, short confirmation times, no user fees and collective governance, while the Smart Vault provides off-chain, peer-to-peer storage where users are always in control of their data.

Background

Smart contracts are immutable computer programs that are the basis for running Lightstreams applications known as Decentralised Applications (DApps). Lightstreams is designed to support Ethereum-based smart contracts that are written in the Solidity computer language, enabling applications to be cross-compatible between Ethereum and Lightstreams. Currently, Solidity has the greatest developer community, software tools and libraries to support the development of DApps.

A defining behaviour of a DApp is that each peer in the network must be able to run the same smart contract program to reproduce the same result with the same inputs. For this reason, both the smart contract and the input data are broadcast as immutable blocks of data between to every peer in the network. To coordinate agreement between peers on the order and correct state of blocks, a consensus protocol is needed.

Until now, Proof-of-Work (PoW) has been the leading blockchain consensus protocol, which is currently the consensus protocol of the Ethereum network. A replacement for PoW is needed due to the following issues:

- **Slow** (low tx throughput). Ethereum can process approximately 24 tps (~380 tx per block at a block time of 16 secs) versus the Visa network that can process 2,000 tps.
- **No guaranteed finality**. Users are recommended to wait at least 6 blocks (96 secs) for a transaction to be accepted, however, the transaction is never 100% confirmed.
- **Responsiveness.** The user experience of DApps can feel sluggish due to low network throughput and long confirmation times.
- **Upfront fees.** Users need to have a positive digital wallet balance before they can use a DApp. Today, consumers expect to use applications for free before making a choice to purchase.
- **Environmental**. Validation of transactions (aka mining) by peers in the network consumes energy that is unsustainable in the long term. It is estimated that tonnes of CO^2 are produced annually for powering blockchain mining operations.

Along with these technical issues, blockchain networks also suffer from various structural issues. Current networks are not designed to gather feedback from the individual users of the network. Most are based on anonymity and pseudonymity

accounts; there is no notion of an individual person's identity within the system. This often means that controversial decisions are decided in favour of the largest stakeholders of the network that may not be aligned with the users of the network. For example, miners, mining pools and exchanges can hold a significant amount of cryptocurrency in their digital wallets and can greatly influence the decisions of network upgrades.

A sustainable peer-to-peer network requires that the peers operate independently to one another and have a certain amount of equality between them. To achieve this end, we believe that designed into the network must be a feedback loop where the users and applications can participate in the design and behaviour of the network.

Overview

The following is a brief overview of the Lightstreams governance model.

1. **Authority node**. A node can operate as an *Authority* node provided they hold or rent a *Licence* and is a member of the *Approved Validator List*.
    a. An Authority node can hold or rent only one Licence.
    b. To become a member of the Approved Validator List, a node must:
        i. Complete a security audit by an approved *Security Auditor*; and
        ii. Be voted onto the Approved Validator List by a majority of *Delegators*.

2. **Validator Bond**. A bond must be deposited by an Authority node into a Validator Bond smart contract
    a. An Authority node must deposit a bond into a Validator Bond smart contract.
    b. The bond will be released when each Licence is assigned to a new holder. There is an unbonding waiting time period from the time a Licence is reassigned to when the bond is released. The unbonding time mitigates long-range attacks
    c. Any penalties will be subtracted from the bond and transferred to the Foundation. The Authority node will be required to top up their bond balance when a penalty is charged.
    d. An Authority node will be dismissed from the Validator Set for malicious actions. In this situation the entire bond will be transferred to the Foundation.

e. The Validator Bond will be equal the Valuation Price of the Licence that an Authority node holds.

3. **Licence Owner**.
    a. New Licences will be issued via an auction process.
    b. A Licence Owner must publish a *Valuation Price* for the Licence they hold.
    c. A Licence Owner will pay a periodic *Foundation Fee* based on the Valuation Price.
    d. After the auction process, a Licence can change owners when a buyer places a bid price higher than the *Valuation Price*. The difference between the bid price and the Valuation Price must be at least 5% of the previous Valuation Price. The owner will have a *Counter Bid Time* to provide a higher counterbid to avoid losing the Licence. If they do not provide a Counter Bid, the buyer pays the owner the bid amount and the Licence transfers.
    e. When a Licence changes owner, there will be a period (a suggested 3 - 6 months) when new buyers cannot bid for the same Licence.
    f. Licence Owners can rent their Licence to Authority nodes for a rental period (from 3 to 12 months). After the rental period the Licence is automatically returned to the owner.
    g. If the Licence changes owners during the rental period then the rental agreement terms remain the same.

