

# xx network

## White Paper



V2.0  
April 15, 2021

The information provided in this white paper pertaining to xx network, the xx coin (the "Coins"), xx network business assets, strategy and operations is for general informational purposes only and is not a formal offer to sell or a solicitation of an offer to buy any Coins, securities, options, futures, or other derivatives related to securities in any jurisdiction and its content is not prescribed by securities laws. Information contained in this white paper should not be relied upon as advice to buy or sell or hold Coins or securities or as an offer to sell Coins. This presentation does not take into account nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information in this white paper is believed to be accurate and reliable, xx network and its agents, advisors, directors, officers, employees and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information and xx network expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. xx network reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient thereof.

Neither xx network nor any xx network representatives shall have any liability whatsoever, under contract, tort, trust or otherwise, to you or any person resulting from the use of the information in this white paper by you or any of your representatives or for omissions from the information in this presentation. Additionally, xx network undertakes no obligation to comment on the expectations of, or statements made by third parties in respect of the matters discussed in this white paper.

This white paper contains forward looking statements, including among other things, statements concerning the distribution of xx coins, and other statements identified by words such as "could," "expects," "intends," "may," "plans," "potential," "should," "will," "would," or similar expressions and the negatives of those terms. Forward-looking statements are not promises or guarantees of future performance, and are subject to a variety of risks and uncertainties, many of which are beyond our control. Actual results could differ materially from those anticipated in such forward-looking statements as a result of various risks and uncertainties, which include, without limitation, market risks and uncertainties and the satisfaction of losing conditions for a distribution of xx coins. Forward-looking statements speak only as of the date hereof, and, except as required by law, xx network undertakes no obligation to update or revise these forward-looking statements.

# Table of Contents

<b>Table of Contents</b>	<b>3</b>
<b>Our Vision</b>	<b>4</b>
<b>Introducing the xx network</b>	<b>5</b>
<b>xx coin</b>	<b>6</b>
<b>xx blockchain</b>	<b>7</b>
<b>xx nodes</b>	<b>8</b>
<b>xx network mix packets and communications</b>	<b>9</b>
<b>xx governance</b>	<b>11</b>
<b>xx coin economics</b>	<b>12</b>
<b>Appendix I: Network Communications Economics</b>	<b>14</b>
<b>Appendix II: Projected Node Specifications</b>	<b>17</b>
<b>Appendix III: Staked Governance</b>	<b>18</b>

## Our Vision

*“The choice between keeping information in the hands of individuals or of organizations is being made each time any government or business decides to automate another set of transactions. In one direction lies unprecedented scrutiny and control of people's lives, in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates.”*

These words, concluding a 1992 *Scientific American* article titled “Achieving Electronic Privacy” by David Chaum, warned the public of a “dossier society” where corporations and governments could manipulate and control the public through the gathering of data. It also described the first architecture enabling users, through cryptography, to take control over their own information. Since then, most of the world’s information networks have chosen to place user data in the hands of organizations rather than the individuals from whom it is gathered. Whether by accident or by design, these networks have violated privacy, leaked vital information, spied on intimate conversations, sold personal details to the highest bidder, and facilitated the manipulation of public opinion and elections.

The resulting crisis of confidence has inspired research and investment in decentralized networks and blockchains that empower individual users to manage and govern the network without relying on intermediaries. While Bitcoin and other blockchains have made important strides towards decentralization, existing networks have failed to realize the concept’s potential.

All current blockchain networks have several fundamental weaknesses. They are built around mechanisms that can lead to the consolidation of power, threatening the decentralized nature of the network. They lack the speed and scalability to serve users at a global scale, which prevents mainstream adoption of the technology. They rely on cryptography that may be vulnerable to nation-state adversaries and, soon, to the use of quantum computers, limiting the security of the financial products and data they manage. Finally, they fail to provide usable privacy, exposing user metadata and identifying information to anyone monitoring the network.

