CPCOIN

WHITE PAPER

V.5.23 - 04th May 2023

CryptoPerformance

CryptoPerformance Coin ($CPC) and the CP Ecosystem

DISCLAIMER OF LIABILITY

Dear potential investor, We would like to remind you that this white paper is for informational purposes only, and does not establish a legally binding relationship between you and CryptoPerformance Group. The information contained within this white paper is not intended to serve as a brochure, nor does it represent an offer to purchase or an invitation to invest in any cryptocurrency. We urge you to consult with a legal, financial, or fiscal advisor before making any investment decisions. Nothing contained in this white paper should be construed as an invitation or solicitation to engage in any investment activity. We emphasize the importance of conducting due diligence and performing independent research to ensure that any investment decisions are informed and responsible. Please note that this white paper may have been translated into multiple languages. In the event of any inconsistencies between the various versions, the English version shall be considered the authoritative version. Thank you for your interest in CryptoPerformance.

The CryptoPerformance Team

This White Paper is confidential and intended solely for the recipient's information. It may not be used, published, or redistributed without the prior written consent of CryptoPerformance Group and the Founders.

Restricted transmission

This white paper must not be taken or transmitted to any jurisdiction where distribution or dissemination of this white paper is prohibited or restricted.

Risk statements

Purchasing CPCoin involves substantial risk and may lead to a loss of a substantial or entire amount of the money involved. Prior to purchasing CPCoin, you should carefully assess and take into account the risks, including those listed in any other documentation. A purchaser should not purchase CPC for speculative or investment purposes. Purchasers should only purchase CPC if they fully understand the nature of the CPC and accept the risks inherent to the CPC. The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of CP Group.

Cryptocurrencies may be subject to expropriation and/or theft; hackers or other malicious groups or organizations may attempt to interfere with our system/network in various ways, including malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing, and spoofing which may result in the loss of your coins or the loss of your ability to access or control your coins. In such event, there may be no remedy, and holders of coins are not guaranteed any remedy, refund, or compensation.

The regulatory status of cryptocurrencies and digital assets is currently unsettled, varies among jurisdictions and subject to significant uncertainty. It is possible that in the future, certain laws, regulations, policies or rules relating to cryptographic tokens, digital assets, blockchain technology, or blockchain applications may be implemented which directly or indirectly affect or restrict holders' right to acquire, own, hold, sell, convert, trade, or use the coins. The uncertainty in tax legislation relating to cryptocurrencies and digital assets may expose holders to tax consequences associated with the use or trading of cryptocurrencies.

Digital assets and related products and services carry significant risks. Potential purchasers should assess the nature of, and their own appetite for, relevant risks independently and consult their advisers before making any decisions.

Professional advice You must consult a lawyer, accountant, tax professional and/or any other professional advisors as necessary prior to determining whether to purchase CPCoins.

Caution Regarding Forward-Looking Statements

This white paper contains certain forward-looking statements that are based on the belief of CP Group as well as certain assumptions made by and information available to CP Group regarding the business we operate. Forward-looking statements, by their nature, are subject to significant risks and uncertainties. The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of CP Group. Forward-looking statements may involve estimates and assumptions and are subject to risks, uncertainties and other factors beyond our control and prediction. Accordingly, these factors could cause actual results or outcomes that differ materially from those expressed in the forward-looking statements. Any forward-looking statement speaks only as of the date of which such statement is made, we undertake no obligation to update any forward-looking statements to reflect events or circumstances after the date on which such statement is made or to reflect the occurrence of unanticipated events.

Consumer Protection Fund

Consumer protection fund is solely established to support the community if a chain error in transactions occurs. When the fund remains untouched, it is not added to the circulating supply.

Contents

1. CEOs' Letter

Dear valued readers, On behalf of the entire CryptoPerformance Group team, we would like to welcome you to our white paper. We are excited to share with you our vision for a decentralized ecosystem that empowers individuals and businesses alike through innovative blockchain technology. At CryptoPerformance, we believe in the power of blockchain to transform industries and create new opportunities for growth and development. Our team is comprised of experts in finance, technology, and marketing, who have come together to build a platform that is fast, scalable, and secure. Our ecosystem is centered around two key components: the CPCx0 Chain and CPCoin. The CPCx0 Chain is designed to be fast, scalable, and interoperable, making it ideal for a wide range of use cases from DeFi to supply chain management. CPCoin, on the other hand, serves as the native currency of the CPCx0 ecosystem, providing users with a fixed supply, staking rewards, and multi-asset support. Our ecosystem has the potential to revolutionize the way that businesses operate and individuals transact. Our commitment to innovation and growth is reflected in our roadmap, which includes exciting developments such as CP SAFE, CP PAD, CP INVESTMENTS, CP GAMING, Cx0 Developer Center and more. We understand that the key to wide adoption, is to make information and knowledge accessible to as many users as possible, which is why we have strived to make our white paper as accessible and informative as possible. Our goal is to provide you with a comprehensive overview of our ecosystem, its key features, and its many benefits. We invite you to join us on this exciting journey and become a part of the growing CP community. Thank you for your interest in our project and we look forward to your feedback and support.

Giuseppe Rimola & Horst Staebler

2. Overview of the CryptoPerformance Ecosystem

The CryptoPerformance Ecosystem is a comprehensive, decentralized platform designed to empower individuals and businesses by leveraging innovative blockchain technology. With a strong focus on speed, scalability, and security, the ecosystem aims to revolutionize the way businesses operate and individuals transact, providing a solid foundation for a wide range of applications, including DeFi, supply chain management, gaming, and more.

At the heart of the CryptoPerformance Ecosystem are two key components: the CPCx0 Chain and CPCoin. The CPCx0 Chain is a fast, scalable, and interoperable blockchain infrastructure that supports multiple use cases and seamless integration with other blockchain networks thanks to cross-chain connections. Its modular design allows for the addition of new transaction types and features, ensuring that the platform remains at the forefront of technological advancements in the crypto space.

CPCoin, the native currency of the CPCx0 ecosystem, is a fixed-supply token with multi-asset support, providing users with various benefits such as staking rewards, transaction processing, and participation in the ecosystem's growth. CPCoin is designed to be a secure and efficient medium of exchange, underpinning all transactions within the ecosystem.

CryptoPerformance has developed an ambitious roadmap that outlines a range of exciting developments and services aimed at further enhancing the platform's capabilities:

CP EXCHANGE: A secure, user-friendly trading platform for cryptocurrencies and digital assets.

CP GAMING: A hub for Web3 gaming experiences and opportunities.

CP SAFE: A secure storage solution for digital assets, providing peace of mind for users.

CP PAD: A launchpad for innovative projects, fostering growth and development within the ecosystem.

CP INVESTMENTS: A platform for investment opportunities in various digital assets and projects existing in the CPCx0 Chain.

CP MERCHANT: A solution for businesses to easily integrate and accept cryptocurrency payments.

CP PAY APP: A mobile app for seamless cryptocurrency payments and management.

CP PAYROLL: A payroll solution for businesses to pay employees using cryptocurrencies.

The CryptoPerformance team, consisting of experts in finance, technology, and marketing, is dedicated to fostering a community-driven ecosystem that encourages innovation, growth, and accessibility. By providing comprehensive information and knowledge about the platform and its features, CryptoPerformance aims to facilitate widespread adoption and participation in the digital economy.

3. CPCx0 Chain

3.1. Overview of the CPCx0 Chain

The CPCx0 Chain is the backbone of the CryptoPerformance Ecosystem, designed as a fast, scalable, and interoperable blockchain infrastructure that powers a wide range of applications and services. Created with user experience and adaptability in mind, the CPCx0 Chain lays a strong foundation for the decentralized platform.

With its focus on speed, the CPCx0 Chain ensures rapid transaction processing, enabling efficient and seamless exchanges across the ecosystem. Its scalable architecture allows the platform to handle a growing number of users and transactions, making it suitable for various use cases, from DeFi and supply chain management to gaming and beyond.

The interoperable nature of the CPCx0 Chain allows for seamless integration with other blockchain networks, fostering collaboration and the sharing of resources across different ecosystems. This feature opens up new possibilities for cross-chain interactions and broad-ens the scope of the CryptoPerformance Ecosystem.

The modular design of the CPCx0 Chain supports the addition of new transaction types and features, ensuring that the platform remains up-to-date with the latest technological advancements in the crypto space. This adaptability allows the CryptoPerformance Ecosystem to continuously evolve and expand, offering state-of-the-art building blocks for the digital economy.

In summary, the CPCx0 Chain is the core of the CryptoPerformance Ecosystem, pro-viding a fast, scalable, and interoperable blockchain infrastructure that paves the way for a multitude of applications and services, ultimately empowering individuals and businesses to harness the power of blockchain technology.

3.2. Key Features of the CPCx0 Chain

- **High-performance architecture:** The CPCx0 Chain is designed to provide fast and efficient transaction processing. Built on a high-performance architecture, it ensures rapid block confirmation times and supports a high throughput of transactions er second (TPS). This enables the seamless handling of large transaction volumes, making it suitable for various use cases, from DeFi to supply chain management.

- **Scalability:** As the CryptoPerformance Ecosystem grows and attracts more users, the CPCx0 Chain is designed to scale accordingly. Its architecture allows for the handling of an increasing number of transactions, ensuring that the network remains performant even as demand increases. This scalability ensures the long-term viability of the platform.

- **Interoperability:** The CPCx0 Chain supports cross-chain communication, allowing it to interact with other blockchain networks seamlessly. This interoperability opens up new possibilities for cross-chain interactions and the sharing of resources across different ecosystems, fostering collaboration and broadening the scope of the CryptoPerformance Ecosystem.

- **Security and cryptography**: The CPCx0 Chain employs state-of-the-art cryptographic techniques to ensure the security and integrity of the network. It utilizes elliptic curve cryptography (ECC) for key exchange and digital signatures, providing strong security with smaller key sizes. The encryption algorithm is based on Curve25519 and ECKCDSA, offering a balance of speed and security for a key size of only 32 bytes.

- **Modular transaction types:** The CPCx0 Chain supports a modular approach to transactions, allowing for the easy addition of new transaction types and features as the platform evolves. This modularity ensures that the platform remains up-to-date with the latest technological advancements in the crypto space and can adapt to changing user requirements.

- **Energy-efficient consensus mechanism:** The CPCx0 Chain employs an energy efficient consensus mechanism that prioritizes sustainability while maintaining network security. By minimizing the energy consumption required to maintain the network, the CPCx0 Chain ensures a more eco-friendly and cost-effective platform.

- **Accessible development tools:** The core of the CPCx0 Chain is written in enterprise-friendly programming languages, such as Java and NodeJS, and the frontend is built with AngularJS. This choice of languages and frameworks makes it easier for developers to engage with the platform and contribute to its growth. The matured and large developer communities for these tools provide access to a wealth of proven components and frameworks, streamlining the development process.

- **Continuous integration and innovation:** The CryptoPerformance team actively monitors the crypto space for new technologies and powerful protocols. The CPCx0 Chain is designed to facilitate the integration of these cutting-edge features, ensuring that the platform remains at the forefront of innovation in the blockchain industry. This commitment to continuous integration and innovation sets the stage for ongoing growth and development within the CryptoPerformance Ecosystem.