4. **Block production**.
    a. Blocks are created by Authority nodes validating transactions and grouping them into proposed blocks.
    b. An Authority node will collect the transaction gas fees for validating transactions.
    c. Each Authority node will have a turn to propose a new block in a round robin schedule.
    d. Proposed blocks will be verified and voted on by other Authority nodes in the Validator Set.
    e. Each Authority node will have equal voting power.
    f. An Authority node will receive a *Block Reward* for producing blocks. The Block Reward will be an amount in PHT defined by the Foundation.

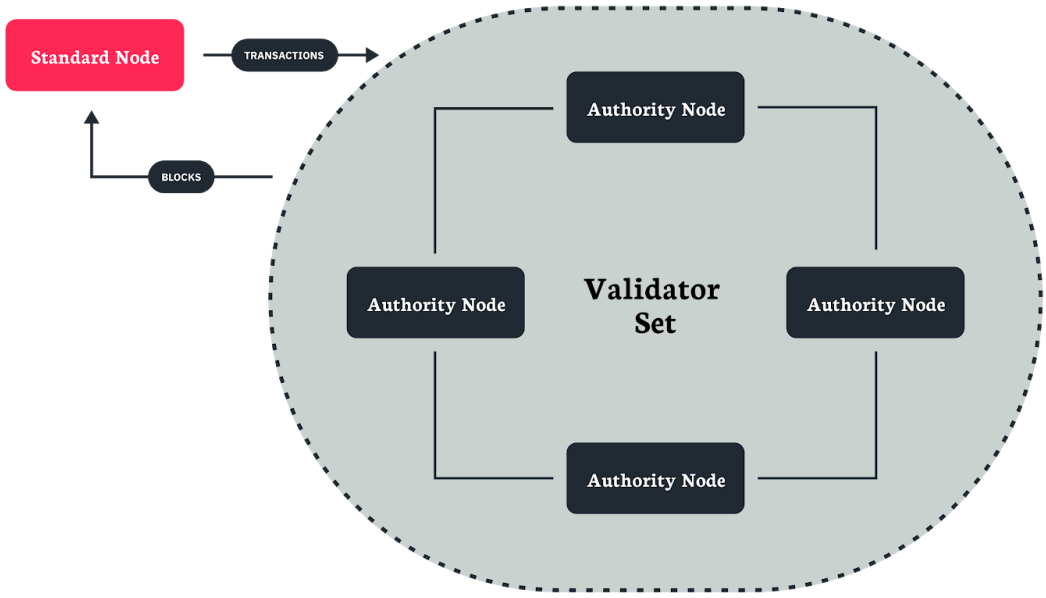
5. **No User Fees**. To enable freemium usage models, application creators can bear the costs of running their applications instead of their users. How this would work:

a. Applications pre-fund a smart contract to reserve funds for processing application-specific transactions.
b. A user sends an application-specific transaction to an Authority node with no transaction fees.
c. An Authority node will deduct the required transaction fees form the pre-funded smart contract and process the transaction.

6. **Network Upgrades**. The Network Protocol is upgraded through a Protocol Upgrade process.
    a. A *Lightstreams Improvement Proposal (LIP)* is submitted by any *Verified Account*.
    b. The proposal is voted upon by Verified Accounts using a Quadratic Voting procedure as follows.
    c. Development is completed, reviewed and tested.
    d. Authority nodes upgrade to the new version of the protocol software.

7. **Delegator**. A Delegator role is to vote on behalf of other users who have delegated their votes.
    a. A Delegator partakes in voting on nodes that have been nominated to become Authority nodes.
    b. A Delegator partakes in voting for LIPs.
    c. A User can assign their votes to another Delegator at any time.