The xx network is the first platform capable of meaningfully solving each of the above challenges. This breakthrough is based on novel innovations and decades of research. We believe that the xx network will dramatically empower a great many individuals to participate in a new user-controlled era of information technology.

## Introducing the xx network

The original promise of the Internet was an open, free, and trusted online environment where users could exchange information and ideas. Web 2.0 technology built on this vision by bringing rich interactivity and enabling user content, which launched some of the most widely used online platforms in the world including Facebook, Google, and Amazon. As these “free to use” platforms grew in scope and capability, their users’ data became, in effect, the product. This commoditization of personal data has eroded trust and harmed the free, open nature of the Internet.

The xx network intends to be a new type of platform, offering a protected digital sphere, through which its users can share ideas and exchange value in a secure and private way. It is comprised of five major components:

- **Currency:** A secure and optionally denominated digital currency, the xx coin, that can be traded among users and businesses while incentivizing the operation of the network.
- **Blockchain:** A breakthrough consensus algorithm and blockchain protocol, ensuring consensus-based operations and capable of scaling to meet any level of demand.
- **Nodes:** A decentralized, global network of conventional servers, each independently owned/operated and running the xx network software.
- **Communication:** A way to communicate with the network and other users using mix packets so that there is no leaking of information about the data being sent or the linkage between sender and recipient.
- **Governance:** A democratic governance system that enforces the transparent operation of the network and empowers users to participate.

We do not expect all of our users to have the time or interest to fully understand the details of our technology, however our vision of a community-governed network is best realized with well-informed users. Accordingly, it is our intention to make everything as clear, transparent, and accessible as possible.

In this white paper, we aim to present each of the above five components as currently conceived in an approachable, relatively nontechnical manner. Further, this white paper constitutes our proposal for the development of the xx network and the xx coins and it remains subject to change on an ongoing basis as to the extent the xx network deems it necessary or advisable. Neither the xx network nor any of its related parties make any representations or warranties, express, implied, statutory, or otherwise concerning the success or potential success of the development or commercialization of the xx network or xx coins.

We welcome deeper scrutiny from experts wishing to dig into the details and will release our source code and separate, more technical documents. These will form a set of living documents that will evolve and may change for any number of reasons including the input from the community.

## xx coin

The xx coin is the native digital currency of the xx network. The xx coin secures the network through staking, enables payments, incentivizes governance, and acts as the network's economic vehicle. To achieve this, the xx coin is both cryptographically and structurally unique. Coins rely upon one-time-use hash-based signatures. They provide quantum-security that can be used to construct denominated payments which, when combined with xx network usage, facilitate even more private payments.

xx coin technology is capable of supporting many coin structures, including:

- **Denominated coins** emulate physical money by having pre-set values, which are base-two numbers such as 1, 2, 4, 8, 16, 32, etc<sup>1</sup>.
- **Wallets** allow users to have a multi-use address in order to send and receive xx coins. This is achieved by linking a list of hash-based public keys to the wallet address. Transactions sent via wallets lack the privacy properties offered by denominated coins.
- **Multi-signature**, whether denominated or wallet based, requires signatures from different parties in order to be spent. This type can be used to escrow funds, share custody, and act as the core operation in dApp consensus.

Denominated xx coins are tailored to leverage the unprecedented privacy provided by the network's communications layer. Payments are split into multiple denominated coins that form individual transactions indistinguishable from one another. After being processed by the communications layer, transactions are provided to the current leader of consensus, who has no way of identifying how much money is being spent or is owned by each user.

xx coins can be converted to **paid postage** in order to send paid mix packets through the xx network. **Free postage** is made available to all users in limited quantities to support free sending of messages. *Further details can be found in the xx network communications and xx coin economics sections as well as Appendix II: Network Communications Economics.*

A critical goal of the xx network is to broadly distribute coin ownership by MainNet in order to ensure robustness of the network, create egalitarian incentives, and support decentralization.

---

<sup>1</sup> Fractional base two coins are also supported such as  $\frac{1}{2}$ ,  $\frac{1}{4}$ ,  $\frac{1}{8}$ , ect.

