COLOSSUS XT

The Consumer's Privacy Coin

A Proof-Of-Stake 3.0 Privacy-based Cryptocurrency

GreenPaper

Version 1.1
"Spread the Grid"

This paper is a living document. It will develop alongside COLX and Colossus Grid. Please check back for updates.

Abstract

In this whitepaper, we are introducing Colossus XT (COLX) as a privacy-enabled cryptocurrency for the everyday user. Currently, COLX features a number of technologies that benefit users' privacy and/or the participation of small individual investors in the COLX network – such as obfuscation and a see-saw rewards mechanism for staking nodes and masternodes. The paper will also outline future developments in COLX designed to further enhance its usefulness to individuals and small businesses – most importantly, a decentralized marketplace and Colossus Grid, a decentralized grid computing framework.

COLX is built upon PIVX, which itself is built upon the popular DASH cryptocurrency. While their lineages can all be traced back to the original Satoshi Core, each project has chosen a particular direction with goals and ideals that represent the communities they serve.

The COLX blockchain was designed from the outset to provide a privacy coin for the everyday user. COLX's goal is to facilitate customer-to-customer (C2C) and business-to-customer (B2C) transactions of low to medium payment sizes.

Current features of COLX that make it distinctly suited for this purpose are:

- A **large supply** of more than 10 billion coins, enabling a lower-than-1:1 split with major fiat currencies such as USD and EUR.
- Therefore the ability to **determine prices for everyday items** without juggling decimal places.
- **Low to zero transaction fees** (also see section "Zero-Fee").

With an eye on the horizon, COLX is developing two novel services to fulfil its mission:

- **Colossus Grid**, a decentralized, distributed grid computing framework
- **A general-purpose decentralized marketplace**

In addition to C2C and B2C transactions for customers and small businesses, COLX also offers a significant opportunity for the individual crypto investor in particular, as opposed to “whales” and high net-worth individuals that dominate most cryptocurrency infrastructures.

- The COLX network, due to its relative novelty, currently has **fewer masternodes** than other comparable networks, thus offering a **higher return-on-investment (ROI)** even for modest investments in masternodes.
- COLX is developing a **Shared Masternodes** technology (see section “Shared Masternodes” below), which will allow small investors to pool their funds in order to run a masternode with shared expenses and shared revenues, thus **lowering entrance barriers to this profitable niche.**

COLX is supported by a dedicated team that welcomes new supporters of any background. Find more information at Colossuscoinxt.org.

Acknowledgements

Colossus XT would not have been possible without the prior works of the respective Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash and PIVX teams. Open source software and its contributors are constantly paving the way toward new and exciting innovations. When information and knowledge are free to build upon, society as a whole benefits. We are grateful to our predecessors for the opportunity to contribute to this
growing ecosystem.

What Are Cryptocurrencies – and Why Are They Not Private?

The Birth of Bitcoin

The history of cryptocurrencies starts in the year 2009. Satoshi Nakamoto – a single researcher or, more likely, a group of anonymous researchers that have not been identified to date – published their seminal paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” .

In it, they presented not only the concept of the world’s first cryptocurrency called Bitcoin, but introduced the technology that has since been the basis of almost every cryptocurrency: The blockchain.

The Blockchain

The blockchain is a solution to the most severe problem of digital currencies: The fact that any digital information can be copied identically for almost no cost at all. In an ecosystem in which participants do not trust each other, each participant is tempted to spend their money multiple times – the so-called “double spending problem”.

In traditional economies, this problem is addressed by the existence of a third-party authority, for example each country’s central bank in charge of fiat money creation, or consumer banks making sure that each dollar in a customer’s checking account can only be spent once.

This dependence on third-party authorities, however, has its drawbacks: It grants those authorities significant power which they can use and abuse. For example, banks might decide to freeze an individual’s
or company’s account on the mere suspicion of illegal activity, instead of waiting for legal proof.

Cypherpunks

In the global hacker scene, there have long been currents of libertarianism whose proponents want to minimize the power that nation-states wield over individuals. Those have led to the development of the cypherpunks movement – activists who promote cryptography and related tools to protect the individual's freedom and privacy from spying eyes of governments and agencies . Arguably, this movement has finally led to the development of the first cryptocurrency, Bitcoin – the first truly decentralized currency that promised independence from central and other banks, especially in a time when trust in the banking system was even more eroded than usual.

Hashing and Proof-of-Work

Ironically, the double spending problem is solved in Bitcoin in a way that is detrimental to privacy; it heavily relies on transparency. To be concrete, any cryptocurrency transaction becomes valid only once it has been made part of a block on the blockchain. And the blockchain is exactly what its name suggests: A chain of sequential blocks.

Through a series of hashing functions , the transactions within a block and the sequence of blocks are protected against tampering, or more accurately: Such tampering is easily detected and therefore rejected
by the community.

The blockchain is stored not on a single server, but on each server in the network of participating peers. Each peer can build new blocks out of new transactions that are available in the network – in fact, this mining activity is encouraged by rewarding the successful miner with an amount of Bitcoin for the respective block. This means that naturally, the blockchain can diverge into several branches, but it only has one single valid branch: The longest.

A Bit of Game Theory

To make sure that a malignant participant of the network cannot make his own chain, containing fraudulent transactions, the longest in the network, Nakamoto recycled a concept that had first been suggested to fight spam in the worldwide e-mail network: Proof-of-work.

In proof-of-work, in order to create a valid new block, the miner has to solve a completely useless mathematical puzzle, whose main feature is the fact that it is difficult and therefore consumes a considerable amount of time and energy. Thus, from a game-theoretical point of view, the cost of falsifying the blockchain soon exceed the potential gain. This principle is also reflected by the recommendation to wait a larger number of new blocks for confirmation of a high-sum transaction than for a low-sum transaction .

Transparency vs. Privacy

Proof-of-work, together with the other Bitcoin features described above, make up the so-called consensus mechanism of Bitcoin. This is the element that replaces trust or third-party authority in an
decentralized system.