Authority Nodes

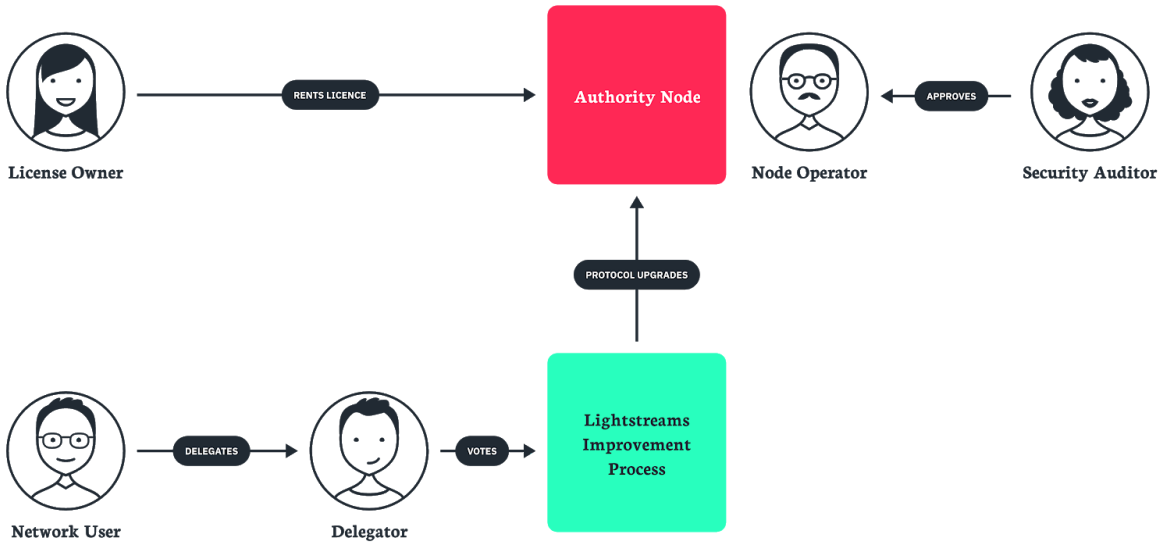


Lightstreams DPOA Consensus

Lightstreams' Delegated Proof of Authority (DPoA) is a consensus protocol with a limit on the number of nodes authorised to propose and vote on blocks. These nodes are called Authority nodes and form an independent and decentralised group called the Validator Set. Authority nodes in the Validator Set vote on blocks proposed by other Authority nodes. When a supermajority (⅔) agrees on the validity of a proposed block, this block is finalised and becomes part of the Lightstreams blockchain.

Note: In the formative phase of network post Go-Live, Authority Nodes will be operated by the Lightstreams team. There will be a gradual roll-out to partners for

inclusion in the initial Validator Set.



Actors in Lightstreams Governance Model

In order for a node to become an Authority node they must hold a Licence and be a member of the Approved Authority List. The amount of income an Authority node can generate depends on the number of Licences that they hold. To be a member of the Approved Authority List, a node must complete an approved security audit by an approved Security Auditor and pass a vote by a majority of Delegators.

Note: Delegators and Security Auditors will initially be selected by the Lightstreams Foundation.

Licences

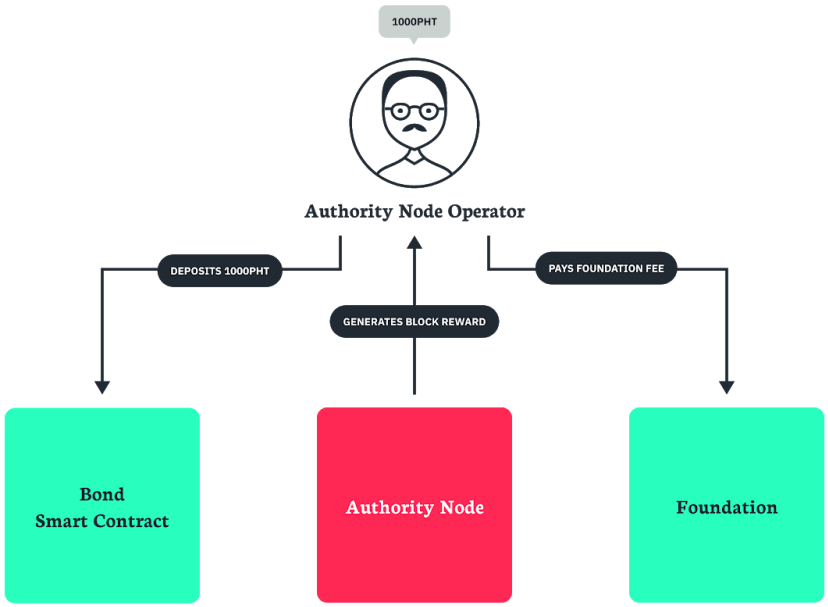
Licences are required to operate an Authority node. An Authority node can hold multiple Licences, which can be obtained via:

- Purchasing a new Licence via an auction.
- Purchasing a Licence from a Licence Owner via a bidding process.
- Renting a Licence from a Licence Owner.