4. CryptoPerformance Coin - CPCoin ($CPC)

*4.1. **Overview of CPCoin***

CPCoin is the native digital currency of the CryptoPerformance Ecosystem, designed to facilitate transactions, reward users, and serve as the underlying asset for various services within the platform. As an integral part of the CPCx0 Chain, CPCoin offers users a fixed supply, ensuring long-term value stability and protection against inflation.

CPCoin is created to be versatile and user-friendly, supporting a wide range of applications and services within the CryptoPerformance Ecosystem. From decentralized finance (DeFi to gaming and supply chain management, CPCoin provides a seamless and secure means of exchange for users across the platform.

Staking rewards are another key feature of CPCoin, incentivizing users to participate in the network and contribute to its growth. By staking their coins, users can earn rewards for contributing to the normalisation of CPCoin volatility.

Moreover, CPCoin offers multi-asset support, allowing users to easily access and manage a diverse range of digital assets within the CryptoPerformance Ecosystem. This flexibility ensures that CPCoin remains adaptable and relevant in the ever-evolving landscape of digital currencies and blockchain technology.

In summary, CPCoin is the lifeblood of the CryptoPerformance Ecosystem, providing users with a fast, secure, and versatile digital currency designed to empower individuals and businesses alike in their journey through the world of blockchain.

*4.2. **Key Features of CPCoin***

- **Fixed Supply:** CPCoin has a predetermined and fixed total supply, ensuring scarcity and reducing inflationary risks. This feature makes the coin a valuable asset in the long term, as it will not be diluted by excessive issuance.

- **Staking Rewards:** CPCoin holders can earn staking rewards by participating in the network's consensus process. This encourages users to hold and stake their coins, thus contributing to network security and stability while being rewarded for such actions.

- **Multi-Asset Support:** CPCoin is designed to support multiple assets within the CPCx0 ecosystem. This flexibility allows for seamless integration of various tokens and digital assets, making the platform more versatile and accommodating for users and businesses.

- **Secure and Decentralized:** CPCoin leverages the security and decentralization benefits of blockchain technology. This ensures that the coin's transactions are resistant to censorship and manipulation while providing transparency and trust.

- **Fast and Scalable:** CPCoin is built on the CPCx0 Chain, which is designed for high throughput and low latency. This enables the coin to process transactions quickly and efficiently, making it suitable for various use cases, including payments, remittances, and micropayments.

- **Interoperable:** CPCoin's interoperability features allow it to interact with other blockchains and networks seamlessly. This enables users and businesses to leverage the best aspects of various blockchain technologies and enjoy the benefits of cross-chain functionality.

- **Eco-friendly Consensus Mechanism:** CPCoin employs an energy-efficient consensus mechanism, reducing its environmental impact compared to traditional Proof of Work-based cryptocurrencies. This aligns with the growing demand for sustainable and eco-friendly blockchain solutions.

- **User-friendly Wallets and Applications:** CPCoin can be easily accessed and managed through our user-friendly Cx0 Wallet, making it accessible to users of varying technical backgrounds. This helps drive adoption and usage of the coin within the wider community.

The CPCoin is hard-coded on the CPCx0 Chain. The CPCoin transfers are secure, inexpensive and fast, within 15 seconds. The CPCoin has its own CPCoin Decentralized & Secure Smart Wallet (Cx0). CPCx0 Chain is the innovative proprietary chain of CryptoPerformance Group. Data collection and coin storage on the chain is immutable.

*4.3. **CPCoin Tokenomics***

CPCx0 Chain's native coin CPC is primarily used to pay the translation fees on the network and the rewards for validators. CPC's entire supply of 250,000,000 coins was issued in November 2021 to replace the old CPC token.

CPCoin started with a circulating supply of zero and releases CPC through secondary distribution on a monthly basis to the circulating supply. Coins are allocated in subsequent distributions (including for staking purposes.

New circulating supply is published daily on explorer (https://smartexplorer.cpcoin.io and forwarded to coin market information sites.

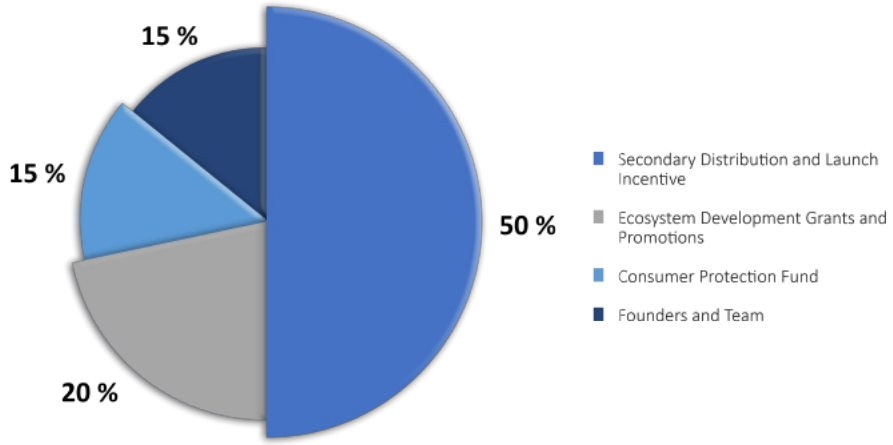
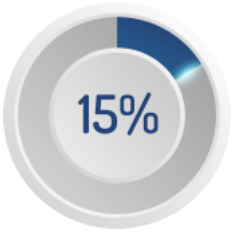
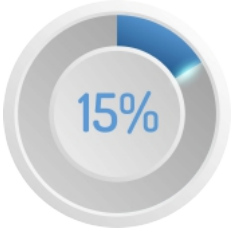


Figure 1: **Breakdown of the CPCcoin supply**

CPCoin was issued directly through secondary distribution without presale or ICO.

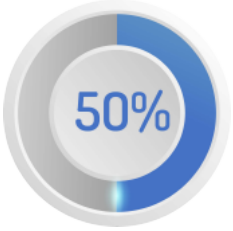


15% of the total supply, 37.5 million CPC, was distributed to the founders and team. These tokens will be frozen until 31 December 2021.



15% of the total supply, 37.5 million CPC, was frozen for Consumer Protection Fund until 31 December 2022.

20% of the total supply, 50.0 million CPC, was distributed for Ecosystem Development Grants and Promotions.



50% of the total supply, 125 million CPC, is locked. These tokens will be directly into thmarket monthly based on the schedule.

The secondary distribution inserts coins monthly onto the market. The secondary distribution can vary depending on market demand, which can prolong or shorten issuance. The schedule can vary depending on market demand.

The secondary distribution started on 10.10.2020 and will continue until the total supply is reached. The detailed schedule of secondary distribution can be found below.

- **Yearly Supply:** 3 years
- **Date:** From 10.10.2020
- **Supply Secondary Distribution:** Until total supply is reached

Yearly Supply			Monthly Supply		
Period	% of Total Supply	CPCoin mln	Period	% of Total Supply	CPCoin mln
Overall	50 %	125			
Year 1	15 %	37.5	Monthly	1.25 %	3.125
Year 2	16 %	40.0	Monthly	1.33 %	3.333
Year 3	19 %	47.5	Monthly	1.58 %	3.958

Figure 2: **Breakdown of the CPC coin supply**

Once the total supply is reached, validators can start receiving rewards from staking. Until then, the validators can only receive the transaction fee, which is included in the block created by the validators.

The transaction fee depends on the total amount of transactions; CPCoin and subcurrencies on the CPCx0 Chain:

- From 0 to 1,000: transaction fee is 0.060%
- From 1,000+ to 2,500: transaction fee is 0.050%
- From 2,500+ to 5,000: transaction fee is 0.040%
- From 5,000+ to 10,000: transaction fee is 0.030%
- From 10,000+ to 20,000: transaction fee is 0.020%
- From 20,000+ to 50,000: transaction fee is 0.015%
- From 50,000+ to 100,000: transaction fee is 0.012%
- From 100,000+ to 500,000: transaction fee is 0.010%
- From 500,000+ to 1,000,000: transaction fee is 0.008%
- From 1,000,001+: transaction fee is 0.005%

Besides the normal transactions used for payment, CPCx0 Chain also has other types of particular transactions.

Table 1: **Special Transactions Fees**

Type of special transaction	Transaction fee (CPC)
Creating a new token Creating	10,000
a new asset Creating	10,000
crowdfunding Account control	10,000
configuration	0.1
Approving a controlled transaction	1.0
Sending private message	0.2
Open a voting poll Per	100.0
vote	1.0

The transactions can be subject to change in the future.

*4.4. **Ecosystem Growth & Developer Activity***

Since its creation, the CPCx0 Chain has been a 100% value-driven project focusing on solving real use cases for communities. With this in mind, CPCx0 Chain is already in the process to launch two large and innovative projects in 2023, which will be announced in the coming months. In 2023 the CPCx0 Chain will support new token launches from the community, token assets, apps, and many other innovative features for newcomers, professionals, and businesses.

Our preliminary focus in the future is to continue solving community problems, especially problems that have existed on Web2 for a long time. The cross-chain connection will be our secondary focus to bring our blockchain solutions to the larger community.

As a hybrid chain, CPCx0 Chain maintains control of the chain. With the Developer Center, users can contribute to the CPCx0 Chain by implementing new nodes, creating new tokens, creating new projects, etc. However, all of them must pass the CPCx0 Chain verification process, depending on the activity that the contributor wants to undertake. The CPC team will review every request from the contributor and will approve best practice projects.

4.4.1. ***CPCoin - The native token of CPCx0 Chain***

CPCoin is the native coin of the CPCx0 Chain, designed to facilitate seamless transactions within the blockchain ecosystem. To understand its significance, it's crucial to differentiate between two key terms in the blockchain industry: cryptocurrency and token.

Cryptocurrency: A digital or virtual currency secured by cryptography, rendering counterfeiting or double-spending nearly impossible. Cryptocurrencies operate within decentralized networks based on blockchain technology, a distributed ledger enforced by a network of disparate computers. Each cryptocurrency functions on its distinct blockchain and is intended for use as currency, money, or a payment method.

Token (Crypto Token): A denomination or unit of a cryptocurrency that operates on a blockchain, which serves as a medium for creating and executing decentralized apps (dApps and smart contracts. Tokens facilitate transactions within the blockchain ecosystem, enabling users to interact with dApps and smart contracts seamlessly.

As the native digital currency of the CPCx0 Chain, CPCoin plays a crucial role in enabling secure, efficient, and decentralized transactions within the platform, fostering a robust and innovative ecosystem for users to interact with blockchain-based applications.

4.4.1.1. ***Understanding Cryptocurrency and Native Tokens.*** The primary distinction between a cryptocurrency and a token lies in their relationship to the blockchain. While cryptocurrencies are the native assets of a blockchain (e.g., BTC or ETH, tokens are built on an existing blockchain. Native tokens serve as the inherent digital currency of a particular blockchain.

Each independent blockchain has its own native token, functioning as a reward for validators who add blocks to the blockchain and as a payment method for transaction fees. In this context, CPCoin is the native token of the CPCx0 Chain, representing the platform's underlying digital currency that enables seamless transactions and incentivizes the network's validators.

4.4.1.2. ***Classifying Cryptocurrencies: Types and Functions.*** Cryptocurrencies can be classified into several categories based on their use cases and characteristics:

- **Payment Tokens:** Designed for use as alternative means of payment and exchange, payment tokens aim to provide a decentralized method for buying and selling goods and services without traditional intermediaries. These tokens typically have limited additional functions. CPCoin, the native token of the CPCx0 Chain, is an example of a payment token.