This consensus mechanism only works if all participants of the peer-to-peer network have the ability to check each other's transactions and blocks. Therefore, transaction details are openly visible for network participants and, because Bitcoin's blockchain is public, for the whole world.

Pseudonymous and Anonymous Transactions

Of course, Bitcoin transactions do not contain the sender's or recipient's real name, as would be the case with a traditional bank transfer. Instead, only Bitcoin addresses, which are derived from the Bitcoin participant's public key, become visible. Therefore, the public address of a participant can be understood as their pseudonym in the network – Bitcoin is not anonymous, but pseudonymous.

This is an important distinction: Truly anonymous transactions can never be traced back to their origin. In other words, the individual who signed the transaction can never be identified. Pseudonymous transactions, on the other hand, are identifiable as soon as information from more than one source can be linked.

If a Bitcoin address is used more than once, an observer could triangulate the information included in different transactions to identify the individual who owns the Bitcoin address. Many modern wallets solve this by creating a new address for every transaction. However, once a Bitcoin user chooses to use an address more than once – for example by posting it on a website to accept donations – it is potentially identifiable.

And, of course – fiat/coin exchanges and internet service providers potentially know all of their users' Bitcoin addresses as they are able to link them to bank accounts and IP addresses, respectively.

The good news: Privacy-friendly cryptocurrencies exist.

Colossus XT (COLX) – A Privacy-Enabled Cryptocurrency

Since the inception of Bitcoin, cryptographers and blockchain developers have been working on protocols that enable truly anonymous transactions. This opened the doors for a new class of cryptocurrency: Privacy-enabled cryptocurrencies.

In this whitepaper, we are introducing Colossus XT (COLX) as a privacy-enabled cryptocurrency powering Colossus Grid, a decentralized grid computing framework.

A Solid Foundation

Every home needs a solid foundation, and COLX is no different. COLX is built upon PIVX , which itself is built upon the popular DASH cryptocurrency. While their lineages can all be traced back to the original Satoshi Core, each project has chosen a particular direction with goals and ideals that represent the communities they serve. We will extend, and place emphasis on, the privacy coin features of our predecessor platforms by exploring new technologies, while creating tool sets and opportunities for COLX's integration into present day technology platforms.

Why COLX?

COLX is not the world's first privacy-enabled cryptocurrency. So why are we developing COLX as a new project, instead of contributing to DASH, PIVX or others?

Like any new cryptocurrency worth its salt, COLX builds upon the solid foundations laid by its predecessors, but will introduce new features that they are missing.

In the case of COLX, these crucial new features are:

- **Colossus Grid**, a decentralized, distributed grid computing framework
- **A general-purpose decentralized marketplace**

In particular, the COLX blockchain was designed from the outset to provide a privacy coin for the everyday user. COLX's goal is to facilitate customer-to-customer (C2C) and business-to-customer (B2C) transactions of low to medium payment sizes.

With these goals in mind, COLX has been designed with:

- A **large supply** of more than 10 billion coins, enabling a lower-than-1:1 split with major fiat currencies such as USD and EUR.
- Therefore the ability to **determine prices for everyday items** without juggling decimal places.
- **Low to zero transaction fees** (also see section "Zero-Fee").

In addition to C2C and B2C transactions for customers and small businesses, COLX also offers a significant opportunity for the individual crypto investor in particular, as opposed to "whales" and high net-worth individuals that dominate most cryptocurrency infrastructures.

- The COLX network, due to its relative novelty, currently has **fewer masternodes** than other comparable networks, thus offering a **higher return-on-investment (ROI)** even for modest investments in masternodes.
- COLX is developing a **Shared Masternodes** technology (see section "Shared Masternodes" below), which will allow small investors to pool their funds in order to run a masternode with shared expenses and shared revenues, thus **lowering entrance barriers to this profitable niche.**

Future services of COLX that will further contribute to its usefulness especially to individuals and small businesses will be discussed further below (see “COLX Upcoming Features”).

Why do we think that COLX is the necessary next step in the evolution of privacy-friendly cryptocurrencies? In order to answer this question, let us explain the vision behind COLX.

COLX: The Vision

Like a linked chain, COLX relies on the strength and abilities of each of its team members – even more so in the near future as we begin to tackle the implementation of Colossus Grid: A demanding project in which all of us will strive to fulfil a higher purpose.

COLX Core Principles

As a team, we have adopted certain core principles that guide our work:

- We believe in **empowerment of the individual**, and of communities.
- We believe in the **right to free speech**, and in the **freedom to conduct commerce** as a core component of that right. This can take many forms, whether it is the freedom to contribute to a cause, to buy and sell products and services, to raise money through crowdfunding, or to run a business that has value to your customers.
- Using blockchain and related decentralized technologies, we want COLX to **help individuals and communities take back economic power**, and achieve their goals more efficiently and with greater independence, and without the compromises of needing to give up data and being subject to control of corporations and other centralized groups.

COLX Goals

The overarching goal of the COLX community is to provide a private, community-based cryptocurrency and blockchain platform that forms the foundation of free and sustainable decentralized commerce.

This goal not only includes the core blockchain, but all related applications and ventures constructed on top of the platform. In addition to conforming to our guiding principles, COLX technology will also be heavily oriented towards utility and efficiency, for example:

- Scalability, speed, security and reliability of transactions
- The option to decide between private and transparent transactions
- Adequate rewards for participation in the COLX network and Colossus Grid
- Widespread accessibility and ease of use

The last of these – accessibility and ease of use – are essential elements of our vision:
COLX is a technology for everyone – not just those with advanced technical skills.

COLX will be easy to acquire and exchange for goods and services globally, with the ability to provide a smooth and intuitive user experience for people around the world.

The prime application of COLX that makes it attractive for everyday use will be its integration with a fully decentralized marketplace. There, users will be able to buy and sell resources using COLX as a means of payment – transparently or privately, according to their own choice.