## xx blockchain

The xx blockchain is the decentralization mechanism of the xx network, allowing independently operated nodes to come to a publicly verifiable agreement on the execution of transactions and network operations. The xx blockchain consists of a **blockchain data structure** which immutably publishes the transaction results, and a **consensus mechanism** to enforce the collective agreement on the state of data by a quorum of nodes.

Building on the pioneering work of others in the blockchain space, the xx network has developed a new consensus protocol, called **xx consensus**, that achieves **linear scalability**. Xx consensus is based on a family of protocols, called byzantine fault tolerant (BFT) consensus, characterized by low latencies, safety during large-scale node failure, and the ability to remain secure if up to one-third of the network is compromised or goes offline. xx consensus is distinguished from existing BFT approaches in its quantum resistance, high transaction throughput, and ability to scale to thousands of nodes.

xx consensus leverages three core innovations:

**Committed Randomness** is a way to generate unmanipulatable global randomness every block. Each node in the xx network publicly commits (using hash functions) to a large number of random values that they generate but keep secret. Every round, a node who is chosen to be a block producer (by a prior round's random), reveals a predetermined secret that is verifiable by the rest of the network. When combined with the chain of all prior revealed randoms extending back to the random published in the genesis block, a new verifiable but unmanipulatable random is generated to schedule nodes for subsequent rounds.

**Endorser Sampling** enables xx consensus to achieve its scaling properties by randomly selecting a constant-sized subset of the network to endorse a block. In BFT consensus protocols, communication latency becomes unworkable as the network grows in size, as all nodes must communicate with all other nodes. To compound the problem, a majority of nodes must receive and verify every transaction, which becomes infeasible when dealing with large, quantum-secure signatures in a large network. By sampling a subset of the network to receive, verify, and endorse the transactions in a block, the majority of nodes only need to receive a condensed ledger of all transactions along with the endorsement of the sampled nodes.

**Compact Group Endorsement Signatures** can not only improve consensus performance but also allow for mobile devices to efficiently receive and verify proof that a transaction is complete. The xx network has developed a new quantum-secure group-signature scheme based on hash signatures that vastly reduces the size of proofs of finality. To achieve this, each endorser signs only a small number of bits corresponding to the block. As a result, each individual signature is insecure on its own, but if enough endorsers sign the same block, then the signature as a whole is quantum-secure, compact, and quick to validate.

## xx nodes

The xx nodes are the servers that collectively operate the xx network. Achieving the necessary capability and scalability to serve a global user-base and replace centralized systems requires xx nodes to be reliable and performant. The network will launch with hardware, bandwidth, uptime, and xx coin bonding requirements for all nodes. The xx network promotes an egalitarian approach, where any independent individual or organization is welcome to apply to the xx network to become a node.

There will be at least two roles explicitly defined for nodes: mix node and validator. Mix nodes are responsible for executing the xx mix packet protocol and delivering batches of transactions to validators. Validators are responsible for executing the xx consensus protocol, processing transactions, and providing unmanipulatable randomness to mix nodes for scheduling. More node roles may be added through governance to add new features to the network, such as private smart contracts.

To prevent Sybil attacks, where multiple seemingly independent nodes are controlled by a single entity, the xx network relies on a robust and democratic governance process enforced by **nominated staking** to select and approve new nodes from the pool of applicants. Moving forward, and through governance, the community can modify the node application requirements to take into account supply and demand of network resources.

Running a node requires some expertise, time, and money to acquire and maintain the computing hardware and bond. To ensure that nodes remain independent and self-sufficient, an incentivization system is built into the xx network. Nodes that correctly participate in the network are ultimately compensated in xx coins. More details about this mechanism are presented in the **xx coin economics** section.