- **Stablecoins:** These cryptocurrencies have their value pegged or tied to another currency, commodity, or financial instrument. Stablecoins can be further classified into Fiat-Collateralized, Crypto-Collateralized, and Algorithmic Stablecoins.

- **Security Tokens:** Representing ownership or other rights, security tokens are digital assets that transfer value from an asset or bundle of assets to a token. In simple terms, security tokens are digital forms of traditional investments, such as stocks or bonds.

- **Utility Tokens:** Integrated into a blockchain protocol, utility tokens are used to access the services of that protocol. They are not intended for direct investment like security tokens, but can be used to pay for services within their specific ecosystems. Utility tokens and their associated platforms share a synergistic relationship, with the platform offering security for the token while the token drives network activity to strengthen the platform's economy. Utility tokens can be compared to coupons or vouchers for a specific ecosystem.

Understanding the various types of cryptocurrencies and their functions allows investors and users to make informed decisions about which digital assets to engage with and how they can be utilized within the broader blockchain ecosystem.

*4.5. **Ecosystem***

All fees are incurred on the central CryptoPerformance Platform, on the decentralized CPCx0 Chain as well as all other products of the CryptoPerformance Group (CryptoPerformance BANQ, CP Charity for Charities and many more).

*4.6. **Coin Information***

The CPCoins are issued directly to the market and has been created with an upper limit of 250 million, this will not be increased.

Name/Ticker	: **CPCoin/CPC**
Decimals	: **8**
Maximum Supply	: **250.000.000,00**
Coin Distribution Mechanisms	: **Secondary distribution (no pre-sale, no ICO)**
Blockchain	: **CPCx0 Chain**
Storing of CPCoin	: **CPC Secure Wallet** https://smartwallet.cpcoin.io

5. Evolution Staking

CPCoin is the core utility and framework token of the CPCx0 blockchain network and, as such, does not reward its users or owners by merely buying it on an Exchange or holding it in a decentralized wallet.

However, for certain selected and registered users, the CP Platform will launch a temporary promotional program called the "Evolution Staking Program" which will reward CPCoin users and depositors only and exclusively on the CP Platform's own custodial wallet with a "custody incentive reward", which will grant CPCoin rewards based on the liquidity provided and kept within the CP Platform for certain periods. Please note: the Evolution Staking Program is a limited-time unilateral promotional program only of the CP Platform itself, and it is not an inherent feature, characteristic or right of the CPCoin; holding or using CPCoin on any other platform or Exchange, or even on the CP Platform but outside of the promotional periods, will not result in any CPCoin reward.

T&Cs, facts sheet and restrictions of the Evolution Staking Program are consultable directly and only on the CP Platform website.

- **Start Criteria:** CryptoPerformance approved users all over the world (not included: USA, China, Iraq, Libya, South Yemen, Syria, Sudan, North Korea, Iran, Afghanistan)
- **Start Date:** 10.11.2020
- **Duration:** Until 31.12.2023 or until Ecosystem Development Grants have reached limit (depending on demand can be extended)
- **Evolution Staking CPC Frequency:** Daily 24 hours
- **Evolution Staking CPC aCPC**: 0.0665 bonus CPC (aCPC) per 100 CPC per day, paid every 8 hours. aCPC are frozen for 365 days
- **CPC Allocation:** CP Platform in the CPC Evolution Staking.

5.1. Average Program

The CP Average Program is a subscription that can be purchased daily, weekly or bimonthly. Customers can lean back and relax, as the program buys cryptocurrencies fully automatically at a set time. The program revolves around the "dollar cost average effect".

6. CryptoPerformance Ecosystem Overview

6.1. CP BANQ

6.1.1. Overview

CP BANQ is a Neobanking Platform designed to help users manage their cryptocurrency accounts with ease. With the ability to track expenses, manage investments, and spend cryptocurrencies like cash, CP BANQ allows users to access the world's best crypto assets all in one app.

By signing up for a CP BANQ account, users become eligible for a CP Crypto Visa Card, which allows for free crypto transfers and transaction-free withdrawals from any ATM point in the world. This debit card also enables online and offine payments on the international VISA circuit and global transfers associated with an IBAN.

The CP BANQ app is designed to make managing, tracking, and investing funds simple. Users can easily swap cryptos to FIAT, check transaction history, track funds, pay bills and invoices, and transfer money to any account globally.

CP BANQ is also a secure and compliant platform, backed by 24/7 expert support. The app is regulated and KYC compliant, ensuring the security of all online and in-store transactions from fraud and third-party interference. Users are also granted extra 3DS protection, which adds an additional layer of security.

With access to all cryptocurrencies, IBANs, and a crypto Visa card, CP BANQ paves the way to the crypto payment revolution.

6.1.2. Key Features

- **Multi-Currency Support:** CP BANQ provides support for multiple cryptocurren-cies, including the CPC token. It also allows users to deposit fiat currency, which can be converted into crypto using the in-app exchange.

- **International IBANs:** CP BANQ provides users with International Bank Account Numbers (IBANs) that can be used to receive and send payments globally. This feature enables users to conduct cross-border transactions without the need for traditional banking systems.

- **CP Crypto Visa Card:** CP BANQ users can also apply for a CP Crypto Visa Card, which allows them to spend their cryptocurrencies like cash. The debit card can be used to make online and offline payments on the international Visa circuit, and users can withdraw their funds from any ATM point in the world.

- **In-App Cryptocurrency Exchange:** The CP BANQ app includes an in-app cryptocurrency exchange that enables users to swap between different cryptocurrencies or convert crypto to fiat currency. The exchange has a low transaction fee of 2.5%.

- **Real-time Transaction Monitoring:** CP BANQ provides users with real-time monitoring of their transactions. Users can track their spending, view their transaction history, and receive real-time push notifications with every transaction.

- **Secure and Compliant:** CP BANQ is fully compliant with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. The platform uses Visa security and fraud prevention to protect users' funds and transactions.

- **Custody Services:** CP BANQ provides custody services for USD, EUR, GBP, and CPC. This feature enables users to store their funds securely on the platform.

- **Easy to Use:** CP BANQ is designed to be user-friendly, with a simple and intuitive interface. The platform is accessible from anywhere, and users can manage their assets 24/7 using the app.

In summary, CP BANQ provides a comprehensive suite of tools and features for managing cryptocurrency assets. It offers multi-currency support, IBANs for global payments, a crypto Visa card for spending, an in-app exchange, real-time transaction monitoring, custody services, and compliance with regulatory requirements. The platform is easy to use and provides users with a seamless experience for managing their cryptocurrency assets.

6.2. Cx0 Developer Center

6.2.1. Overview

The Cx0 Developer Center is a white label token creation and digital asset platform built on the CPCx0 Chain. This platform is designed to empower developers and businesses to create customized tokens and digital assets with unique features such as fixed supply, fixed rate issuance, and token burning. The portal offers a range of benefits, including an intuitive user interface, pre-built smart contracts, and a suite of APIs to enable easy creation and management of tokens and digital assets. Moreover, the Cx0 Developer Center provides a range of tools for managing and distributing tokens, such as an easy-to-use wallet, an API for integrating tokens into existing platforms, and analytics tools to track token usage and performance. With a low learning curve and quick time-to-market, the Cx0 Developer Center enables developers and businesses to create and deploy customized tokens quickly and efficiently, making it a powerful tool for creating value-driven solutions on the CPCx0 Chain.

*6.2.2. **Key Features***

The Cx0 Developer Center is a robust and versatile platform designed to provide developers and businesses with the necessary tools to create customized tokens and digital assets on the CPCx0 Chain. The platform offers a variety of key features that make it an attractive choice for developers and businesses looking to build on the CPCx0 Chain.

One of the key features of the Cx0 Developer Center is its intuitive user interface. The platform is designed to be easy to use, with a low learning curve that allows developers and businesses to quickly get up to speed and start building tokens and digital assets. The user interface is well-organized and streamlined, making it simple to navigate and access the tools needed to build, manage, and distribute tokens and digital assets.

Another important feature of the Cx0 Developer Center is its pre-built smart contracts. The platform offers a variety of pre-built smart contracts that can be customized to meet the specific needs of developers and businesses. These smart contracts provide a range of functionalities, including fixed supply, fixed rate issuance, and token burning, among others.

The Cx0 Developer Center also offers a suite of APIs that enable developers and businesses to create and manage tokens and digital assets. These APIs allow for a high degree of customization, making it possible to tailor tokens and digital assets to meet specific business needs. The APIs are well-documented and easy to use, providing developers and businesses with the flexibility they need to build customized tokens and digital assets.

In addition to these key features, the Cx0 Developer Center provides a number of tools for managing and distributing tokens and digital assets. These tools include an easy-to-use wallet for users to manage their tokens, an API for integrating tokens into existing platforms and applications, and a set of analytics tools to track token usage and performance. These tools make it easy for developers and businesses to manage and distribute their tokens and digital assets, and to track their performance over time.

Overall, the Cx0 Developer Center offers a powerful set of tools and features that make it an ideal choice for developers and businesses looking to build on the CPCx0 Chain. Its ease of use, pre-built smart contracts, suite of APIs, and range of management and distribution tools make it a comprehensive and versatile platform that can meet the needs of developers and businesses of all sizes and types.

6.3. *Future Developments of the CP Ecosystem*

6.3.1. *CP Exchange*

CP EXCHANGE is an advanced cryptocurrency exchange that provides users with a comprehensive range of trading options. With its cutting-edge technology and secure trading platform, CP EXCHANGE enables users to easily buy, sell, and trade cryptocurrencies across a wide range of markets. By providing a simple and intuitive trading interface, CP EXCHANGE is helping to drive the adoption of cryptocurrencies as a mainstream investment asset.

6.3.2. *CP Gaming*

CP GAMING is a Web3 launchpad that empowers developers to create innovative new gaming projects. By providing a comprehensive suite of tools and resources, CP GAMING streamlines the process of creating new games and enables developers to connect with a wider audience. With its cutting-edge technology and innovative features, CP GAMING is a leading platform for the next generation of gaming experiences.

6.3.3. *CP Safe*

CP SAFE is an advanced trust service designed to provide users with secure and efficient custody solutions. Through CP SAFE, users can receive Euro, Dollar, and Pound Sterling IBANs to facilitate payments in both fiat and crypto. Additionally, CP SAFE offers a range of crypto wallets to enable users to easily manage their digital assets. By placing values into custody, businesses can grow their wealth and invest in innovative projects.

6.3.4. *CP Pad*

CP PAD is a Web3 launchpad that fuels innovative projects and empowers decentralized growth. As part of the CPCoin and CP BANQ ecosystems, CP PAD streamlines the process of launching new projects and helps them gain exposure to a wider audience. With its streamlined interface and comprehensive suite of features, CP PAD provides a simple and intuitive way for developers to launch new projects and gain access to the latest tools and resources.

6.3.5. *CP Investments*

CP INVESTMENTS is a Web3 launchpad that connects investors with the latest innovative projects in the cryptocurrency space. Through CP INVESTMENTS, users can access a comprehensive range of investment opportunities, including ICOs, STOs, and IEOs. By connecting investors with cutting-edge projects, CP INVESTMENTS helps to drive innova-tion in the digital currency space and provides opportunities for growth and wealth creation.