The marketplace will be the foundation of a thriving ecosystem of COLX applications and businesses – built both by the COLX development team and the COLX community.

Participation in the COLX ecosystem is free and permissionless – no central authority involved. Changes and improvements to the COLX core code will be made by the COLX community, for the COLX community.

All of the implementation decisions of COLX have been determined by our principles as described above. In the following sections, we will present them in greater detail.

COLX Overview

COLX started out as a proof-of-work (PoW) cryptocurrency based on a Quark algorithm. It originated from ColossusCoin V2 (CV2). 12 billion coins were generated in the genesis COLX block (PoW) to allow for a 1:1 coinswap from CV2. No coins were pre-mined and kept by the development team.

After termination of the PoW phase, COLX has transitioned to a proof-of-stake (PoS) consensus mechanism based on a masternodes network architecture (more about masternodes below).

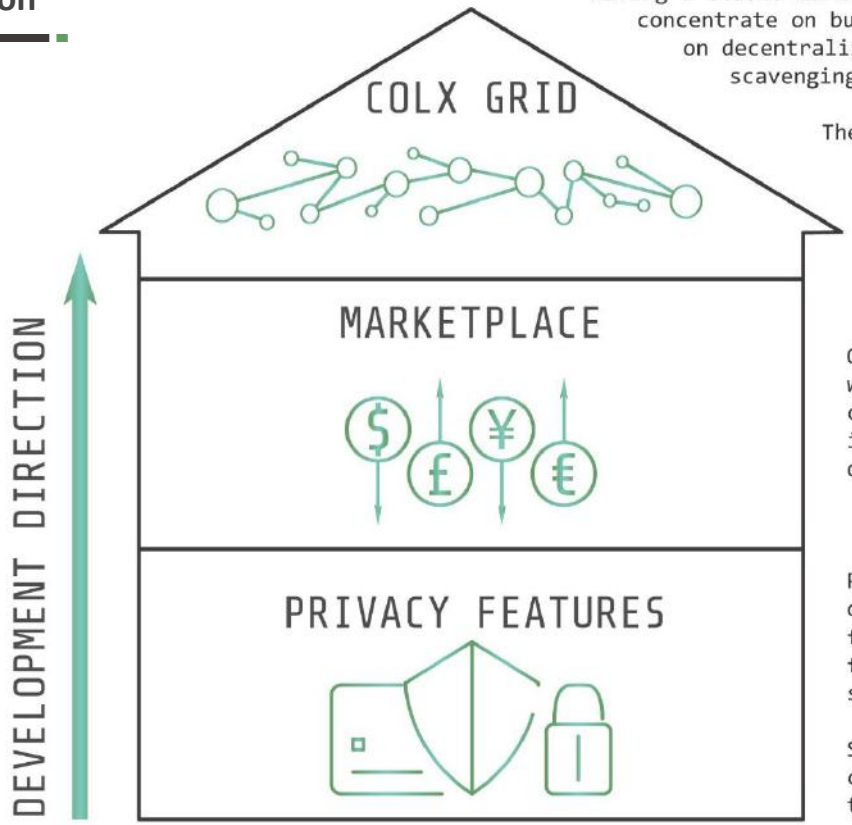
Coin Details

Ticker	COLX
Block Time	60 seconds
Block Size	2 MB
Current Supply	10,829,566,033 COLX
Maximum Supply	No maximum, Supply increases by 1250 through block 302,399, then by 1000 forever
Coin Supply Control	All transaction fees are burnt from coin supply
Minted Confirmations	90
Transaction Confirmations	6
Transaction Fee	10 COLX / kb. Zero fee send available
Stake Minimum Age	7 days
Masternodes	10,000,000 COLX per Masternode
Port	51572

COLX Features

COLX aims to preserve and improve all features of its predecessors that are privacy-friendly and encourage a truly decentralized ecosystem, while introducing new features to power its decentralized marketplace and the Colossus Grid project.

ColssusXT Vision



Having a stable marketplace will allow us to concentrate on building the grid which will focus on decentralized storage and compute cycle scavenging.

The decentralized marketplace will allow an avenue for users to buy and sell their unused device resources managed by the grid all while riding on the backbone of a world class privacy coin blockchain.

Once we have a secure and private way for users to utilize COLX we create the ability to buy and sell items and services using the decentralized marketplace.

Privacy features and the evolution of the network are the foundation for building the COLX brand. All future COLX features require this solid foundation.

Starting here we ensure that users can have a secure and private way to utilize COLX.

These features will be presented in detail below.

Consensus Mechanisms

PoW-based blockchains are not only energetically inefficient and thus environmentally questionable, they also show a clear tendency towards centralization inconsistent with blockchain technology's underlying philosophy of decentralization. In short, the economic model behind PoW favours large mining farms in countries with cheap energy and/or cold climates, rather than incentivizing mining equally for individuals all over the network.

Of all alternative consensus models, PoS is the one with the longest track record in theory and in real-world applications. In contrast to PoW, described earlier in this paper, PoS is not based on finding solutions for hard, but essentially useless, mathematical problems. Rather, a node's eligibility to determine the next valid block depends on this node's "stake" in the network. In general, in PoS architectures, the amount of coins controlled by this node and/or the coins' age, sometimes with an element of randomization.

PoS therefore has a different incentivization structure: While miners in PoW currencies often hold a larger amount of coins themselves, but are not required to do so, they may or may not be intrinsically motivated to keep the network and consensus mechanism stable. In PoS, the consensus mechanism is guarded by those who own a considerable proportion of the currency, or in other words, of those who have much to lose if the consensus mechanism fails.

Specifically in COLX and its predecessor PIVX, PoS is implemented with a masternodes network architecture. Masternodes were pioneered by DASH; however, DASH combines them with a PoW algorithm, while COLX and PIVX have abandoned their PoW after mining of the total coin supply was completed. COLX's PoW phase was based on the Quark hashing algorithm.