*Further details can be found in the xx governance section and Appendix III: Projected Node Specifications.*



## xx network mix packets and communications

Communication between computers is the essence of the Internet and the basis for user-to-user messaging, websites, social media, and smartphone apps. Unfortunately, these communication systems have a flaw that has proven to be a serious threat to society, a flaw that allows organizations to monitor and store information on users. While some services offer end-to-end encryption to protect the specific contents of each communication, this is insufficient to protect the “metadata” associated with who is talking to whom and when. Machine learning algorithms fed with seemingly innocuous user metadata can already uncover the nature of a user’s activities and even their beliefs and habits. For example, the collection and analysis of metadata has fueled the growing capability of organizations to manipulate public opinion and, in turn, threaten fundamental freedoms.

The xx network is the first step towards a protected internet. It is intended to provide effective protection against leaking metadata by severing the identifiable link between the user and associated actions, in effect “shredding” metadata before it is even constituted. The xx network will be capable of mixing thousands to possibly millions of mix packets per second, potentially delivering each in just a few seconds.

The first proposed solution for protecting metadata was born out of mix-cascade networks, introduced by David Chaum in 1979. This breakthrough approach forwarded a batch of messages from server to server, each server reordering and decrypting the batch<sup>2</sup>. This original proposal required time-consuming public key operations for each message at each node and endpoint, making the approach impractical for many consumer scale use cases such as real-time messaging or interactive online applications where latencies are expected to be under 5 seconds.

As its communications layer, the xx network leverages a variant of the breakthrough cMix protocol with end-to-end encrypted mix packets. Through partially homomorphic encryption techniques, the network precomputes<sup>3</sup> the vast majority of operations in advance, allowing batches of packets to be mixed through the network and delivered with little overhead or latency. Mix packets within the communications protocol are all the same size and delivered in unison. As a result, the xx network thwarts the two mechanisms of metadata analysis: packet length and packet timing.

In the xx network, unpredictably chosen teams of nodes take turns in operating the mix packet protocol. The client encrypts mix packets for the final recipient and then adds symmetric encryption for each node in the team. So long as any node in a team remains honest, these encryptions make it impossible for any collusion or compromise to tell who

---

<sup>2</sup> David Chaum. “Untraceable electronic mail, return addresses, and digital pseudonyms”

<sup>3</sup> Precomputations in xx cMix: <https://xx.network/blog/real-cryptography-real-time>

the endpoints are or whether a client is sending a payment, communicating with a **dApp**<sup>4</sup>, or sending a message.

## Free and Paid Network Usage

Private use of the communication layer within the xx network is designed to be freely accessible to anyone with a suitable mobile phone. To further this goal, users will be provided an account with free postage<sup>5</sup> upon either creating a KYC identity, or staking or burning a small number of xx coins, or through further mechanisms that become available. The allotted free use is sufficient for most users to message in their day-to-day life, but insufficient for dApps, smart contracts, and businesses operating on the xx network which communicate at volume. Any user, dApp, or business will be able to pay for additional bandwidth by purchasing paid postage with xx coins.

*Further details can be found in the xx cMix Architecture Brief and the academic paper on the cMix protocol.*

---

<sup>4</sup> A distributed application (dApp) is a software application run collectively by multiple nodes on a network rather than on a single device

<sup>5</sup> More details on postage can be found in the xx coin economics

## xx governance

Since there is no central authority managing the network and resolving disputes, the xx network requires **governance** to achieve collective agreement on code and core data updates. Governance in the xx network will rely on **nominated staking**.

Governance in decentralized platforms is used to describe leader and membership selection in consensus, code changes, and/or treasury management among other things. While it's possible to have separate or even multiple mechanisms to handle each of these facets, almost all of the proven approaches use **proof of stake (PoS)** or **proof of work (PoW)** to prevent sybils and ensure that malicious actors risk significant resources or money in any attempt to disrupt the network.

The xx network believes the performance and energy cost of PoW systems is too extreme while not doing enough to prevent centralization of power in mining farms and domination of hardware supply. We are similarly concerned with PoS systems being operated by whales (large token holders) and exchanges and excluding smaller coin holders from running nodes or earning incentives. In principle we would prefer a one-user-one-vote approach though this requires knowing who your voters are through expensive and slow centralized points of failure in KYCing the community or relying on unproven reputation mechanisms.

