White Paper

V1.3
12/18/2019

The information provided in this white paper pertaining to Praxxis Corp. ("Praxxis" or the "Company"), the xx coin (the “Coins”), Praxxis 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, Praxxis 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 Praxxis expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Praxxis 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 Praxxis nor any Praxxis 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, Praxxis 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, Praxxis undertakes no obligation to update or revise these forward-looking statements.

Table of Contents

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, such as concentrated token distributions, 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 individually and solve all of them simultaneously. This breakthrough is based on novel innovations and decades of research. The network is composed of two projects, Elixxir and Praxxis, which are established and led by David Chaum. 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, and now threatens our freedoms and democracy itself.

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 without leaking information about the data being sent nor the sender or 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 Praxxis deems it necessary or advisable. Neither Praxxis 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 coins

The xx coin is the native digital currency of the xx network. It 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 used to construct denominated payments which, when potentially combined with xx communications, 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[1]. Each coin can only be spent once because of the type of signature used.
- ***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 Elixxir. Payments are split into multiple denominated coins that form individual transactions indistinguishable from one another. After being processed by Elixxir, 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 communications 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 communications and xx token economics sections as well as Appendix II: 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.

Further details can be found in the Praxxis Technical Paper.

[1] Fractional base two coins are also supported such as ½, ¼, ⅛, ect.

xx blockchain

The xx blockchain is the mechanism of decentralization in 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 is comprised of a **blockchain data structure** which immutably publishes the results of transactions, and a **consensus mechanism**, which enforces the collective agreement on the state of data by a quorum of the nodes.

Building on the pioneering work of others in the blockchain space, Praxxis 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 is built on five core mechanisms:

NodeCon is a unique, powerful way to initialize the network. All initial node operators are invited to attend an event where they meet each other, establish quantum-secure communication channels by exchanging symmetric keys, and collectively generate an unmanipulatable random value that will be used to seed randomness for all future blocks. The physical, but virtually auditable, aspect of NodeCon ensures that the network is initialized in a quantum-secure manner and makes it difficult for any single entity to establish a large Sybil presence in the initial network.

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 one generated at NodeCon, 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.

Efficient Fallbacks are needed anytime malicious behavior or an unreliable network disrupts a round of consensus. If a block producer is unresponsive, xx consensus will produce an empty block with the same linear scalability as a normal block and select a new block producer for the next round. If the endorser sample is unable to generate a valid endorsement of the block then a new sample is rapidly chosen.

Compact Endorsement Signatures not only improve consensus performance but also allow for mobile devices to efficiently receive and verify proof that a transaction is complete. xx consensus 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 signatures as a whole is quantum-secure, compact, and quick to validate.

Further details can be found in the Praxxis Technical Paper.

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.

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 that selects and approves 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. 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 token economics** section.

Further details can be found in Appendix III: Projected Node Specifications.

xx communication

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, allowing organizations and governments to monitor and store information on users. While some services offer end-to-end encryption to protect the exact 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. The collection and analysis of metadata fuel the growing capability of organizations and governments 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 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[2]. 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 Elixxir's variant of the breakthrough cMix protocol with end-to-end encrypted packets. Through partially homomorphic encryption techniques, the network precomputes[3] the vast majority of operations in advance, allowing batches of messages to be mixed through the network and delivered with little overhead or latency. Packets within Elixxir's cMix protocol are all the same size and delivered in unison. As a result, Elixxir 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 Elixxir's cMix protocol. The client encrypts messages for the final recipient and then adds symmetric encryption for each node in the team. These encryptions make it impossible for any collusion or compromise of less than all nodes in a team to tell who the endpoints are

[2] David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms"
[3] Precomputations in Elixxir: https://elixxir.io/blog/real-cryptography-real-time

or whether a client is sending a payment, communicating with a **dApp**[4], or sending a message.

Free and Paid Communication

Private communication 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[5] upon either creating an authenticated user account, or burning a small number of xx coins, or through further mechanisms that become available. The allotted free messaging is sufficient for most users 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 Elixxir Architecture Brief and the academic paper on the cMix protocol.

[4] A distributed application (dApp) is a software application run collectively by multiple nodes on a network rather than on a single device

[5] More details on postage can be found in the xx token 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 **sample voting (SV)**[6].