Note: In the formative stages of the network, the rental and bidding processes for acquiring a licence may not be implemented.

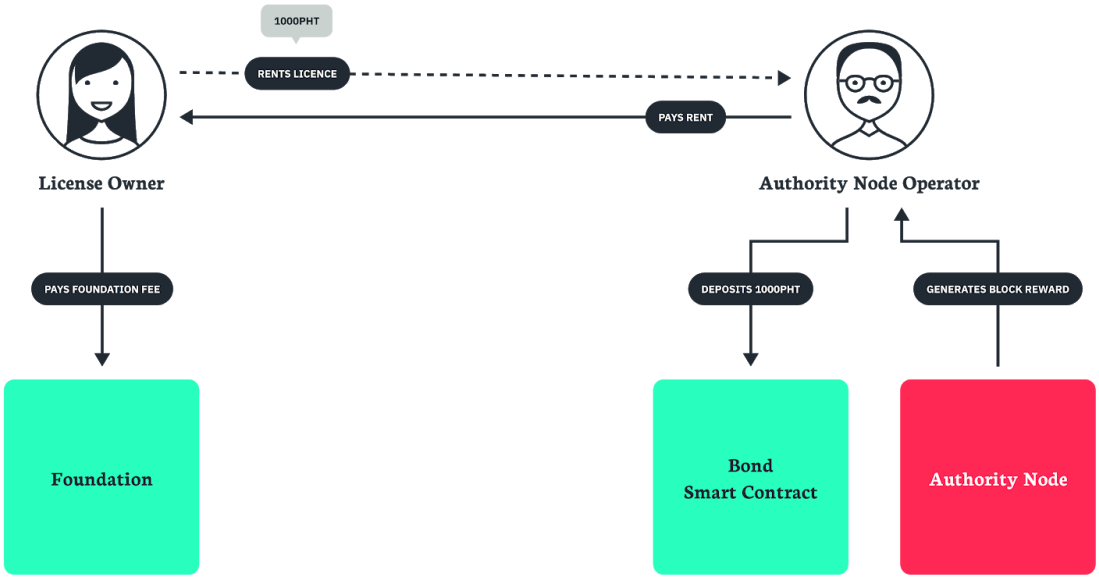
The number of issued Licences will be recorded on a smart contract with their associated owners and current renters.

When new Licences are created, the Foundation will implement an auction process. During the auction anyone can bid to purchase a Licence.



Authority Node - Owning a Licence

Licence Owners do not need to run Authority nodes in order to generate revenue. They can rent out their Licence to an Authority node for a period of time. When an Authority node rents a Licence, for every Block Reward generated, the Authority node must pay the required rent to the Licence Owner. After the rental period has finished the Licence will automatically be returned to the owner.



Authority Node - Renting a Licence

A Licence Owner cannot increase the rent during the period that the Licence is rented.

A Licence Owner must publish a Valuation Price. The Valuation Price can be higher or lower than the actual price paid for the Licence. The Valuation Price is the value the Licence Owner must sell the Licence to a new owner.

Foundation Fee

A Foundation Fee per Licence held by a Licence Owner. The Foundation Fee is based on a Harberger Tax model and is calculated as a percentage of the Valuation Price of a Licence. The higher the Valuation Price the higher the Foundation Fee.

Foundation Fee = Licence Valuation Price x Foundation Fee Percentage

Foundation Fees collected by the Foundation will be used for further funding of the network.

Bidding for a Licence

To purchase a Licence from a Licence Owner a buyer must bid higher than the published Valuation Price in order to purchase the Licence. When valid bid is placed, the owner has to respond with a higher counterbid within a Bidding Period in order to retain the Licence. If there is no valid counterbid, the Licence changes owners and there is a New Owner Period when no bids can be placed to purchase the Licence.