6.3.6. ***CP Merchant***

CP MERCHANT is an advanced payment solution that enables businesses to easily accept cryptocurrency payments. With its streamlined interface and fast, secure transactions, CP MERCHANT provides a simple and efficient way for businesses to integrate cryptocurrency payments into their existing payment systems. By reducing fees and improving security, CP MERCHANT is helping to drive the adoption of cryptocurrency payments across a wide range of industries.

6.3.7. ***CP Pay App***

CP PAY APP is an advanced payment solution that enables businesses to easily accept cryptocurrency payments. With its streamlined interface and fast, secure transactions, CP PAY APP provides a simple and efficient way for businesses to integrate cryptocurrency payments into their existing payment systems. By reducing fees and improving security, CP PAY APP is helping to drive the adoption of cryptocurrency payments across a wide range of industries.

6.3.8. ***CP Payroll***

CP PAYROLL is a streamlined payroll solution that simplifies the process of distributing salaries in cryptocurrencies. By enabling businesses to easily distribute salaries to employees around the world, CP PAYROLL is helping to drive the adoption of cryptocurrency payments in the workplace. With its fast, efficient transactions and low fees, CP PAYROLL is a leading solution for businesses looking to improve their global payment systems.

7. Technical Overview

On January 3, 2009, the first Bitcoin transaction marked the beginning of a groundbreaking era in globalization and interconnectedness. Satoshi Nakamoto accomplished the seemingly impossible by establishing a currency and payment system free from centralized control. This currency, known as Bitcoin, is powered by an underlying technology called the blockchain.

Although Bitcoin has been in use for over eight years, it is only recently that the full potential of blockchain technology has started to emerge. Blockchain is revolutionizing economic processes in much the same way that the internet transformed information accessibility. Today, individuals can access the global economy on equal terms with others, breaking down barriers and fostering inclusivity.

In this context, we introduce CPC—a versatile blockchain platform designed for users across various industries and applications. This multipurpose platform leverages the power of blockchain technology to empower individuals and organizations, unlocking new opportunities and driving innovation in the rapidly evolving digital landscape.

7.1. ***What is a Blockchain?***

A **blockchain** is a distributed database that enables the creation of a digital ledger of transactions, shared across a network of computers. Utilizing advanced cryptography, it allows each participant to securely interact with the ledger without a central authority. The blockchain maintains a constantly growing list of records (blocks), each containing a timestamp and a link to the previous block.

The emergence of cryptocurrencies, tokens, digital coins, and other blockchain-based digital assets has given rise to a **financial superhighway**, directly connecting billions of people worldwide. This global network empowers individuals to trade products and services across borders, bypassing traditional intermediaries. Blockchain technology ensures that the value of such transactions remains secure, immune to political interference, oversupply, or unauthorized third-party alterations.

As blockchain technology continues to reshape the financial landscape, it is becoming increasingly clear that centralized financial systems will struggle to accommodate the vast number of complex transactions executed daily on the financial superhighway.

CPC is based on a user and service-centric multipurpose blockchain platform (CPCx0 Chain) and is a cryptocurrency built upon a proven open-source crypto projects' framework. As a crypto-technology integrator, it combines and enhances existing and new crypto-technology features and services, creating a powerful platform for the digital economy. By harnessing the revolutionary potential of blockchain technology, it aims to redefine the future of financial interactions and drive innovation across industries and applications.

7.2. Introduction

Since its inception, blockchain technology has sparked controversy due to its most natural application—value transfer using a network token. While decentralized money represents a groundbreaking development, blockchain technology has far more to offer. As a distributed database, blockchain enables various types of distributed ledger entries, with their nature depending on the interpretation of the technology's users. **CPC** is an innovative, secure, decentralized payment system built on cutting-edge cryptocurrency technologies, designed to create digital economies akin to traditional financial services.

7.2.1. Mission and Goals

CPC's mission is to make the complex cryptocurrency market accessible to everyone, accelerating the adoption of blockchain technology and democratizing ownership of cryptocurrencies. CPC simplifies the purchasing and transfer of cryptocurrencies, allowing average individuals to participate in the new economy. The CPC foundation aligns with the philosophical mission established by Satoshi Nakamoto, putting the power back into the hands of the people where it belongs.

7.2.2. Current Challenges in the Market

The long-term success of cryptocurrencies is intrinsically linked to achieving widespread adoption. While the potential for crypto to become a global payment method is well-recognized, its current status as a speculative asset overshadows its utility as an everyday currency. Several factors have impeded the mainstream acceptance of cryptocurrencies, despite the exponential growth and increased recognition of blockchain technology.

Firstly, negative publicity surrounding the volatile nature of the crypto market, as well as concerns over bubble speculations, has contributed to public skepticism. This skepticism is further exacerbated by the prevalence of scams and fraudulent schemes in the ecosystem, which deter potential users from embracing cryptocurrencies.

Secondly, many existing platforms and applications feature complex user interfaces, making it difficult for the average person to navigate the crypto landscape. This barrier to entry significantly hampers the adoption of digital currencies as people struggle to understand and engage with the technology.

Lastly, security concerns remain a pressing issue in the cryptocurrency market. Instances of hacking and cyberattacks on crypto exchanges, as well as individual user devices and wallets, heighten the uncertainty and risk associated with this emerging technology.

To foster widespread adoption, it is crucial to address these challenges head-on. By developing user-friendly platforms, enhancing security measures, and promoting transparent and ethical practices within the crypto ecosystem, we can pave the way for a future where cryptocurrencies are an integral part of the global financial landscape.

*7.2.3. **Addressed Issues***

Cryptocurrency, as a decentralized, blockchain-based financial system, boasts immutability and autonomy as its defining features. Although cryptocurrencies empower users to circumvent intermediaries and maintain independence from traditional financial institutions, no digital currency, including Bitcoin, has successfully become a widely utilized monetary asset. Merchants and service providers remain apprehensive about accepting cryptocurrency payments, primarily due to concerns regarding exchange losses, regulatory challenges, and high volatility.

CPC is designed to confront the fundamental obstacles that impede the integration of cryptocurrencies into the global financial system. By crafting solutions that promote the use of digital currencies as a viable payment method, CPC seeks to unleash the full potential of blockchain technology and facilitate the mainstream adoption of cryptocurrencies.

By addressing these crucial pain points, CPC aims to establish a more inclusive and accessible financial landscape that harnesses the transformative power of blockchain technology, empowering individuals and organizations alike to embrace the myriad opportunities presented by digital currencies.

*7.3. **Technology***

CPC is a 100% proof of stake cryptocurrency, built upon proven open-source projects and written in Java. Its unique proof of stake algorithm does not rely on the "coin age" concept employed by other proof of stake cryptocurrencies and is resistant to "nothing at stake" attacks. A total of 250 million tokens were distributed in the genesis block. Curve25519 cryptography is utilized to provide a balance of security and required processing power, in conjunction with the widely-used SHA256 hashing algorithms.

*7.3.1. **Technical Background***

Blocks are generated on average every 15 seconds by accounts that are unlocked on network nodes. As the full token supply already exists, CPC is redistributed through transaction fees, which are awarded to an account when it successfully creates a block. This process, known as forging, is akin to the "mining" concept employed by other cryptocurrencies. CPC transactions are based on a series of core transaction types that do not necessitate any script processing or transaction input/output processing on the part of network nodes.

*7.3.2. **Proof-of-Stake (POS)***

In CPC's system, each token in an account can be considered as a miniature mining rig. The more tokens held in the account, the greater the chance the account will earn the right to generate a block. The total reward received as a result of block generation is the sum of the transaction fees located within the block. CPC does not generate any new tokens as a result of block creation. Redistribution of CPC occurs through block generators receiving transaction fees, so the term "forging" is used instead of "mining". Subsequent blocks are generated based on verifiable, unique, and nearly unpredictable information from the preceding block. Blocks are interconnected through these relationships, creating a chain of blocks (and transactions) that can be traced back to the genesis block.

CPC's proof of stake algorithm adheres to the following basic principles:

1. A cumulative difficulty value is stored as a parameter in each block, and each subsequent block derives its new "difficulty" from the previous block's value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty.

2. To prevent account holders from manipulating their probability of block generation by moving their stake between accounts, tokens must remain stationary within an account for 1,440 blocks before contributing to the block generation process. Tokens meeting this criterion contribute to an account's effective balance, which is used to determine forging probability.

3. To deter an attacker from generating a new chain from the genesis block, the network allows chain reorganization only up to 720 blocks behind the current block height. Any block submitted at a height lower than this threshold is rejected, effectively establishing a moving checkpoint.

4. Transactions are considered secure once they are encoded into a block that is at least 10 blocks behind the current block height, due to the extremely low probability of any account taking control of the blockchain by generating its own chain of blocks.

*7.3.3. **The Coin***

The total supply comprises 250 million coins, divisible to eight decimal places. All coins were issued with the creation of the genesis block, leaving the genesis account with an initial negative balance of 250 million coins. The existence of anti-coins in the genesis account has a couple of interesting side effects:

- The genesis account cannot issue transactions of any kind since its balance is negative, and it cannot pay transaction fees.

- Any coins sent to the genesis account are effectively destroyed, as the account's negative balance will cancel them out.

The term "coins" is chosen deliberately, as CPC intends to serve as a base protocol providing numerous other functions. While CPC's most basic function is that of a traditional payment system, it was designed to do far more.

7.4. ***Nodes***

A node on the CPC network is any device contributing transaction or block data to the network. Any device running the CPC software is considered a node. Nodes can be divided into two types: hallmarked and normal. A hallmarked node is a node tagged with an encrypted token derived from an account's private key, which can be decoded to reveal a specific account address and balance associated with the node. Hallmarked nodes provide a level of accountability and trust, making them more trusted than non-hallmarked nodes on the network.

The larger the balance of an account tied to a hallmarked node, the more trust is given to that node. Though an attacker might want to hallmark a node to gain trustworthiness within the network and then use that trust for malicious purposes, the barrier to entry (cost of tokens required to build adequate trust discourages such abuse.

More than that CPCx0 Chain as a hybrid chain, use a node management layer to secure the trusted node on it.

Each node on the chain will update the list of valid nodes from the CPCx0 Admin server every one min.

Anytime a new node wants to join our chain, it needs the approval from our CPCx0 Admin to be added to the list of valid nodes. Only after that, it can join our chain successfully.

Each node on the CPC network can process and broadcast both transactions and block information. Blocks are validated as they are received from other nodes, and in cases where block validation fails, nodes may be temporarily "blacklisted" to prevent the propagation of invalid block data. Each node features built-in DDOS (Distributed Denial of Services defense mechanisms that restrict the number of network requests from any peer to 15 per second.

7.5. ***Blocks***

As in other cryptocurrencies, the ledger of CPCx0 Chain transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred.

By spacing out commits, we give all network participants enough time to come to consensus: even though transaction requests occur dozens of times per second, blocks are only created and committed on CPCx0 Chain once every fifthteen seconds.