We believe that with some modifications, a nominated stake approach provides an inclusive governance mechanism that incentivizes active participation in the community while ensuring that nodes are held accountable for their actions. In such a system, the community selects the active set of nodes by nominating their own coins on their favorite nodes in exchange for a share of the rewards generated. Similarly, code changes and other governance decisions are made by nominating coins with special conviction modifiers used to mitigate domination by whales.

The xx network plans on having four primary chambers of governance:

- **Council** - The council is a representative chamber elected by the coin holders to develop referenda and manage the treasury.
- **Tech Committee** - The tech committee is a group of technical experts and developers who are selected by the council to develop features, patch bugs, and manage emergency issues.
- **Coin Holders** - The coin holders are the community at large, using their staked xx coin to approve referenda, elect the council, and select the active node set.
- **Users** - The users represent the coin holders who spend xx coin to use the various features of the platform. They approve referenda, elect the council, and select the active node set with voting power determined by how much xx coin they have spent on transaction fees. This chamber may not become active until later.

*Further details can be found in Appendix IV: Staked Governance*

## xx coin economics

The xx network is proposed with an economic model that accelerates the inherent utility of a scalable, quantum-secure coin and leverages the growth and versatility of the platform's native private messaging functionality. As compensation for the work of consensus and messaging, nodes will receive a **reward** composed of a share of the **fees** paid into the network and an **inflationary reward** of newly minted xx coins.

Inflation will be according to an inflation curve starting with higher inflation to support the early network and tapering down to maintain the later network. While the majority of the inflationary reward is given to the nodes and coin holders, portions are transferred to the treasury. Further details can be found in *Appendix I: Network Communications Economics*.

### Coin Allocation

In the genesis block, one billion xx coins will be minted. The initial distribution of the coins will be via an ERC-1404 smart contract<sup>6</sup>. When MainNet goes live, it is planned that this smart contract will be converted to an intermediary coin vehicle before becoming an official xx coin on the xx network.

A total of 30% of the xx coins are reserved for sale by the xx network. 25% of the xx coins are reserved for project creators and vest over 3 years. 10% of the xx coins are reserved for an xx network Foundation to incentivize ecosystem development (developer awards etc.). The final 35% are allocated for coin holders to receive as staking and incentive rewards for participating in node nomination and governance and for pre-MainNet node rewards and community air drops.

### Postage

Postage is a unit that quantifies the amount of computing power and bandwidth required to transmit data privately across the xx network. To ensure that the network is universally accessible, all postage accounts automatically accrue free postage gradually over time. High volume users will need to purchase paid postage with xx coins. All transmissions, for dApps, user-to-user messages, payments, and so forth, will consume postage. Block rewards are paid to Nodes in xx coins, and are driven by transaction fees and paid postage used on the xx network, supplemented by inflation and the 30% staking rewards coin allocation..

---

<sup>6</sup> A smart contract is a self-executing contract whereby the terms of the agreement between the parties are directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network, making them unchangeable and final.

## Communications and Mix Packet Processing

Communications, a core utility of the xx network, scales differently than with traditional decentralized systems. Where most decentralized systems slow down as they scale, adding more nodes to the xx network increases mix packet capacity and drives growth. As more users use more mix packets, the network generates more revenue supporting the onboarding of more nodes. This increases throughput and allows for expanded utilization — creating a virtuous cycle. Further details can be found in *Appendix II: Communications and Mix Packet Economics*.

Private payments with the xx coin accelerate this engine. In order to make payments private, denominated coins are split into individual messages as described in the **xx coin** section. Due to the limitations on free postage, private payments will likely require the use of paid postage to submit the entire payment simultaneously for fast finality.