In order to place a bid the buyer must have deposited the required collateral to cover paying the Foundation Fee for a defined period of blocks. There will also be a minimum increase in bid size of 5% that can be placed by a buyer.

Producing Blocks

Transactions are sent by network accounts or programmatically by smart contracts. A block is produced by an Authority node validating transactions and grouping them into a proposed block. Each Authority node will have a turn in a round-robin schedule for proposing a block during a *Block Period*. Authority nodes within the Validator Set will vote on proposed Blocks, each having equal voting power that is uncorrelated to the number of Licences that they hold

Processing transactions will require a transaction fee to be paid similar to the Ethereum gas system. An Authority node will collect the fee for each transaction that they process. An Authority node will also generate Block Rewards for every valid block that they produce.

The *Block Reward* is an amount in PHT specified by the Foundation. An Authority node will be permitted to generate a Block Reward for successfully producing a valid block that has been passed a supermajority (⅔) vote by the Authority nodes in the Validator Set.

If therefore no transactions for 1 min, then an Authority Node can propose a Null Block and be rewarded Null Block Reward.

Null Block Reward = 30 x Block Reward / Number of Authority Nodes.

Note: In the formative stages of the network post go-live, no Block Rewards will be generated by Authority Nodes.

Validator Bond

An Authority node must deposit a Validator Bond into a smart contract equal to the Valuation Price of the Licences that an Authority node holds. For example, if the Authority node holds a Licence valued a 5000 PHT, then they must deposit 5,000 PHT into the Validator Bond smart contract.

An Authority node will have their bond released when they decide to leave Validator Set. There will be a wait time for their bond to be released in order to mitigate long-range attacks.

Authority nodes will be charged penalties for various Protocol Faults. Faults can include, operating a node below the minimum throughput speed or being unavailable due to being offline.

Authority nodes will lose their entire bond and be immediately evicted from the Validator Set for participating in malicious actions. Malicious actions include attempting attacks to undermine the network. All penalties and eviction decisions will be decided by the supermajority (⅔) of the Authority nodes.

Penalties for Protocol Faults

Protocol Faults	Description	Penalty
Unavailability	An Authority node goes offline or does not respond due to a system crash.	The Authority node is charged a fine and must wait 48 hrs before being permitted to re-enter the Validator Set.
Poor Performance	An Authority node is operating below the	The Authority node is charged a fine and must wait 48 hrs before

	minimum threshold period for processing transactions and producing blocks.	being permitted to re-enter the Validator Set.
Short Range Attacks	Authority nodes collude to create blocks in support of a recent invalid fork. For example, an attempt to record a double spend.	Each Authority node must bond tokens in order to join the Validator Set. If an invalid block is generated the offending Authority node loses their bond and is dismissed.
Long Range Attacks	Authority nodes collude to build an alternative blockchain starting from genesis. This can cause new nodes joining the network to believe the alternative blockchain is the correct history.	Authority nodes must wait an Unbonding Period from when they decide to leave the Validator Set for their bond to be released. If a long range attack is discovered during the Unbonding Period the Authority node will lose their bond. A moving history checkpoint will be created every 100 blocks. The checkpoint is signed by all Authority nodes and is an added measure to ensure that a second alternative chain without the checkpoints would indicate an attack.

No User Fees

Today, consumers expect to use applications for free before making the choice to purchase. Lightstreams enables this behaviour by permitting application creators to bear the costs of running their applications instead of their users. This is very similar to how application creators pay for infrastructure costs in traditions models (e.g. Amazon Web Services).

In order to take advantage of this option, application creators pre-fund a smart contract, reserving funds on behalf of the users for processing transactions.

For a registered applications, a user can send an application-specific transaction to an Authority node with no transaction fees. An Authority node will deduct the required gas fees form the pre-funded smart contract and process the transaction. The transaction will be signed by the user so that a receiving smart contract will know the transaction is from the user and not the Authority node.

Verified Accounts

Verified Accounts help provide a feedback loop where application creators and users can participate in the design and behaviour of the network. Verified Accounts can also be harnessed by applications to determine the uniqueness of an account or request access to profile information.

A Verified Account is a Digital Wallet verified by an approved *Identity Service Provider*. An Identity Service Provider verifies the user's personal information by giving a verification ranking (Basic: mobile phone verification, Advanced: Passport/National ID verification) and then publishing a unique id that represents this information.