Proof-of-Stake (PoS) 3.0 in COLX

COLX operates with a PoS consensus mechanism, meaning that anyone who can prove they hold COLX can help secure the network, i.e., has a chance to create the newest block.

Unlike for masternodes (see below), there is no barrier to entry in the form of high collateral funds. Staking participants only need to prove that they own a minimum of 1 COLX. This proof is delivered by locking up a certain amount of COLX into a deposit. Any participant who does this is considered a validator, and the network of validators then participate in the consensus algorithm. The likelihood of each node being chosen to confirm a block and receive the associated staking reward is based on the number of COLX being staked by this node. Thus, even when staking just a small amount of COLX, the likelihood of being chosen for a block is very low indeed, but not zero.

COLX utilizes Proof-of-Stake version 3.0 to protect the community against attacks based on coin age that used to be possible in earlier versions of PoS. In PoS 3.0, coin age has been removed completely from the consensus process.

Masternodes and Staking

Interconnected masternodes are the backbone of the COLX network.

The purpose of masternodes in the COLX network is the processing of transactions, thus aiding in the creation of new blocks; for this, they receive block rewards. In addition, they perform certain services for COLX participants (more on these below). Regular participants in the COLX network also discover new blocks and are rewarded accordingly; however, they don't offer the additional services that masternodes do.

In order not to tilt the distribution of block rewards in an unfair manner that favours either masternodes or regular staking participants, block rewards are balanced with a so-called see-saw mechanism (see below). By balancing block rewards in this manner incentivizes the creation of new staking nodes when masternodes are overrepresented in the network, and the creation of new masternodes when staking nodes are overrepresented.

Regular staking participants merely need to run a wallet software which proves that they have coins in the wallet. For their participation in staking as a so-called staking node, they are then rewarded with
block rewards.

Additional Services Provided by Masternodes

In addition to transaction confirmations, masternodes provide the following services that are crucial to the functioning of the COLX network:

- Decentralized budgeting system with immutable proposal and voting systems
- Coin mixing (obfuscation) to enable truly private transactions
- Instant transactions (SwiftTX)

They will be explained in detail in later sections of the present paper.

How to Establish a Masternode

Any COLX network participant can set up a masternode.

In order to do so, this participant's COLX wallet must contain at least a balance of 10,000,000 COLX. Exactly this amount is then locked as collateral in a transaction that is paired with the masternode.

The masternode itself can be set up to run on a Virtual Private Server (VPS) in the cloud, or at home on a PC or even a Raspberry Pi, if certain technical conditions are met, such as a static IPv6 address. COLX masternodes support IPv6.

For those participants who desire additional privacy, the setup of masternodes using Tor/Onion routers is another option.

Once the masternode is set up, it will keep operating even if the wallet containing the 10,000,000 COLX is offline, potentially even in cold storage, providing additional security to the masternode owner.

The owner of a masternode is free to terminate the service of their masternode at any time, and reclaim their locked collateral funds of 10,000,000 COLX.

Masternode Economy

Since masternode owners perpetually receive a portion of the block rewards, the maintenance of masternodes can be an attractive business model in which some initial setup effort and some ongoing oversight are rewarded with a largely passive income stream, comparable to the maintenance of a rental property.

As of this writing (3/5/2018), there are about 200 active masternodes operating in the COLX network. This amounts to about 2 billion COLX locked as masternode collateral, decreasing the circulating supply from ~10.8 billion to ~8.8 billion COLX.

The return on investment (RoI) for a masternode owner based on these conditions is about 20% per annum. These numbers will change as masternodes are added or removed from the COLX network, and as block rewards gradually decrease over time at specified block intervals.

As the barrier to entry for COLX masternodes will increase over time, due to likely price appreciation, one of our main goals is to deliver a **Shared Masternodes technology** which permits smaller investors to pool their coins in a trustless and secure way, and collectively reap the benefits of providing network services.

This new COLX masternode technology will expand the capabilities of the backbone infrastructure supporting the network, and will ensure that it is capable of handling the transaction loads and data storage requirements of a mass-market user base

In summary, the maintenance of masternodes offers the following tangible and intangible perks to their owners:

- Participation in COLX governance and the security of the COLX network
- Masternode rewards
- Commodity option for future sales

See-Saw Algorithm for Masternode and Staking Rewards

Cryptocurrencies in which a high proportion of total coin supply is locked in masternodes suffer from certain problems: Low liquidity and significant price volatility. As COLX is in its essence not a scheme to obtain passive income through masternodes, but aims to be a fully functional and liquid cryptocurrency with a multitude of practical applications and high transactability, it follows a strategy to prevent that locked-in collateral funds in masternodes are incentivized too highly.

This strategy is known as the **see-saw algorithm for reward distribution.**

Reward Distribution

Phase	Block Height	Reward	Masternodes & Stakers	Masternodes Proposal Budget
Phase 1	1081 - 151,200	2500 COLX	90% (2250 COLX)	10% (250 COLX)
Phase 2	151,201 - 302,399	1250 COLX	90% (1125 COLX)	10% (125 COLX)
Phase 3	302,400 - Infinite	1000 COLX	90% (900 COLX)	10% (100 COLX)