Sample voting, developed by David Chaum, randomly polls a subset of the voting population, incentivizing the selected subset of voters to make informed decisions without intermediating representatives. In SV, fewer voters cast a vote on a given topic. As a result, when selected to participate in a poll, voters can be incentivized with fixed or lottery-based token awards without any linking of compensation to votes. Because the number of active voters is relatively small and because of the public cryptographic verifiability that each vote is tallied correctly, voters know their votes have significant sway, encouraging them to be responsible and to research the topics in depth in order to make informed choices.

While any non-polling place election inherently holds the risk of vote buying, such as when a buyer views a live stream of a voter in the act of voting, decoy ballots combined with a proof of decoy can undermine the vote-buying market eliminating this risk. Unique decoy ballot technology provides ballots that are verifiably not tallied but are impossible for anyone but the owner to differentiate from a real ballot. By flooding the vote-buying market with decoy ballots, the market for purchasing votes is effectively destroyed. “Proof of decoy” provided to requestors of decoy ballots allows them to be sure they are not receiving countable ballots.

The primary legislative engine of the xx network will be one user, one vote. Every vote will be according to SV, with voters selected from those users who have been authenticated as unique. Initially, users will be authenticated through their participation in token sales, with further mechanisms for authentication added as the network matures. Governance will make many decisions, including the addition of nodes to the network, the removal of nodes for malfeasance, the addition of more sources of authenticated users, and changes to the software of the network. Some types of proposals, including changes to token economics or changes to governance itself, will require a supermajority in order to be approved.

Within the xx network, such direct democracy may be ideal. Problems with the “tyranny of the masses” are significantly reduced by the network’s decentralization and privacy. The remaining concern is to protect those groups who are critical to its function. Some types of votes may require approval from subgroups within the network, such as nodes or those who pay to send messages.

[6] David Chaum. “Random-Sample Voting”. https://rsvoting.org/whitepaper/white_paper.pdf

Foundation

The foundation will receive a portion of the block reward, which will be used to fund its activities. It will be tasked with a variety of responsibilities including: community development, attending and hosting events, software development, and so forth.

xx token 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 **block reward** composed of a share of the **income** the network generates and an **inflationary reward** of newly minted xx coins.

Inflation is expected to be 0.5–0.8% per year, with a run up averaging at most 2.0% in initial phases of the network. While the majority of the block reward is given to the nodes, portions are transferred to the foundation and governance to incentivize voting. Further details can be found in *Appendix I: Network Bootstrapping*.

Token Distribution

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[7]. 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 70% of the xx coins are reserved for sale or other disposition by the Company. These xx coins are intended to be disbursed or allocated to the community through public sales, private sales, auctions, and community incentivization programs by MainNet launch. 25% of the xx coins are reserved for project creators and WBM Corp. (the developer of Praxxis software) and 5% of the xx coins are reserved for the xx network ecosystem (developer awards etc.).

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 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 paid postage used on the xx network, supplemented by inflation.

Communications

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

[7] 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.

more nodes to the xx network increases messaging capacity and drives growth. As more users send more private messages, 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 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.

xx roadmap

Development of the xx network has been divided into the following phases:

- ***Internal TestNet****:* An internal prototype network of 3 nodes deployed across two continents used to develop and demonstrate the technology.
- ***AlphaNet****:* The first publicly available phase of the network. It is composed of 8 nodes across 4 continents, operated by Elixxir, Praxxis, and partner companies.
- ***BetaNet****:* a larger and more widespread network with up to 600 nodes selected through a community driven process;
- ***MainNet****:* the final implementation of the xx network, operated by thousands of globally distributed nodes chosen through xx governance.

In order to complete these phases, Elixxir, Praxxis, and the xx network plan to pursue the following timeline and roadmap:

- September 2018: Elixxir announced and TestNet demonstrated.
- January 2019: Start of the BetaNet node selection process.
- May 2019: Release of the xx collective app.
- June 2019: Announcement of the BetaNet nodes, along with the selection of 600 nodes from a pool of 870 applications.
- June 2019: Launch of the ArrowSDK developer program.
- August 2019: Announcement of Praxxis.
- September 2019: Release of the xx network AlphaNet.
- November 2019: Release of the xx messenger via the xx collective app.
- Early 2020: Planned release of the xx network BetaNet.
- Late 2020: Planned release of the xx network MainNet.