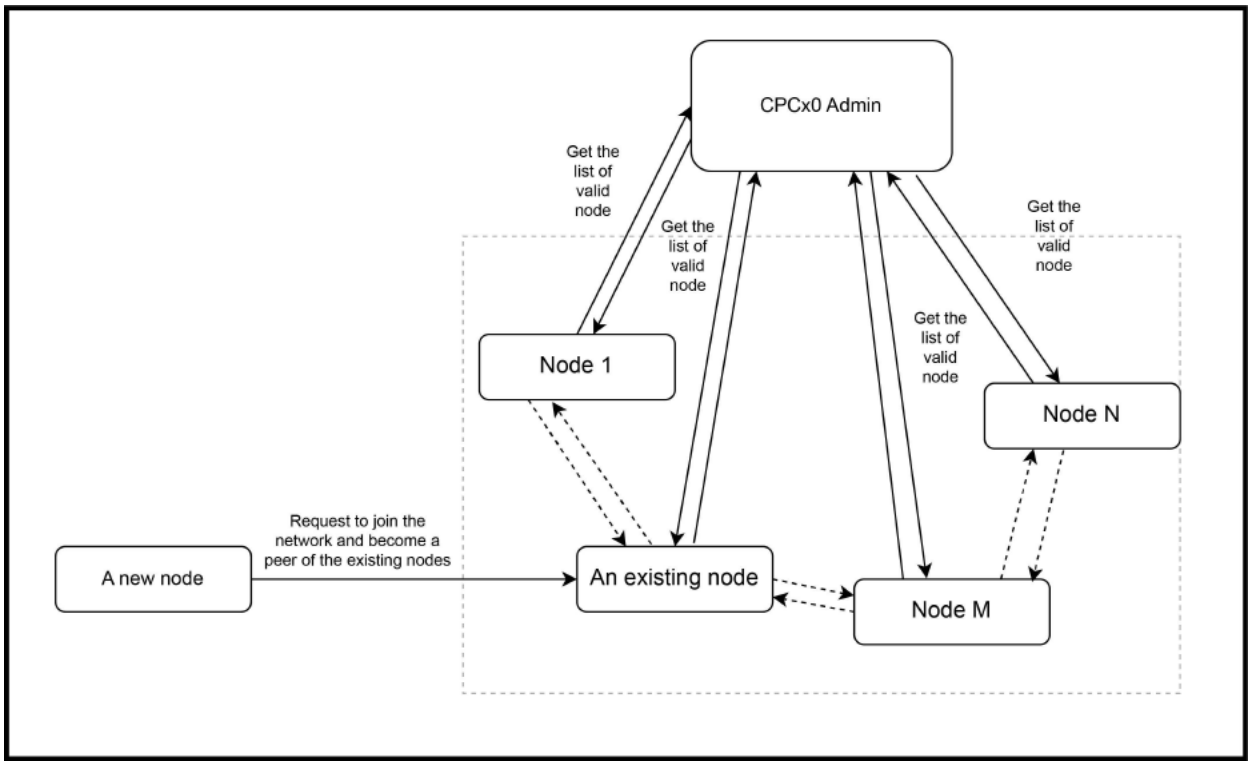


Figure 3: Network Nodes

*7.5.1. **Block creation***

To preserve the transaction history, blocks are strictly ordered (every new block created contains a reference to its parent block), and transactions within blocks are strictly ordered as well.

Once a block is put together by a selected validator (or a forger - two names are same) on the network, it is propagated to the rest of the network; all nodes add this block to the end of their blockchain, and a new validator is selected to create the next block. When the block comes to a node, all possible parameters of the block are verified, including the effective balance of the block generator's account. This proves that the generating account actually contains the effective balance (stake) that won it the right to generate the block.

Here are fields that a block could have:

- **Block or Block ID:** The id of the block.
- **Height:** The height of the block. Using this value we could know how many blocks have been minted in the chain.
- **Previous block ID:** The id of the previous block.
- **Previous block hash:** The hash of the previous block.
- **Payload length:** The size of the block in bytes.

- **Timestamp:** The time that the block is generated (in seconds since the genesis block).
- **Total amount TQT:** The amount has been transferred of all transactions of the block. The unit is calculated in TQT which is 1 CPC = 108 TQT.
- **Total fee TQT:** The total fee of all transactions of the block. The unit is calculated in TQT which is 1 CPC = 108 TQT.
- **Number of transactions:** The number of all transactions that the block bundled.
- **Generator RS:** The account address of the generator (forger) of the block.
- **Generator:** The account id of the generator (forger) of the block.
- **Generation signature:** The signature of the generator (forger) of the block.
- **Block signature:** The signature of the block that the generator (forger) signs.
- **Payload hash:** The hash of the block body.
- **Base target:** The base target of the block.
- **Cumulative Difficulty:** The cumulative difficulty of the block. This value will be used to decide which chain (blocks) should follow in case a fork happens.
- **Transactions:** The list of transactions that the block bundles.

*7.5.2. **How to become a validator***

A validator is a type of wallet that has provided its private key to a node, given that there is a minimum of one confirmed incoming transaction with 1440 confirmations. Upon meeting these criteria, the wallet assumes the role of a validator or forger within the blockchain. The wallet's effective balance, which consists of funds held for at least 1440 blocks, is staked and utilized by the node when selecting a validator for block generation.

Each node can have up to 100 validators. This value could be configured. This number is a parameter and can be changed however this change will lead to a hard fork on the chain.

*7.5.2.1. **How a validator is selected on a node**.* Every 500 ms, the node will sort the list of its validator. Then it goes through each validator from the top of the list and checks the forging condition using our forging algorithm. The first validator that satisfies the condition will gain the right to generate the next block.

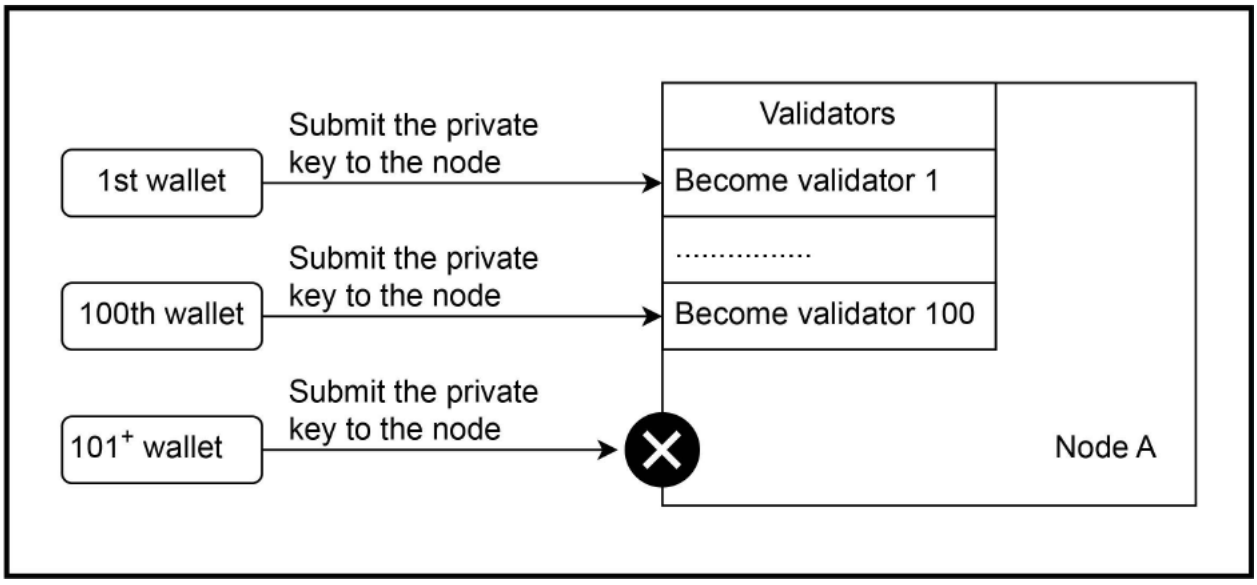


Figure 4: **Validator System**

7.5.2.2. ***How does the node sort the list of its validators?****.* Firstly, all forgers will calculate a value that is used to compare with each other. The lesser that value is, the higher it stands on the top of the sort list. At the end, the forger that has the smallest value will stand on the top of the sorted list. The calculated value should follow this equation:

$V = H \times Be$

where:

- V is the calculated value of a given forger.
- H is the hit value of that forger.
  - Each block on the chain has a generation signature parameter. To participate in the block forging process, an active account cryptographically signs the generation signature of the previous block with its own public key. This creates a 64-byte signature, which is then hashed using SHA256. The first 8 bytes of the resulting hash gives a number, referred to as the account's *hit*.

generationSignatureHash = sha256(signature of the last block + the public key of the validator)

temHit = generationSignatureHash

hit = BigInteger(1, temHit[7], temHit[6], temHit[5], temHit[4], temHit[3], temHit[2], temHit[1],temHit[0])

- B_e is the effective balance of the forger that a given forger compares to.

For example, we have 2 forger A & B that have the hit value and effective balance are [100, 2000] and [200, 1500], respectively. So the Va = 100 * 1500 (Value of A) and Vb = 200 * 2000 (Value of B). Then we got Va < Vb which means forger A should stand before forger B in the sorted list.

Secondly, in case the Va = Vb then the account id of each forger is used. The lesser that value is, the higher it stands in the sorted list.

7.5.3. ***Forging algorithm***

When does a validator satisfy the condition to generate a block?

Three values are key to determining which account is eligible to generate a block, which account earns the right to generate a block, and which block is taken to be the authoritative one in times of conflict: base target value, target value and cumulative difficulty.

7.5.3.1. ***Base Target Value*** . In order to win the right to forge (generate) a block, all active CPCx0 validators "compete" by attempting to generate a hash value that is lower than a given base target value. This base target value varies from block to block, and is derived from the previous block's base target value multiplied by the amount of time that was required to generate that block.

- blocktimeAverage = Average block time of the last three blocks
- If the average block time is greater than 15 seconds then we will increase the base target value using this formulabaseTarget = previousBaseTarget * Math.min(blocktimeAverage, 18)) / 15;
- If the average block time is less than or equal to 15 seconds then we will decrease the base target value using this formula baseTarget = previousBaseTarget - prevBaseTar-get * 64* (15 - Math.max(blocktimeAverage, 12)) / 1500

The minimum base target value is 15,372,286, and the maximum base target value is 854,015,900. Using this algorithm, we intend to keep our block time to be around 15 seconds given that a sufficient effective balance is available.

The parameters in the algorithm is fine tuned based on the optimization process and based on the theory foundation in this paper https://www.docdroid.net/e29h/forging0-5-1-pdf

7.5.3.2. ***Target Value*** . Each account calculates its own target value, based on its current effective stake. This value is:

$T = Tb \times S \times Be$

where:

- T is the new target value
- Tb is the base target value of previous block
- S is the time since the last block, in seconds
- Be is the effective balance of the account

As can be seen from the formula, the target value grows with each second that passes since the timestamp of the previous block. The maximum target value is 2.13503975x 1017. This target value and the base target value are the same for all accounts attempting to forge on top of a specific block. The only account-specific parameter is the effective balance parameter.

7.5.3.3. ***Cumulative Difficulty*** . This number is only used when the block is propagated to the network. The cumulative difficulty value is derived from the base target value, using the formula:

$$D_{cb} = D_{pb} + \frac{2^{64}}{T_b}$$

where:

- D_{cb} is the difficulty of the current block
- D_{pb} is the difficulty of the previous block
- T_b is the base target value for the current block

After the list of validators is sorted, the node goes through each validator and compares the hit of the validator to the current target value. If the computed hit is lower than the target, then the next block can be generated. As noted in the target value formula, the target value increases with each passing second. Even if there are only a few active accounts on the network, one of them will eventually generate a block because the target value will become very large. The corollary of this is that you can estimate the time that will be required for any account to forge a block by comparing that account's hit value to the target value.