# Appendix I: Network Communications Economics

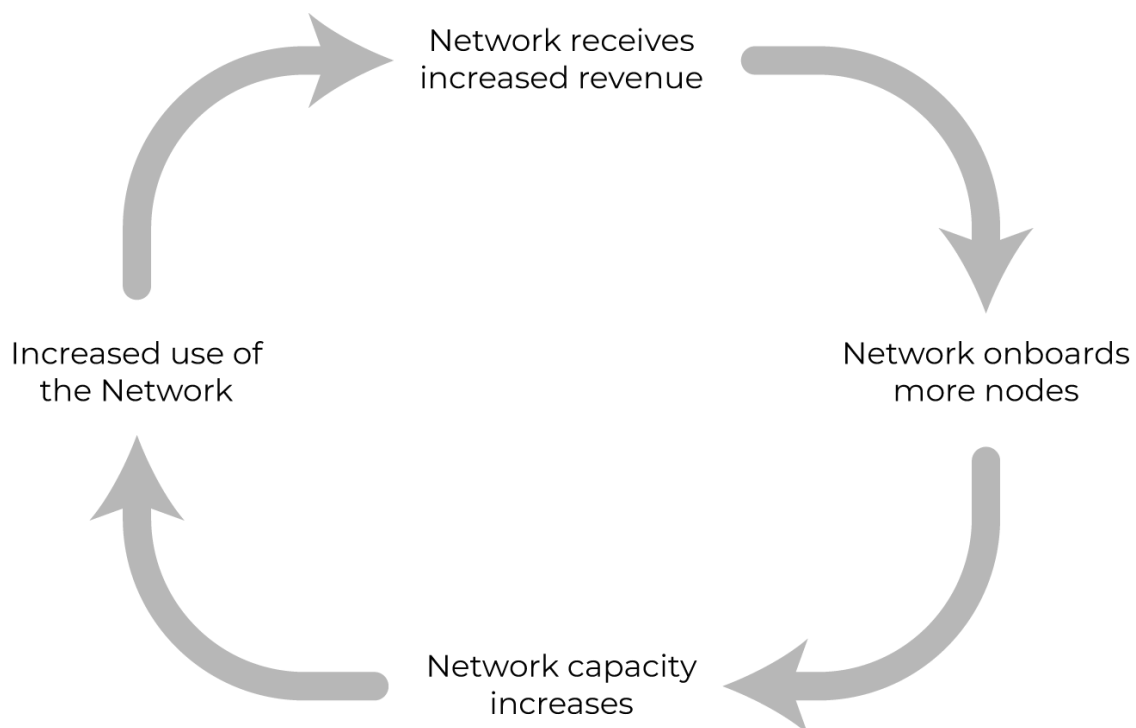
## Scaling Economics

For most blockchains, security is increased as nodes are added. Adding nodes does not, however, improve the fundamental performance of the network. In fact, in most cases, adding nodes actually reduces network capacity.

This penalty on growth is a fundamental problem faced by most modern decentralized networks.

The xx network is very different. One of the network's core technologies is not a blockchain, but a mix network. Every additional node adds processing and relay capacity, supported by the scalable xx consensus protocol. So, as the number of nodes increases, both security and performance improve<sup>7</sup>.

These scaling characteristics of the xx network power a virtuous cycle<sup>8</sup> of growth, which we believe is unique among decentralized platforms.



<sup>7</sup> Further Details on communications scaling can be found in the *xx network Architecture Brief*.

<sup>8</sup> A virtuous cycle is a self propagating cycle in which a desired or positive result leads to further designed or positive results in a chain

This virtuous cycle of growth-driven security and performance improvement can induce substantial growth of the xx network. As utilization of the network increases, revenue increases. This revenue then allows the network to onboard and support the costs of additional nodes, which will then further increase capacity. As capacity increases, availability of the network then increases, thereby stimulating further utilization and starting the cycle again.

## Driven Network Effects

As the network grows, its value is likely to grow at a quadratic rate. This is because of inherent network effects as per Metcalfe's Law<sup>9</sup>. These very favorable network effects have created enormous concentrated economic value and power in the hands of centralized companies like Google and Facebook.