AlphaNet has been launched with 8 independently operated nodes running in 5-node teams achieving 5 to 10 seconds of latency when sending messages through the **xx messenger** dApp. The **BetaNet** node selection process ran from January through June of 2019. Elixxir first solicited community input on selection criteria via a questionnaire that received over 500 responses. The resulting node application process received 870 applications from more than 80 countries around the world. The high quality of these applications led to the selection of 600 node operators for BetaNet. **MainNet** will rely on xx governance to provide a democratic node selection process.

Smartphone users have been downloading the **xx collective** app, available on iOS and Android platforms. The app currently has over 5,000 users on its access list, waiting to experience the **xx messenger**. We are onboarding users as we test the features and capabilities of the AlphaNet, and expect to have several thousand users testing the xx messenger by the end of 2019.

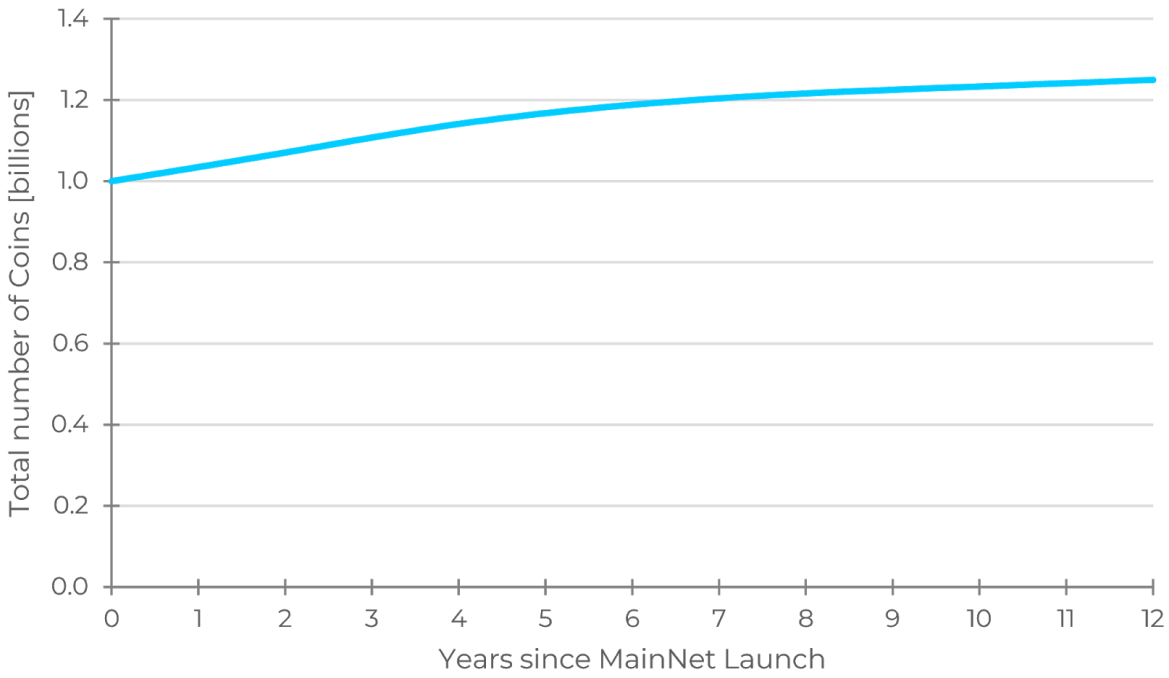
Appendix I: Network Bootstrapping

During network bootstrapping post MainNet launch, the xx network will generate growing but not yet mature levels of paid communications. In order to ensure growth incentives during this time, we propose an initial bootstrapping period with an average inflationary reward of up to 2% to supplement communications revenue.

What follows is a proposal which may change, possibly radically, by MainNet due to a variety of factors, including community input.

This initial schedule will be set in place by the creators of the network, with control given to xx governance following MainNet launch. The initial proposal includes a 9-year bootstrapping period averaging 2.0% year-over-year inflation which then transitions into a long-term inflationary model which averages 0.65% year-over-year inflation.

The following graph describes the inflation of the network as proposed over the first 12 years. The network will start with 3.4% inflation per year for 3 years and then over the course of 6 years taper down to 0.65% inflation.



This inflation graph assumes that within 3 to 5 years the network will begin accruing significant fees from paid communications. Governance will be able to modify and update the inflation tables in the event that messaging fees grow at a different rate or other economic factors are not appropriately calibrated.