The last point is significant. Since any node can query the effective balance for any active account, it is possible to iterate through all active accounts in order to determine their individual hit value. This means it is possible to predict, with reasonable accuracy, which account will next win the right to forge a block. A shuffling attack could be mounted by moving stake to an account that will generate the next block, which is another reason why a CPC stake must be stationary for 1440 blocks before it can contribute to forging (via the effective balance value). Interestingly, the new base target value for the next block cannot be reasonably predicted, so the nearly-deterministic process of determining who will forge the next block becomes increasingly stochastic as attempts are made to predict future blocks.

*7.5.4. **How a block is propagated?***

When a validator in a node wins the right to generate a block, it bundles up to 5000 available, unconfirmed transactions into a new block, and populates the block with all of its required parameters. This block is then broadcast to the network as a candidate for the blockchain.

Theoretically, each node can have one validator win the right to generate a block in the node which leads to the situation where multiple blocks are generated.

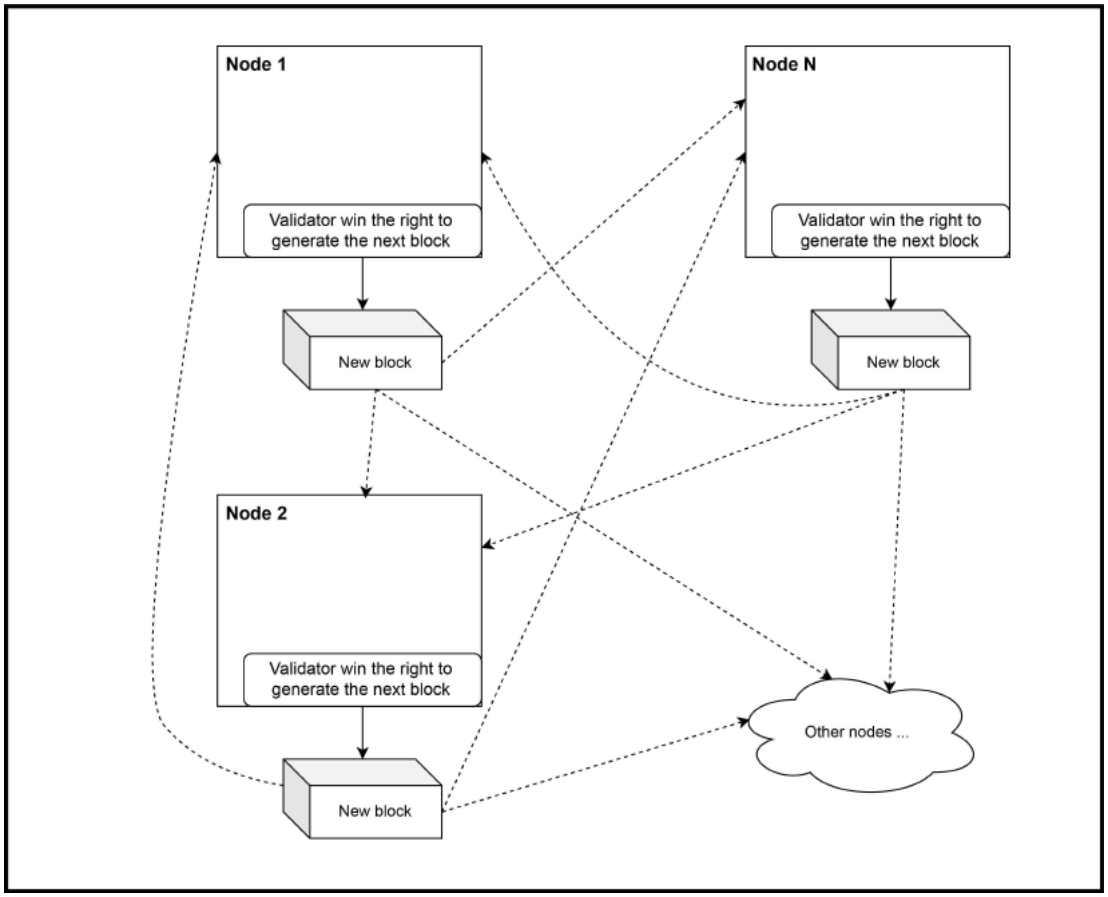


Figure 5: **How a block is propagated**

In this situation where multiple blocks are generated, when a node receives a block from another node, it will compare the received block with the block created by its validator. The node processes the block received from other nodes as following:

- If the previous block id of the processing block is the same as the last block id of the current node then it simply adds that block to its database.
- If the previous block id of the processing block is the same as the previous block id of the last block of the current node and the processing block has the timestamp (thetime the block is created) less than the timestamp of the last block of the current node then the node will remove its last block and add the processing block received from other node as new last block.

Otherwise the node simply ignores this block.

The situation where multiple blocks are generated is nearly impossible when the network runs normally, and it can only happen when some nodes are disconnected from the network for a while then try to connect to the network. The network handles this situation like a fork in the chain. In this case, nodes will select the block with the highest cumulative difficulty value as the authoritative block. As block data is shared between peers, forks (non-authoritative chain fragments) are detected and dismantled by examining the chains' cumulative difficulty values stored in each fork.

The nodes continue broadcasting the block to its peer until all the nodes agree on a block as the authoritative block. In case there are too many nodes on the chain, each node will synchronize/broadcast data with its first 2000 connected peers.

7.5.5. ***Block size***

In CPCx0 Chain, each block contains up to 5000 transactions, all prefaced by a 192-byte header that contains identifying parameters. Each transaction in a block is represented by a maximum of 176 bytes, and the maximum block size is 0.880192 MB.

The maximum of transactions that can be included in a block can be configured inside the code of the chain. Theoretically, we can set any value we want to this value since a block can contain as many transactions as it wants until it breaks its limit, when this happens transactions with higher transaction fee per byte (fee per byte = totalFee / transaction size) will be selected to be added in the block, the rest will be added in the next blocks.

All blocks contain the following parameters:

- A block version, block height value, and block identifier
- A block timestamp, expressed in seconds since the genesis block
- The ID of the account that generated the block, as well as that account's public key
- The ID and hash of the previous block
- The number of transactions stored in the block
- The total amount of CPC represented by transactions and fees in the block
- Transaction data for all transactions included in the block, including their transaction IDs
- The payload length of the block, and the hash value of the block payload
- The block's generation signature
- A signature for the entire block
- The base target value and cumulative difficulty for the block

In order to increase the block size, we will need to change the parameter in the code which specifies the maximum number of transactions in a block and the limit of transaction size. This will require a hard fork on the chain.

*7.6. **Transactions***

Transactions are the only means CPCx0 Chain accounts have of altering their state or balance. Each transaction performs only one function, the record of which is permanently stored on the network once that transaction has been included in a block.

*7.6.1. **Transaction Confirmations***

All CPC transactions are considered unconfirmed until they are included in a valid network block. A transaction included in a block receives one confirmation, with each subsequent block adding one more confirmation. Transactions not included in a block before their deadline expire and are removed from the transaction pool.

*7.6.2. **Transaction Deadlines***

Every transaction contains a deadline parameter, set to a number of minutes from the time the transaction is submitted to the network. The default deadline is 1440 minutes (24 hours). Transactions not included in a block before the deadline expires are removed from the network.

*7.6.3. **Transaction Types***

CPC transactions are categorized into types and subtypes, allowing for modular growth and development of the CPC protocol without creating dependencies on other "base" functions. New transaction types and subtypes can be added to support features as they are integrated, such as subscriptions, escrow, and automated transactions, known as advanced transactions.

*7.6.4. **Transaction Creation and Processing***

Creating and processing a CPC transaction involves the following steps:

- **Specify transaction parameters**: The sender specifies parameters for the transaction, including the private key for the sending account, a specified fee, a deadline, and an optional referenced transaction.

- **Check transaction inputs**: All values for the transaction inputs are checked, ensuring mandatory parameters are specified, fees are greater than zero, deadlines are at least one minute into the future, and referenced transactions are processed before the current transaction.

- Compute public key and validate parameters: If no exceptions are thrown during parameter checking, the public key for the generating account is computed using the supplied secret passphrase. Account information for the generating account is retrieved, and transaction parameters are further validated to ensure the sending account's balance is not zero and the unconfirmed balance is not lower than the transaction amount plus the transaction fee.

- **Create and broadcast the transaction**: If the sending account has sufficient funds, a new transaction is created with a type and subtype value matching the transaction being made. A unique transaction ID is generated, the transaction is signed using the sending account's private key, and the encrypted transaction data is placed within a message instructing network peers to process the transaction. The transaction is then broadcast to all peers on the network.

- **Server response**: The server responds with a result code, either the transaction ID if the transaction creation was successful or an error code and message if any parameter checks fail.

7.6.5. What's a transaction

Transactions are cryptographically signed instructions from accounts. An account will initiate a transaction to update the state of the CPCx0 Chain. The simplest transaction is transferring CPC from one account to another.

A CPCx0 transaction refers to an action initiated by an externally-owned account, in other words an account managed by a human, not a contract. For example, if John sends Bob 1 CPC, John's account must be debited and Bob's must be credited. This state-changing action takes place within a transaction.

7.6.6. How is a transaction created

When a human initiates a transaction through his wallet via a node, the transaction will be created and be put into the unconfirmed transaction pool. The sender specifies parameters for the transaction. Types of transactions vary, and the desired type is specified at transaction creation, but several parameters must be specified for all transactions:

Here are fields a transaction could have. The fields vary depending on type and subtype of a given transaction.

- **Transaction or transaction id:** The id of the transaction.
- **Signature:** the signature of the transaction.
- **Transaction Index:** The index of a transaction in a block.
- **Type:** The type of a transaction. We have 8 types for a transaction now.
- **Sub Type:** The sub type of a given type of a transaction. Each type of a transaction will have different subtypes that serve different purposes.
- **Amount TQT:** The amount that sender transfers to a recipient. The amount is calculated in TQT which is 1 CPC = 10^8 TQT.
- **Fee:** The fee of a transaction. The fee is calculated in TQT which is 1 CPC = 10^8 TQT.
- **Phased:** Indicate whether this transaction is controlled or not.

- **Recipient RS:** The account address of the recipient.
- **Recipient:** The account id of the recipient.
- **Sender RS:** The account address of the sender.
- **Sender:** The account id of the sender.
- **Block timestamp:** The timestamp of the block in which the transaction is bundled. The unit is calculated in seconds since the genesis block.
- **Timestamp:** The timestamp of the transaction. The unit is calculated in seconds since the genesis block.
- **Height:** The height of the block in which the transaction is bundled.
- **Deadline:** The deadline (in minutes) for the transaction to be confirmed. If a transaction has not been included in a block before the transaction deadline expires, the transaction is removed from the network.
- **Full hash:** The hash of the transaction.
- **Block or block ID:** The id of the block that the transaction is bundled.
- **Attachment:** Some transactions will have attachment. This field will specify the information that is attached to a given transaction such as what account controlled this transaction, etc.

Then, all values for the transaction inputs are checked. For example, mandatory parameters must be specified; fees cannot be less than or equal to zero; a transaction deadline cannot be less than one minute into the future; if a referenced transaction is specified, then the current transaction cannot be processed until the referenced transaction has been processed.