The xx network is capable of supporting the growth and scale required to create a truly global decentralized community of users. This departure from previous decentralized networks allows the xx network to benefit from the very same favorable network effects that have driven the value of centralized technology companies.

## Free and Paid Postage

When an xm (mix message) is sent through the xx network it is authenticated to the sender of the message as part of the cryptographic mixing process. During this process, the nodes use the authentication to verify an account on the blockchain to deduct **postage** from it.

### Types of Postage

Postage falls into two categories: free and paid. All accounts periodically accrue a set allotment of free postage at a universal set rate. The intention is that a majority of users will never exceed their allotment of free postage with normal use.

### Free Postage

Free postage is, however, limited in both total number and maximum rate. One cannot accumulate free postage beyond a uniformly applied maximum and there is a limit to the number of free messages that can be used at once.

To ensure no users get locked out of the xx network, free postage will be generated at a slow, continual, albeit discreet, rate. As a result, users who have used all their postage will not wait long before they are able to use free postage.

### Paid Postage

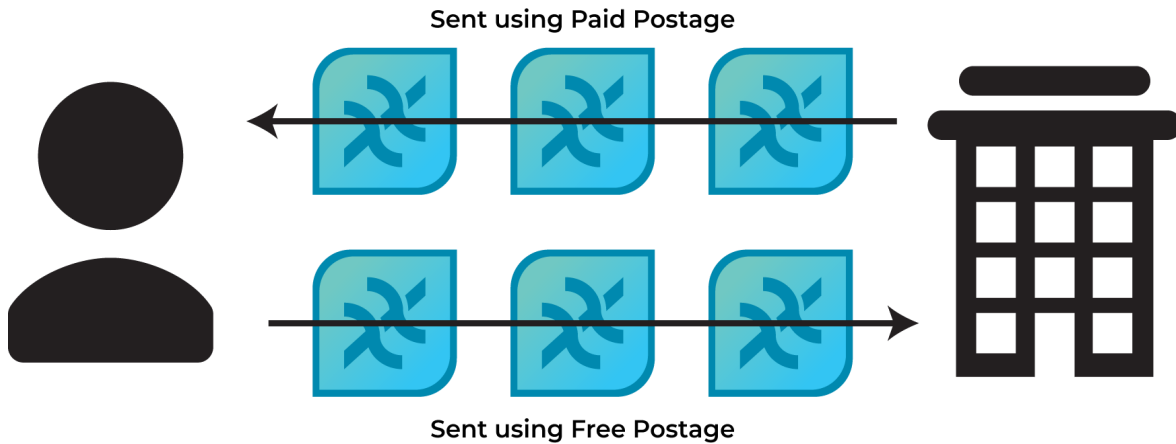
---

<sup>9</sup> <https://www.techopedia.com/definition/29066/metcalfes-law>

All users also have the ability to purchase paid postage in the event that all of their free postage is used up. Usually these paid messages will be needed by high-volume users such as businesses and dApps. The cost to individual paid messages is intended to be negligible.

### Free/Paid Dependency

Free and paid postage mutually coexist and support each other's use. Paid postage will typically be used by a business, dApp, or smart contracts to communicate with their customers or users. However, customers will usually respond using free postage, creating a *free/paid postage dependency* as shown in the figure:



In this common use case, messages sent with paid postage will be associated with a related message sent with free postage. As a result, if the network refuses to accept free postage in favor of paid postage to increase profits, the frequency and use of paid postage will fall, reducing revenue. Given that all messages are anonymous, it is impossible to distinguish free messages that are a component of paid interactions from those that are not, which ensures egalitarian access to the networks as it grows.