Appendix II: Communications Economics

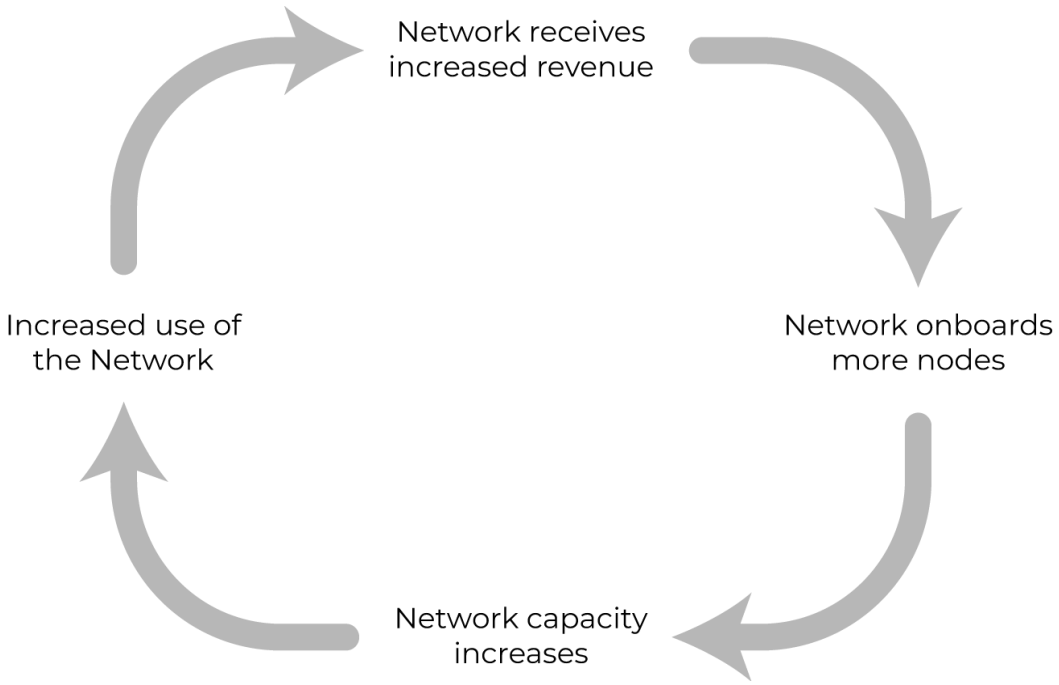
Scaling Economics

For most blockchains, security increases 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 Praxxis consensus protocol. So, as the number of nodes increased, both security and performance improve[8].

These scaling characteristics of the xx network power a virtuous cycle[9] of growth, which we believe is unique among common blockchains.



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

[8] Further Details on Elixxir scaling can be found in the *Elixxir Architecture Brief*.
[9] 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

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[10]. 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.

[10] https://www.techopedia.com/definition/29066/metcalfes-law

Free and Paid Postage

When an xm (mi**x m**essage) 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

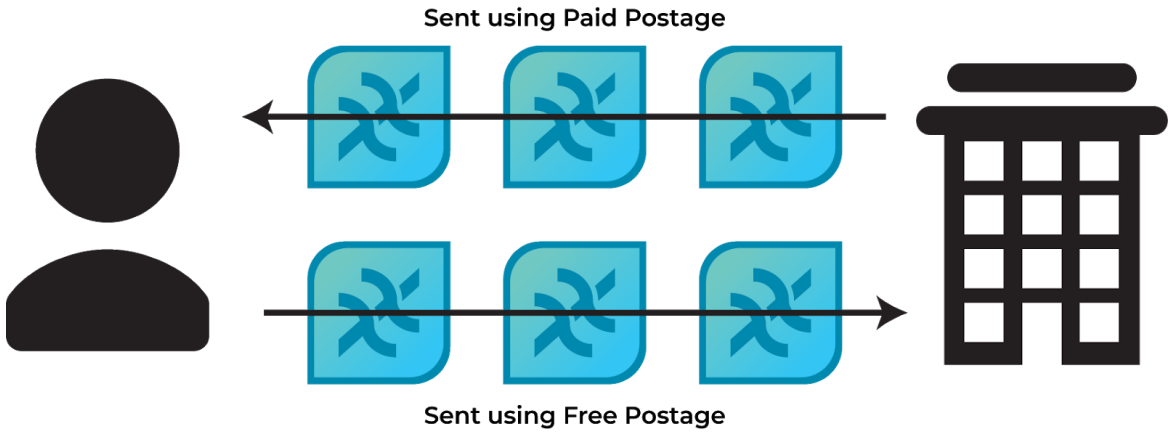
All users also have the ability to purchase paid postage in the event that all of their free postage is used up. Usually these paid messages will be needed by high-volume users such as businesses and dApps. The cost to individual paid messages is intended to be negligible.