After that, if no exceptions are thrown as a result of parameter checking:

(a) The public key for the generating account is computed using the supplied secret passphrase

(b) Account information for the generating account is retrieved, and transaction param-eters are further validated:

- The sending account's balance cannot be zero
- The sending account's unconfirmed balance must not be lower than the transaction amount plus the transaction fee

Finally, if the sending account has sufficient funds for the transaction:

(a) A new transaction is created, with a type and subtype value set to match the kind of transaction being made. All specified parameters are included. A unique transaction ID is generated with the creation of the object

(b) The transaction is signed using the sending account's private key

(c) The encrypted transaction data is placed within a message instructing network peers to process the transaction

All CPCx0 transactions are considered unconfirmed until they are included in a valid network block. The validator bundles up to 5000 available unconfirmed transactions, the transaction with the higher fee per byte will be prioritized to be added in the block.

The newly-created block is distributed to the network by the node (and associated account) that creates them, and a transaction that is included in a block is considered as having received one confirmation. As subsequent blocks are added to the existing blockchain, each additional block adds one more confirmation to the number of confirmations for a transaction. If a transaction is not included in a block before its deadline, it expires and is removed from the transaction pool.

7.6.7. ***How are transaction broadcasted***

Once the transaction is put into the unconfirmed pool, it is broadcasted to the unconfirmed pool in other nodes. When all the nodes agree to add a block in the chain, every node will verify all data fields of the transaction again. The block will be rejected from adding into the database of the node if the node can not verify a transaction inside it.

7.6.8. ***Transaction types***

Categorizing CPCx0 transactions into types and subtypes allows for modular growth and development of the CPCx0 protocol without creating dependencies on other "base" functions. As features are added to the CPCx0 core, new transaction types and subtypes can be added to support them.

All actions on the CPCx0 Chain are recorded in the chain as a transaction. Hence, we will need to create a new transaction type for each new feature on the chain. This new transaction will be totally independent from existing transaction types. A new type of transaction will require a hard fork on the chain.

7.6.8.1. ***CPC Transfer Transaction****.* This type of transaction is used for ordinary payment when the user wants to transfer CPC to a wallet. Its type is 0 and its sub type is 0

7.6.8.2. ***Messaging Transaction****.*

- **Send private message:** Type 1 & Subtype: 0
  - This transaction is used when a user want to send an encrypted message to a wallet on the chain
  - This message will be included in the attachment of the transaction
- **Create a poll:** Type 1 & Subtype: 2
  - This transaction is used when a user want to create a pool on the chain
- **Cast a vote:** Type 1 & Subtype: 3
  - This transaction is used when a user want to make a vote in a pool on the chain
- **Approve controlled transaction:** Type 1 & Subtype: 9
  - This transaction is used when a user need to verify a transaction that has been set up multi-signature control with his/her wallet

7.6.8.3. ***Account Control Transaction****.* This transaction is used to set up multi-signature control for a wallet. Its type is 4 and its sub type is 1

7.6.8.4. ***Token & Asset Issuance Transaction****.* These transactions are used when a user wants to create a token or an asset on the chain.

- The type of transaction to create a token is 5 and its subtype is 0
- The type of transaction to create a asset is 2 and its subtype is 0

As a hybrid chain, we retain the permission to manage which token & asset can be created on our chain. All request to create a token or an asset must be made in https://devcenter.cpcoin.io/

7.6.8.5. ***Token & Asset Transfer Transaction****.* These transactions are used when a user wants to create a token or an asset on the chain.

- The type of transaction to transfer a token is 5 and its subtype is 3
- The type of transaction to transfer a asset is 2 and its subtype is 1

As a hybrid chain, we retain the permission to manage which token & asset can be traded on our chain. The administration team of CPCx0 Chain can manage it in the admin portal of https://devcenter.cpcoin.io/

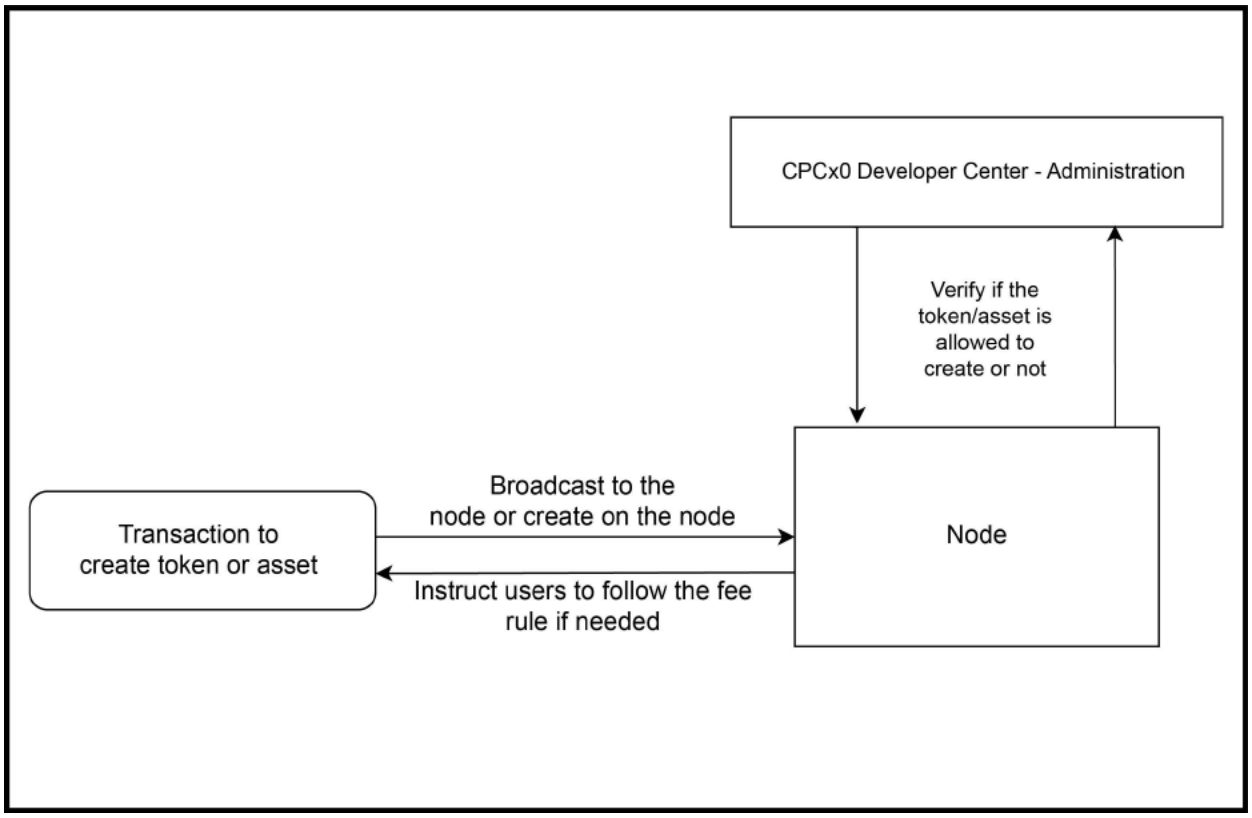


Figure 6: **Token & Asset Issuance Transaction**

*7.6.9. **Transaction Fee***

Transaction fees are the primary mechanism through which CPCx0 Chain are recirculated back into the network. When a CPCx0 Chain account forges a block, all of the transaction fees included in that block are awarded to the forging account as a reward. Until the size of all the transactions in a block exceeds the current 0.880192 MB, the standard fee (which is specified in tokenomic will be sufficient for all transactions to be included in blocks. In situations where the number of unconfirmed transactions exceeds the number that can be placed in a block, forging accounts will likely select transactions with the highest fees per byte. This suggests that transaction processing may be prioritized by including a fee that is higher than the standard.

The transaction fee is decided by the account's owner who initiates the transaction, however when the transaction is created, the node will verify the transaction fee. If the transaction does not meet the required standard, the node will ask the user to increase the transaction fee.

The fee rule for each transaction type is coded into the validation layer of the node and can be changed. Those changes will require a hard fork on the chain.

While CPCx0 Chain remains a private chain without open source code, the validation layer of the node requires all transaction fees to meet the standard. The standard fee of this transaction type is validated from the client side.

CPCx0 Chain will release to the public an update to securely create CPC transfer transactions with the minimum fee of 0.00000002 CPC.

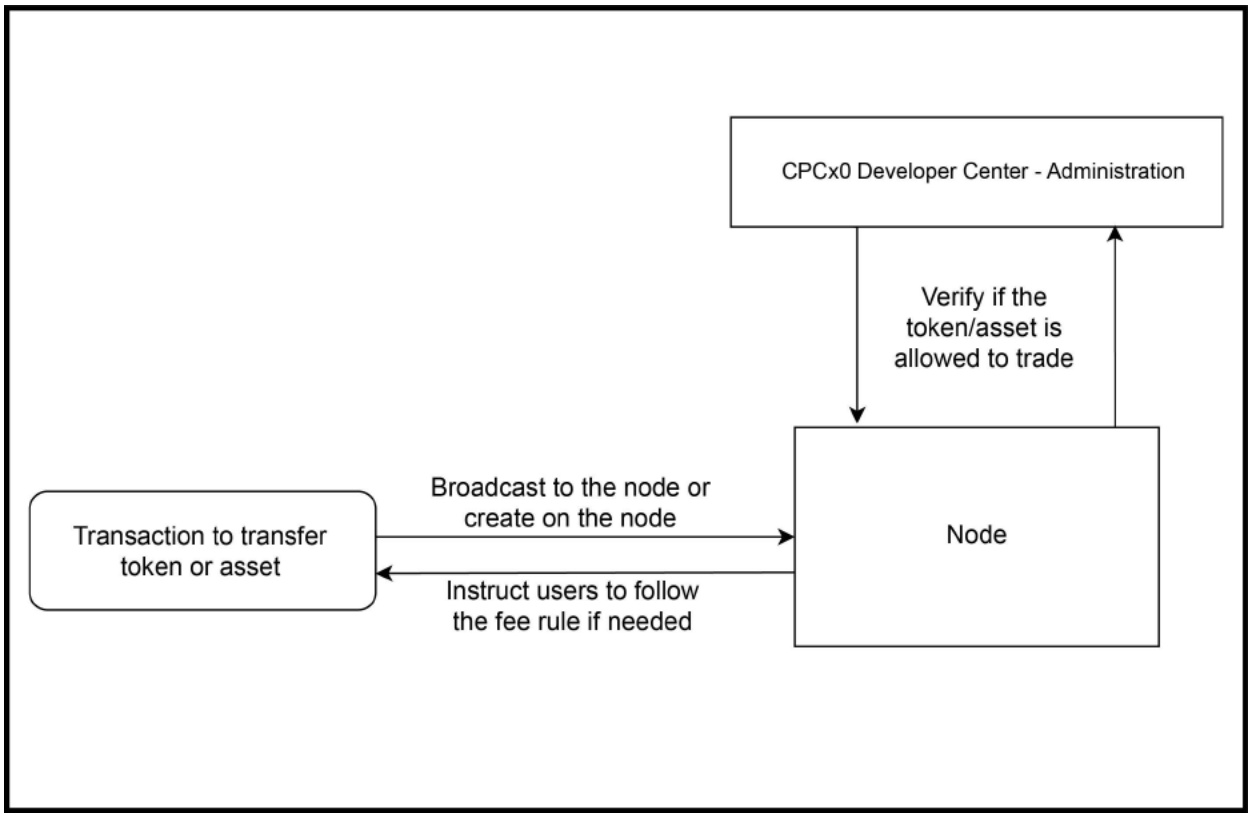


Figure 7: **Token & Asset Transfer Transaction**

*7.7. **Accounts***

CryptoPerformance Coin (CPC) incorporates a brain wallet design, where private keys for all possible account addresses are directly derived from each account's passphrase using a combination of SHA256 and Curve25519 operations. Each account is represented by a 64-bit number, which is expressed as an account address using Reed-Solomon error-correcting notation. This notation can detect up to four errors or correct up to two errors in an account address.