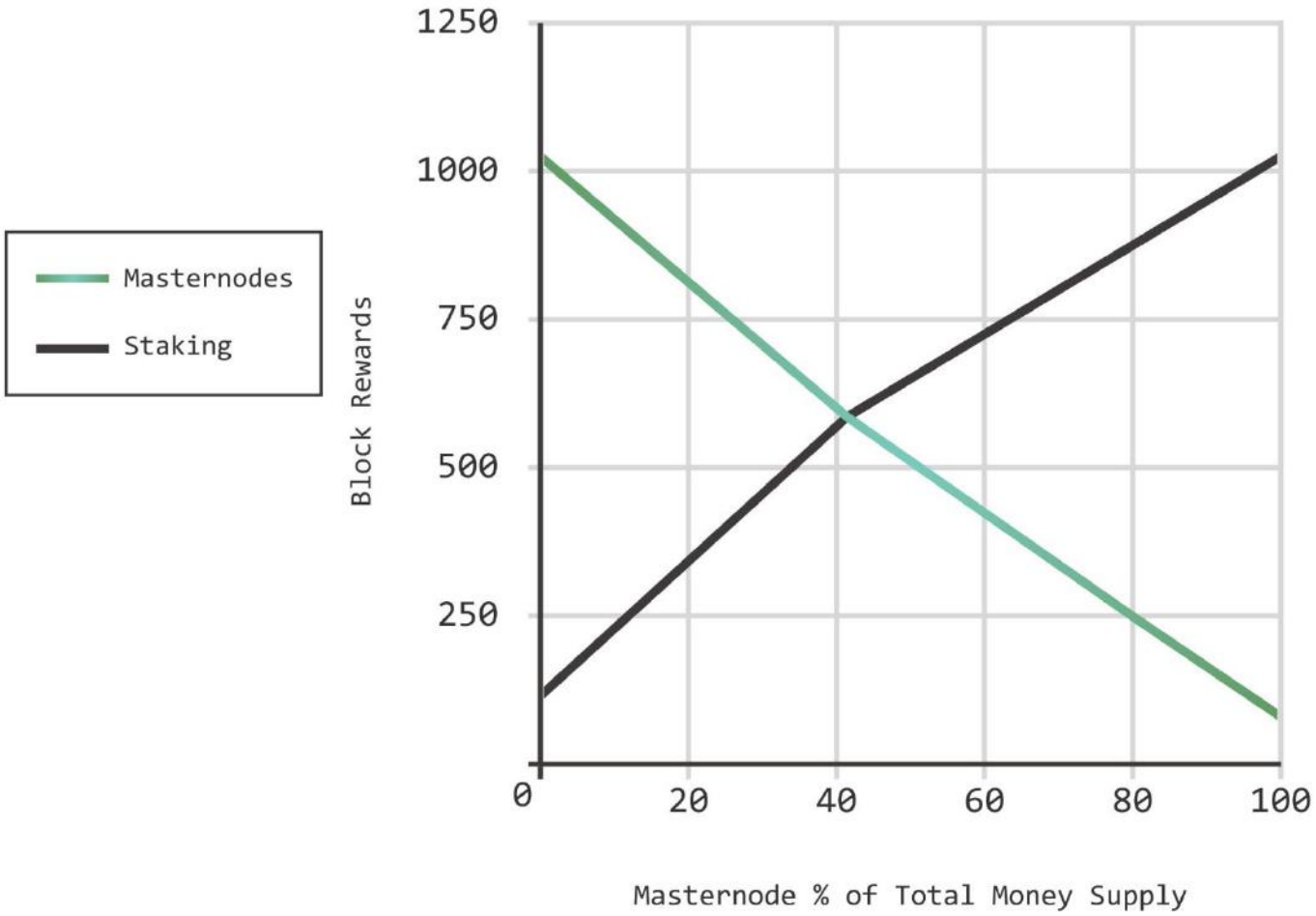
As the chart shows, block rewards decrease with block height in order to implement decreasing inflation of COLX.

From each COLX PoS block reward, 10% are dedicated to the budgeting system (COLX development and governance), and 90% to staking rewards. The Seesaw Reward Balance System then dynamically determines how exactly these 90% are distributed between masternodes and staking nodes.

Essentially, the see-saw algorithm is based on the following principle: An increasing masternode count leads to a smaller portion of the reward being paid out to masternodes, and accordingly to a higher portion of the reward being paid out to regular staking nodes – and vice versa.

With an increasing number of masternodes, the see-saw algorithm disincentivizes the establishment of even more masternodes because it lowers their profitability. To be precise, as soon as more than 41.5% of the total COLX coin supply is locked in masternodes, more than 50% of the block reward will be distributed to regular staking nodes. As long as the amount of locked collateral funds is below the threshold of 41.5%, the see-saw algorithm makes sure that running a masternode is financially more attractive than running a simple staking node, to compensate for the additional effort that a masternode requires in comparison to a simple staking node.

Reward Breakdown



Decentralized Governance And Masternode Voting

COLX aims to be a vibrant platform on which a variety of user-initiated projects live. In order to make the platform adaptable to the needs of the community, COLX utilizes so-called superblocks: These blocks are created once a month and are a singularly important vehicle for the community to control decisions regarding development, online presence and policies: They contain community members' proposals.

Basically, in these proposals members suggest how the 10% of the block rewards that are reserved for these purposes should be spent. The content of a proposal can span one or several budgeting cycles of 30 days.

Anyone can submit a proposal for a transaction fee of 1000 COLX, which are burned after submission, regardless of the community's decision towards the proposal. All submitted proposals are then voted on in the superblock. Only masternodes have the right to vote, and in order for a proposal to be accepted, it needs to earn the approval of 10% of masternodes.

An accepted proposal can be submitted to the blockchain via the relevant developer for an activation fee of 1000 COLX. The author of the proposal can apply for reimbursement of both the submission and activation fees inside the formal proposal; of course, this can only be granted if the proposal is accepted.

In order to improve chances of success for a proposal, it is recommended that the author first seek informal discussion and suggestions from other community members. They can then formulate a pre-formal proposal and post it for open discussion in the COLX forum. After all suggestions have been thoroughly considered, the final proposal can be submitted to the superblock as described above.

Instant Send (SwiftTX)

SwiftTX permits COLX users to have their transactions instantly confirmed and spendable. This is achieved by giving the masternodes special authority to confirm transactions without waiting for the rest of the network.

In detail, when a SwiftTX transaction is sent to the network, a number of masternodes are randomly chosen to process this transaction. If they find the transaction to be valid, they instantly transmit the originating addresses of the funds that are being spent to the rest of the network. The funds are therefore locked against double-spend. This allows the masternodes to confirm the transactions instantly without opening the doors to double-spending. At the next convenient point in time, the transactions will be incorporated into the blockchain.