Postage Denominations

To account for the micro-cost of sending individual messages, postage is denominated in significantly smaller denominations, a factor of roughly 1,000 to 10,000 less than the base denomination of xx coins.

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.

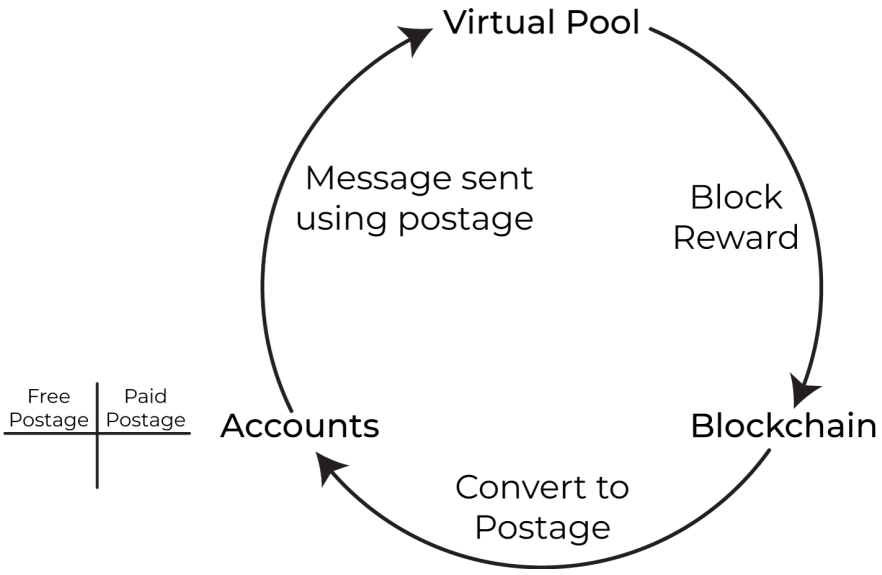
xx Coin Transaction Fees

Postage is designed to ensure the network generates revenue for payments in xx coin. Denominated payments in the xx network transfer the ownership of a series of xx coins by burning each individual spent denomination and creating a new one to replace it. This mechanism allows users to leverage the privacy of Elixxir's mixnet by sending each denomination coin transaction as a separate message, disassociating each coin from all others in the transaction.

The network limits the maximum number of simultaneous free messages an account can send, and as a result, private denominated payments will likely require the use of paid postage to be completed in a timely manner.

Ideally, fees for wallet based transactions should be commensurate with denominated transactions. This combined with their reduced privacy practically ensures wallets with comprise a minority of transactions.

Mechanics of Postage



Accounts

When sending an xm through the xx network, either the free or paid postage from the sender's account are expended to send the message. Free postage is automatically refilled at a fixed rate, while paid postage must be filled by converting denominated xx coins.

Transfers to Accounts

To convert a denominated coin to postage, a message similar to a normal payment is sent. Instead of using the coin's keys to sign and transfer the value to a new coin, the coin's keys sign a user account, transferring the value into that account.

Sending a Message

When sending an xm, postage is deducted from either free or paid postage accounts. These deductions are authorized by the entire team through the same authorization mechanism used to send the message. The value of the paid postage is added to the **virtual pool**.

Virtual Pool

The Virtual Pool is a count of postage that has been used to send messages in the network but has yet to be converted back to xx coins and paid as block rewards. As distinct from the xx coins themselves, this pool can be thought of as a sort of internal measure of account for postage.

The pool acts as a buffer. It will be used to pay a node's block reward not based upon the specific revenue generated in the round that node itself participated in, but rather based upon an average over a set window. This aligns the node's incentives with the network's, ensuring they violate the free/paid dependency for their own gain at the expense of medium and long term network revenue.

Appendix III: 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 BetaNet are as follows:

- Modern High-End Consumer grade CPU (8 physical/16 logical cores)
- 64GB RAM
- 2TB SSD storage
- Mid-Range modern GPU with 32-bit Mul Units (Example: Nvidia GeForce RTX 2070)
- 1Gbps 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 bootstrap inflation numbers have the goal of supporting 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.

These specifications are currently in line for the expectation for MainNet with the exception that MainNet is projected to require increased storage capacity.