This format was introduced to address concerns that misstyped account addresses could lead to irreversible token, alias, or asset transfers to erroneous destination accounts. Account addresses are always prefixed with "Cx0", ensuring easy recognition and differentiation from other cryptocurrency address formats.

The Reed-Solomon encoded account address associated with a secret passphrase is generated as follows:

- The secret passphrase is hashed with SHA256 to derive the account's private key.
- The private key is encrypted with Curve25519 to derive the account's public key.
- The public key is hashed with SHA256 to derive the account ID.
- The first 64 bits of the account ID form the visible account number.
- Reed-Solomon encoding of the visible account number, prefixed with "Cx0", generates the account address.

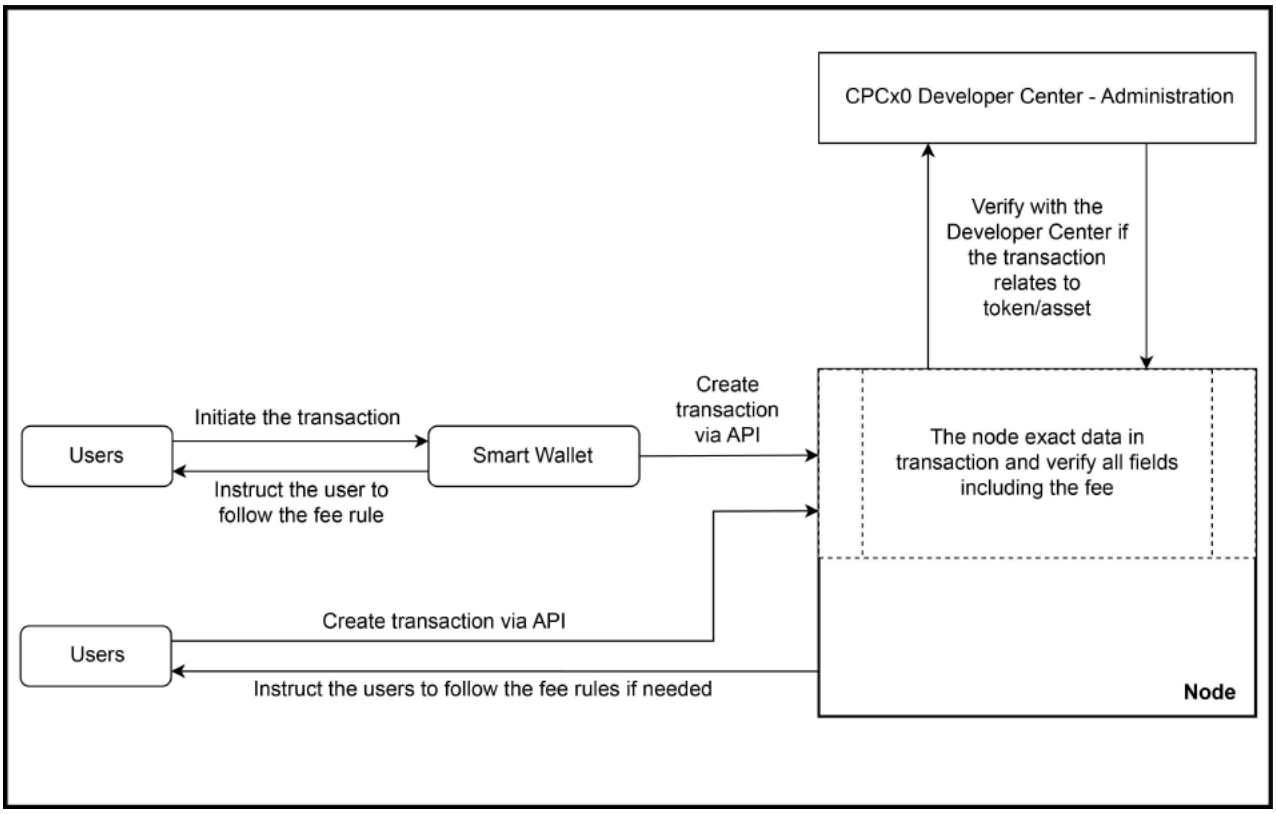


Figure 8: **Transaction Fee Mechanism**

When an account is accessed for the first time using a secret passphrase, it is not secured by a public key. Upon initiating the first outgoing transaction from the account, the 256-bit public key derived from the passphrase is stored on the blockchain, securing the account.

The address space for public keys (2^256) is larger than the address space for account numbers (2^64), resulting in no one-to-one mapping of passphrases to account numbers and potential collisions. To detect and prevent these collisions, a specific passphrase is used to access an account, and once that account is secured by a 256-bit public key, no other public-private key pair can access that account number.

*7.7.1. **Account Balance Properties***

CPC accounts have several distinct balance types, each serving a different purpose and often checked during transaction validation and processing:

- **Effective balance:** This balance is used as the basis for an account's forging calculations. It consists of all tokens that have been stationary in the account for 1440 blocks. The Account Leasing feature also allows an account's effective balance to be temporarily assigned to another account.

- **Guaranteed balance:** This balance consists of all tokens that have been stationary in an account for 1440 blocks. Unlike the effective balance, this balance cannot be assigned to any other account.

- **Basic balance:** This balance represents all transactions that have had at least one confirmation.

- **Forged balance:** This balance displays the total quantity of tokens earned as a result of successfully forging blocks.

- **Unconfirmed balance:** Displayed in CPC clients, this balance represents the current balance of an account minus the tokens involved in unconfirmed, sent transactions.

- **Guaranteed asset balances:** This balance type lists the guaranteed balanes of all assets associated with a specific account.

- **Unconfirmed asset balances:** This balance type lists the unconfirmed balances of all assets associated with a specific account.

7.8. ***Cryptographic***

Elliptic curve cryptography (ECC) is a public key cryptography method that uses elliptic curves algebraic structures over finite fields. ECC provides security with smaller keys compared to other cryptographic methods and can be used for key agreement, digital signatures, pseudorandom generators, and more. In CPC, key exchange is based on the Curve25519 algorithm, while message signing is implemented using the ECKCDSA algorithm.

7.8.1. ***Encryption Algorithm***

When Alice sends an encrypted plain text to Bob, the following steps are taken:

- Calculate shared secret: Alice computes the shared secret using Curve25519(Alice_private_key, Bob_public_key).
- Calculate N seeds: Alice computes N seeds using seedn = SHA256(seedn1), where seed0 = SHA256(shared_secret).
- Calculate N keys: Alice computes N keys using keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X.
- Encrypt plaintext: Alice computes the ciphertext using ciphertext[n] = plaintext[n] XOR keyn.

Upon receiving the ciphertext, Bob decrypts it as follows:

- Calculate shared secret: Bob computes the shared secret using Curve25519 (Bob_private_key, Alice_public_key).
- Calculate N seeds: Bob computes N seeds using seedn = SHA256(seedn1), where seed0 = SHA256(shared_secret) (identical to Alice's step).
- Calculate N keys: Bob computes N keys using keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X (identical to Alice's step).
- Decrypt ciphertext: Bob computes the plaintext using plaintext[n] = ciphertext[n] XOR keyn.

Note : If someone guesses part of the plaintext, they can decode some part of subsequent messages between Alice and Bob if they use the same key pairs. Therefore, it's advised to generate a new pair of private/public keys for each communication.

8. Conclusion

In this white paper, we introduce a comprehensive ecosystem for the digital economy, leveraging the transformative power of blockchain technology and cryptocurrencies. As the landscape of finance evolves, the integration of cryptocurrencies is revolutionizing trust, security, and seamless collaboration across a global system that unites financial institutions, institutional investors, everyday users, and small to large-scale businesses.

The CPC decentralized crypto ecosystemis a groundbreaking project that converges multiple advancements in integration, user experience, and middleware system configurations to establish a robust foundation for contemporary financial applications, as well as those of the future. This innovative model empowers intermediaries to develop bespoke financial services and construct a distributed, super financial market ecosystem through the CPC ecosystem.

Our vision is centered around the belief that a flexible, decentralized value exchange system represents the future of global financial infrastructure. Such a system has the potential to foster financial inclusion, standardize future financial transactions, and redefine the way we conduct business in a digital age.

In contrast to many existing cryptocurrencies, the design philosophy of the CPC ecosystem emphasizes cooperation and feature integration, rather than isolated solutions. This collaborative approach ensures a more cohesive and interconnected financial ecosystem, capable of unlocking untapped potential and driving unprecedented growth.

Ultimately, the CPC decentralized crypto ecosystem aims to revolutionize the digital economy by providing a secure, scalable, and accessible platform that empowers users, businesses, and financial institutions to thrive in an increasingly interconnected world. By embracing the transformative capabilities of blockchain technology, we aspire to pave the way for a new era of financial innovation and inclusivity.

9. References

*9.1. **CPC Resources***

CPC API Tools: https://tools.cpcoin.io

*9.2. **Additional White Papers used for reference***

- Nxt
- Burst
- Heat
- Fimk
- NEM
- Ethereum
- Tendermint
- IPFS

*9.3. **References***

1. Satoshi Nakamoto. Bitcoin: a PeertoPeerElectronic Cash System. (n.d.).Retrieved July 06, 2014, from https://bitcoin.org/bitcoin.pdf
2. ZeroNet, Open, free and uncensorablewebsites using Bitcoin cryptography and BitTorrent network, https://zeronet.io/
3. NxtWhitepaper, http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt
4. Tendermint: Consensus without Mining, 2014 https://tendermint.com/static/docs/tendermint.pdf
5. P2P MiCx0g and UnlinkableBitcoin Transactions
6. IPFS is the Distributed Web
7. Wikipedia, Diffie–Hellman key exchange, https://en.wikipedia.org/wiki/Diffie%E2%8 0%93Hellman_key_exchange
8. Yung, M., Dodis, Y., Kiayias, A., Malkin, T., & Bernstein, D. J. (2006). Curve25519: New DiffieHellmanSpeed Records. Public Key Cryptography, 2006, 207228. doi: 10.1007/11745853_14
9. The Korean CerticatebasedDigital Signature Algorithm
10. Sidechains. Deposit/withdrawal sidechain, https://www.blockstream.com/sidechains. pdf
11. What Proof of Stake Is and Why It Matters http://bitcoinmagazine.com/6528/, 2013
12. Matthew Green et al. Zerocash: Decentralized anonymous payments from bitcoin.
13. National Institute of Standards. FIPS 1802, Secure hash standard, August 2000.
14. JavaScript, Object Notation. See http://json.org/

CryptoPerformance

Contact and Social Media

contact@cryptoperformance.io

cpcoin.io