SwiftTX has been adapted from PIVX and is based on Dash's InstantSend function.

Obfuscation

In order to enable truly private transactions, COLX features Obfuscation as an adaptation of the CoinJoin procedure known from Bitcoin, originally proposed by Gregory Maxwell. Like SwiftTX, the Obfuscation feature as well is offered as a special service by the network of masternodes.

The Obfuscation process is basically a decentralized coin mixing procedure. It is based on the principle of mixing coins held by more than one participant, so that none of the coins can be tracked back to their original holder. In order to achieve this, funds in the COLX wallet are broken down into standard denominations. The wallet sends a message out to the COLX masternodes, indicating that funds are waiting to be obfuscated. As soon as several users (e.g., User A, User B and User C) indicate the same request for obfuscation of the same denomination (e.g., 1 COLX), the respective masternode collects the addresses at which the funds for obfuscation currently reside.

The masternode then combines these information in a new transaction that says: Send 1 COLX from User A to User B, 1 COLX from User B to User C and 1 COLX from User C to User A (of course, not limited to three users – the more participants, the better). Each of the users has created a new receiving address explicitly for this purpose.

Since the masternode does not have access to the users' private keys, it sends the transaction back to the users' wallets, where it is then signed by all participants, and can thus be executed.

Essentially, the users have now swapped a standardized denomination of coins among themselves so that tracing the coins' ownership becomes significantly more difficult for an attacker. During all of this, the masternode never takes possession of the coins.

Because all of this takes place while the coins are at rest in the wallets, they are already obfuscated when the user wants to perform a new transaction – there is no additional waiting period required.

Zero-Fee

Currently, to balance network loads more evenly, the COLX blockchain allows for free transactions if a block would go unfilled otherwise. Confirmations using this technology may take longer than usual.

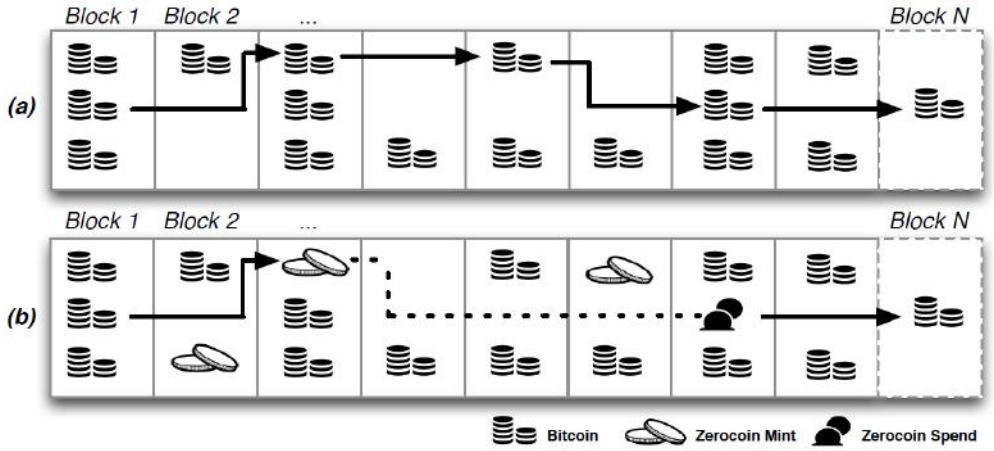
COLX Upcoming Features – Short Term

Zerocoin Protocol

In order to offer COLX's community an easy-to-use option to conduct truly private transactions, COLX will replace the obfuscation feature (see previous section) with the Zerocoin protocol, an even more elegant way to prevent backtracking of transactions.

Zerocoin has been developed by an independent group of researcher from the Johns Hopkins University of Baltimore.

It is based on the idea that during the chain of transactions in which regular coins are spent, so-called zerocoins are minted and spent instead of regular coins so that the coins, in the end, cannot be traced back to their addresses or transactions of origin **(see figure).**



a) Normal Bitcoin transaction history, b) Zerocoin chain. Source: Original Zerocoin publication at https://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf.

Zerocoin and regular COLX transactions exist in parallel: In cases in which anonymous transactions are not required, users may continue to trade regular COLX coins. Anonymous transactions will be performed in zCOL coins.

Shared Masternodes

Experiences with cryptocurrencies preceding COLX have shown that masternodes are likely to show price appreciation with time, especially in the current economic climate. This has raised the barriers to entry for smaller investors who would like to seize this investment opportunity in spite of their limited funds.

COLX is developing a solution to this problem: Shared Masternodes technology, which permits smaller investors to pool their coins in a secure and trustless way, and collectively reap the benefits of providing network services specific to masternodes.

Besides its benefit to the individual investor, Shared Masternodes also contribute to the strength of the COLX network: They incentivize participation of individuals, which poses a counterweight to the centralization of power in the hands of extremely affluent individuals or organizations that has often been observed in other permissionless blockchains.

Shared Masternodes will in time become an additional node layer on the COLX network, one that is available to a broader range of COLX investors than any singular masternode. This will create a three-tiered structure of staking nodes (personal wallets), Shared Masternodes and Full Masternodes.

Initially, Shared and Full Masternodes will have similar sets of features. Experiences with Shared Masternodes in the COLX network and feedback from the COLX community will determine whether or not they will develop distinct capabilities that differ from Full Masternodes.

Wallets

As we believe that COLX is the people's coin, one part of the COLX vision is to make COLX available to as many people as possible, and to be easy to use. To that end, two new mobile wallets will be introduced in 2018: The Android lite wallet and the iOS lite wallet. Existing desktop and web wallets will be refined further, as described below.

Android and iOS Lite Wallets

The Android Wallet will be a mobile wallet available for download from the Google Play Store. In order to address the significant proportion of COLX's user base who prefer Apple computing, an iOS wallet is in development as well, to be available from the App Store. Both will provide a secure and speedy mobile connection to the COLX blockchain and provide all necessary features for a lite mobile wallet: Sending, Receiving, History, and Balance.