The list of approved Identity Service Providers will be maintained via a registry reference by the Authority nodes. Initially the registry will be defined by the Foundation, following which, new Identity Service Providers will be added via the LIP process (see below).

Network Upgrades

The Network rules for defining the functioning of the network will be continuously be added to and improved through software upgrades. Each Authority node must upgrade to the new version of software to ensure that the rules are implemented. Authority nodes that do not upgrade will be penalised via protocol fault penalties when they submit invalid blocks.

Software upgrades will occur via the Lightstreams Protocol Upgrade process.

1. A Lightstreams Improvement Proposal (LIP) is submitted by any Verified Account.
2. The proposal is voted upon by Verified Accounts using a Quadratic Voting procedure as follows:

    a. Users with Verified Account will be each assigned an equal number of voting tokens (VoteMax) for voting on LIP proposals during the Proposal Period.
    b. More than one vote can be submitted by a user when voting on a proposal. Each submitted vote will be subtracted from the user's VoteMax balance during the Proposals Period. Voting balances will be reset to VoteMax when a new Proposals Period begins.
    c. The total amount paid for N votes goes up proportionately to N2. That means that the cost of voting increases in a nonlinear way, the first vote costs 1 votes, the second vote costs 4 votes, and so forth.
    d. Users can delegate their votes to Delegators who will vote on their behalf.
3. The Lightstreams Foundation allocates budget for development of the proposal.
4. Development is completed, reviewed and tested.
5. Authority nodes upgrade to the new version of the protocol software.

Note: During the formative stages of the network post Go-Live, the Lightstreams team will implement changes to the protocol until the LIP process has been put in place.

Note: A Token Curated Governance style system as White Paper may be developed first for the Network Upgrade process until the integration of Identity Service Providers is fully realised.

Delegators

A Delegator is a Verified Account and represents other user accounts. Users that do not wish to review and vote on all governance issues can assign their votes to a Delegator, that has a particular political opinion, who will vote on their behalf. For this service, a Delegator will be entitled to take a percentage of voting tokens as a fee.

At anytime a user will be able to reassign their Voting tokens to another Delegator or back to their own accounts.

Conclusion

Lightstreams is a network designed for privacy-focussed Decentralised Applications (DApps). Granting of access to protected content is controlled through programmable

smart contracts. In order for an application to be responsive, Lightstreams has been designed for fast smart contract confirmation times.

In order to attain fast throughput via short confirmation times, Lightstreams utilises a fixed set of decentralised and independent Authority nodes for validating transactions. Consensus between Authority nodes is achieved through a Delegated Proof of Authority (DPoS) protocol. The protocol consists of a system of licences and delegated votes by network users in order to select Authority nodes and decide on network upgrades.

Lightstreams' peer-to-peer transmission of information provides for a transparent flow of information that is recorded as an untampered history of events for any piece of content, product or service. In order to prevent harmful content from being distributed, proposed system of publishing Channels with Moderators is proposed with further consultation to be sought.

FAQs

Q: Is the Validator Bond pegged to the value of the Validator Licence they hold?
A: No. An Authority node is required to deposit a bond amount equal the valuation of their licence at the time they acquire their licence - either via renting or purchasing. If the valuation of the licence increases or decreases the bond does not need to be adjusted.

Q: How many licences will be issued? Won’t issuing too many cause significant inflation?
A: New licences will be initially be determined by the Foundation and then via the LIP process taking into account the balance between expanding the Validator Set and ensuring inflationary measures are minimised.

Q: What is the advantage of renting a licence?
A: The advantage for Authority node of renting a licence is that they are only required capital to cover the Validator bond, saving 50% of the upfront costs. They also do not run the risk of being evicted from the Validator Set if someone acquires their licence through the bidding process.

Q: Can anyone take part in the voting of LIPs if pass the verification process?
A: Yes.

Q: Can an Authority Node trade their Licence while they are part of the Validator set and proposing blocks?

A: No. If an Authority node is the owner of their licence then they cannot sell their licence while they are part of the Validator set. They must first leave the Validator set before they are permitted to sell their licence. However, if the Authority node is renting their licence then the Licence Owner is permitted to sell their licence to a new owner.