## Appendix II: Projected Node Specifications

Nodes within the xx network are designed to be built with consumer grade hardware. The current proposed, but not yet finalized, specifications for the MainNet are as follows:

- Modern High-End Consumer grade CPU (8 physical/16 logical cores)
- 32GB RAM
- 1TB SSD storage
- Mid-Range modern GPU with 32-bit Mul Units (Example: Nvidia GeForce RTX 2070 or RTX 3060Ti)
- 100Mbps internet connection

Such a machine is expected to fit in a single 1U or 2U rack space. The most difficult to achieve requirement is the 1Gbps connection which is necessary to assure network performance. A survey of colocation prices suggests operating costs range between \$250~\$800 USD per month within the United States, or \$3,000 ~ \$9,600 USD per year. The inflation schedule is expected to cover these costs with a healthy safety margin.

Nodes will also be required to run a gateway which is projected to nominally require a dual or quad core CPU and a 100 Mbps internet connection. Gateways are designed to be scalable with load on cloud infrastructure.

- Modern Medium/Low-End Consumer grade CPU (2 physical/4 logical cores)
- 4GB RAM
- 256 GB SSD storage
- 100Mbps internet connection

As the network matures, it may make sense to have additional node roles, some of which could run on substantially different hardware specifications.

## Appendix III: Staked Governance

Coin holders in our **nominated proof of stake (NPoS)** platform are responsible for electing representatives, approving referenda, and deciding who the active set of nodes in the network are. This is accomplished via a **staking** system where users lock up their coins for a period of time in exchange for decision making power. We characterize three types of decisions: **node membership, referenda, and treasury spending.**

### Node Membership

Most stake-based systems require explicit selection of the active nodes in a network over a specified period of time which we call an **era**. The xx network uses NPoS to select the nodes that have the most stake at the beginning of each era as active nodes in the network. These active nodes will be responsible for performing their role as described in the xx node section in exchange for xx coin rewards at the end of the era.

In order to obtain enough stake to become an active node, candidates will likely need to campaign to the community for support. The community is incentivized to determine which nodes are best for the platform by **nominating** their own coins as stake for their favorite campaigning candidates. In exchange for their nomination, coin holders will get a share of the xx coin rewards earned by a node. This nomination process allows small coin holders to participate in the economics of the platform while ensuring that nodes are held accountable with large slashable stakes.

The use of community nominations attempts to address the concern of whales dominating the node community and economic rewards. In practice, this has not turned out to be 100% effective in other platforms especially if wealthy individuals gain a strong foothold early in the network.

To solve this, the xx network introduces a seeding mechanism by which our **BetaNet node operators** become the initial set of active nodes in the network at MainNet. Our BetaNet nodes are a group of hundreds of unique community-curated nodes representing a wide range of professions, income, cultures, and locations. These nodes are early believers in the vision of the platform, some operating without compensation for nearly a year in support of the network and will become an important decentralizing force in the network.

### Referenda

Referenda are proposals that the community or its representatives can introduce for stake-based voting. A referenda generally has an off-chain and on-chain component. The off-chain component consists of a plaintext description and rationale for the referenda in a forum which encourages healthy discussion and debate. This off-chain component will link to an on-chain transaction which will execute the referenda if successful. Similar to node nominations, coin holders will stake coins to vote on referenda. To mitigate the ability of

large coin holders dominating decision making, a conviction multiplier may be used which locks up coins for longer periods of time to increase voting power.

### Treasury

The treasury is a pool of xx coins that can be used by the community in many ways including: driving development of popular features, rewarding community efforts, marketing, or promoting partnerships. Treasury funds are accumulated by taking a percentage of generated era rewards and transaction fees. Both the council and community can propose treasury transactions with the council voting to approve or reject them. Unused funds are periodically burned to provide deflationary economic pressure and prevent the treasury from becoming big enough to incentivize malicious behavior.

### Chambers



There are three decision making chambers: council, tech committee, and coin holders. The council is elected by coin holders via staked voting with members acting as representatives of the platform, staking their public reputation to propose referenda to the community and approve treasury transactions. The tech committee members are developer groups elected by the council to perform core feature development and emergency bug fixes. All referenda pushed by either the council or tech committee must be approved by the coin holders.