Both lite mobile wallets will soon be equipped with two-factor authentication (2FA) for added security.

In-Wallet Masternode Voting and Proposal System

An upcoming update of the desktop wallet will incorporate a transparent COLX blockchain viewer for the first time, to show COLX budget proposals, voting, and status of the budget process. This is important to the longevity of COLX because the proposal system is vital to the funding of COLX projects and community participation in general.

Masternode holders will be able to easily perform all COLX governance functions from within the wallet's graphic user interface. This will eliminate the need to vote from the web or from the debug console.

Web Wallet

The web-based wallet will provide a platform to host COLX wallets online as a more convenient option for people to store COLX without having to run a full COLX wallet on a personal computer or mobile device. As another lite wallet, it will support the same functions as the mobile lite wallets: Sending, Receiving, History, and Balance.

COLX Upcoming Features – Medium Term

Marketplace

As the consumer's privacy coin, one of the central upcoming features of COLX is a decentralized, privacy-friendly marketplace for peer-to-peer commerce. This marketplace will be powered by COLX as its major currency and will not impose platform fees or other restrictions to free commerce, thus benefiting individuals and small businesses in particular, who do not have the same scaling advantages that enable larger businesses to cope with high platform fees and other charges.

Right now, e-commerce heavily relies on centralized services such as eBay and Amazon. They have restrictive policies, charge high fees and, in summary, create an asymmetrical relationship between themselves and sellers on their platforms that is heavily tilted to favour themselves. In addition, they decline to do business with anyone who does not have access to their preferred means of payment, and they collect personal information, putting users' privacy at risk.

The COLX marketplace will use a different approach to online commerce. It will put the power back in the users' hands. Instead of buyers and sellers going through a centralized service, the COLX marketplace will connect them directly. Because there is no one in the middle of your transactions there are no fees, no restrictions, no accounts to create, and you only reveal the personal information that you choose.

As soon as Colossus Grid (next section) is sufficiently advanced, the marketplace will be tied into it, allowing users not only to sell and buy goods and services, but unused computing resources as well.

I2P Adoption

I2P is an anonymizing network that uses a fully decentralized peer-to-peer model. It is much faster, more secure, and more robust than its better known counterpart Tor.

I2P was originally built to provide hidden services which allow people to host servers at unknown locations, and it provides many of the same benefits that Tor does. Both allow anonymous access to online content, make use of a P2P-style routing structure, and both operate using layered encryption. However, I2P was designed to be a network within the internet with traffic staying contained in its borders. Thus, traffic inside the I2P network is significantly more secure than Tor traffic, which is vulnerable to certain known ways to identify participants (and has been co-financed significantly by the US government).

I2P performs packet-based routing as opposed to Tor's circuit-based routing. This has the benefit of permitting I2P to dynamically route around congestion and service interruptions in a manner similar to the internet's IP routing, providing a higher level of reliability and redundancy to the network itself. Additionally, I2P does not rely on a trusted directory service to obtain route information. Instead, network routes are formed and constantly updated dynamically, with each router constantly evaluating other routers and sharing what it finds.

Finally, I2P establishes two independent simplex tunnels for traffic to traverse the network to and from each host as opposed to Tor's formation of a single duplex circuit. This provides the additional benefit of only disclosing half the traffic in the case of an in-network eavesdropper.

In the future, an I2P cloud will be an important building block of COLX's Colossus Grid described below.

COLX Upcoming Features – Long Term

Colossus Grid

COLX, as you have learned in the past sections, comes with a number of useful features to power a decentralized and privacy-friendly economy. However, the most innovative and unique feature of COLX currently in development – and the one that the team is most proud of – will be presented in this section.

Colossus Grid is based upon several of the features described in this document that are essential to COLX's mission of becoming the consumer's privacy coin – most importantly, I2P and the Zerocoin protocol. It will combine grid computing with decentralized storage features and thus make resources available that now sit unused on the computers of thousands and millions of potential users around the world.

What Is Grid Computing?

Grid computing combines computers from multiple administrative domains to reach a common goal, or to solve a single task .

Machines may collaborate in a grid regardless of their physical distance; they can be connected by a local or a wide area network. Grids are not limited to certain types of machines either; they can integrate mainframes, personal computers and even smartphones.

In a grid, these machines solve tasks as a single computer. This can be (but does not have to be) achieved by parallel computing, for which special kinds of algorithms are necessary to divide computational tasks in a way that they can be processed more efficiently in parallel.

In short, grid systems offer the following two main benefits over centralized systems:

- Scalability - The system can easily be expanded by adding more machines as needed.
- Redundancy - Several machines can provide the same services, so if one is unavailable, computing processes can continue nevertheless.

Grid systems are vendor-independent and can use a variety of standards-based software components. Such systems are independent of the underlying software. They can run on various operating systems, though of course open-source software is preferable in a decentralized context, and can use various communications protocols such as SNA or TCP/IP.

In detail, Colossus Grid – as most grid computing projects – will utilize a cycle-scavenging model. Here, the unused resources in a network of participants (when the user is away or the machine is waiting for user input, even in the scale of less than a second on fast devices) are combined to a grid model and made available to others who need computing resources.

What Is Decentralized Storage?

Analogous to the grid computing model described above, in decentralized storage unused resources that sit on network participants' computers are made available to other participants, thus using the available resources more efficiently.

In order to achieve this in a fast and privacy-friendly manner, data for storage is broken up into individual pieces, each of which may be stored on a different machine. The files are integrated again only upon recall by the owner (storage renter). This is done redundantly on different machines in the network to make sure that even during availability problems of one or more machines, files are still accessible.

Data owners' privacy is preserved by encryption to which only the data owner holds the private key.

What Is Colossus Grid?

Colossus Grid is a novel, privacy-friendly grid computing and decentralized storage framework.

There are a couple of recent developments that are calling for new ways of computing and storage:

- Ever more huge data sources are contributing to our view of the world. Potentially, we can analyse and predict more of the characteristics of the world around us than ever before, across all disciplines and industries – from medicine to cognitive and behavioural sciences, from supply chain to marketing, from automotive and traffic control to climate science.
- But all of these data are worthless if they cannot be processed. In order to process them, even with the most efficient of algorithms, parallel computing is necessary.
- At the same time, parallel computing opens up opportunities to use previously wasted computing resources – empty cycles on users' machines around the world.
- Obviously, the same is true for storage: Big data needs to be stored somewhere, and preferably on already existing storage devices that are under-utilized. With distributed storage, they can be utilized in the most efficient manner possible, and therefore benefit their owners.
- In order to keep the system fair and balanced, and to preserve security and privacy of all involved machines, there is no better way than decentralization. The resources and their distribution should be in the hands of those who own and use them.

Colossus Grid will connect devices in a peer-to-peer network enabling users and applications to rent the cycles and storage of other users' machines. This marketplace of computing power and storage will exclusively run on COLX currency. These resources will be used to complete tasks requiring any amount of computation time and capacity, or allow end users to store data anonymously across the COLX decentralized network. Today, such resources are supplied by entities such as centralized cloud providers which are constrained by closed networks, proprietary payment systems, and hard-coded provisioning operations.

Any user ranging from a single PC owner to a large data center can share resources through Colossus Grid and get paid in COLX for their contributions. Renters of computing power or storage space, on the other hand, may do so at low prices compared to the usual market prices because they are only using resources that already exist – comparable to carsharing being cheaper than taxis or rental cars.

All functions within Colossus Grid are privacy-enabled, largely due to the implementation of Zerocoin in COLX and utilization of I2P, as described in previous sections of this paper.

Last but not least, Colossus Grid, like other models in the sharing economy, is environmentally friendly because it utilizes available resources in the best possible manner with minimum waste and without the need for new production of components that may again only be utilized partly by their owners.

The COLX wallet will act as a middleware system which provides a distributed computing infrastructure and payment system independent from the scientific computation or task.

How and why we use this new colossus supercomputer and decentralized storage array will be driven by the community.

IoT Collaboration

In connection with the so-called internet of things (IoT), data production and consumption is increasing even more dramatically than in other IT-related fields. Not only is the amount of data increasing, but metadata (e.g., about start and end points of data transfer) are growing at an exponential rate with increasing size of the network.

To support such large-scale data size and computation tasks, it is not feasible to employ centralized solutions on cloud servers.

COLX is open to partnerships with IoT companies to distribute the analysis or processing of IoT data across its evolving grid infrastructure.

What Holds COLX Together

COLX is more than the sum of its parts and can only live through its team and community, as you will see in the following sections.

Team Members

The COLX Team is comprised of community members. Being listed is completely optional and we respect each individuals privacy. COLX is actively seeking encouraging more staff and developers to join, in order to strengthen the team as it continues to expand and evolve on a daily basis.

- Aliaksei: Blockchain Developer
- Coneits: Blockchain Developer
- Cryptowner: Web Developer, Project Manager, IT Advisor
- Heat007: Web Developer, Business Development
- Sussoloc46: Technical Support, Public Relations
- InfoDump01: IT Security, Public Relations
- Th82: Marketing, Public relations, Business Development
- Great Gama: Strategic Advisor, Marketing, Business Development, Humans Resources
- Conquistad0r: Technical Writer, Technical Support, Community Support
- ibmpclp: Financial Management
- Nate Murphy: Digital Video Specialist
- Sudo23: Founder of the ColossusCoin Foundation, Advisor

COLX Community

For some projects, communities are an afterthought. COLX's number one priority is the community. With giveaways, contests, a lively discussion platform and a zero tolerance policy toward the harassment of newcomers, COLX strives to be the cryptocurrency for all varieties of end-users.

The COLX coin is structured to be governed by the community in a transparent fashion. The development team is growing constantly through both outreach and active recruiting by the core team as well as proactive ideas, contributions and offers to help coming from the COLX community. We are proud of the large and growing following COLX has gathered to date including more than 5,000 followers on Twitter and over 3,000 members in our Telegram group. We are fostering a friendly and engaging environment where participation and contribution by everyone in the community is encouraged.

Funding

COLX receives funding for its projects through charitable contributions and the masternode proposal system. COLX would not be possible without the gracious support of the community.

The funding and direction of COLX's funding is governed by those in the COLX community with the most stake in enhancing COLX's long term value – the COLX masternode owners, who are each staking 10,000,000 COLX as collateral for their masternode. The mechanism and process behind this governance is built directly into the COLX blockchain code.

Charity

Although we are a relatively young project and have no mass pool of funds in terms of ICO or pre-mine, we actively look to give to those who are less fortunate. The COLX community has been involved with the World Community Grid for quite some time, and will continue to offer support in the future.

https://www.worldcommunitygrid.org

COLX Terms Of Service

By using this software, you acknowledge and understand that the ColossusXT (COLX) software is not intended for use in any illegal activity, and that no person or entity associated with creation, development, marketing, or furtherance of ColossusXT shall be held responsible for use by any individual, group, or entity that is against the law in their respective jurisdiction.

ColossusXT software is an experimental software.

There is no guarantee given here. Use it at your own risk.

Under no circumstances will ColossusXT be responsible for any loss or damage, including loss of coins, loss of data, damage of software/hardware, personal injury, resulting from anyone's use of ColossusXT software or the service, whether online or offline.

This software and the service are provided "As-Is" and ColossusXT makes no warranties of any kind relating to the services and expressly disclaims any and implied warranties, including without limitation the implied warranty of merchantability, fitness for a particular purpose or non-infringement. ColossusXT cannot guarantee and does not promise any specific results from use of ColossusXT and/or the service.

The ColossusXT Development Team