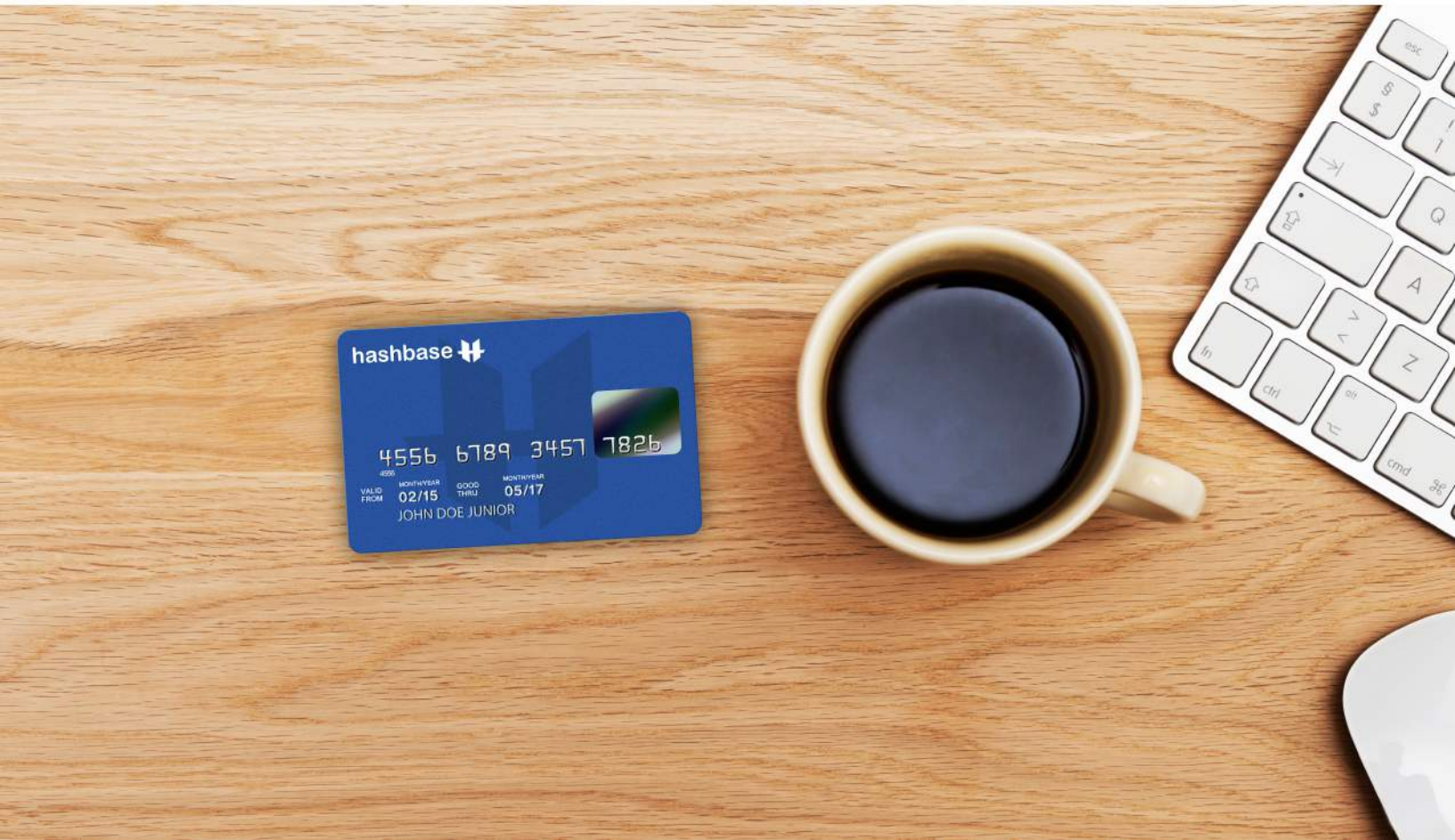
Paycoin

A Cryptocurrency fit for world adoption

White Paper



Abstract

This paper examines Paycoin™, from a technical and practical perspectives as a new cryptocurrency designed to facilitate mass adoption and long-term valuation stability. While cryptocurrency is not a new industry, existing cryptocurrencies have failed to achieve widespread adoption, largely due to their inability to provide a stable network for participants as well as a stable source of value for adopters. The current cryptocurrency environment requires mining participants to invest in hardware that is quick to obsolescence. This environment creates an arms race of computational power investments as mining participants are in constant haste to remain relevant and cost-effective in their mining efforts. Paycoin™ employs a "Smart Proof-of-Stake" protocol preventing this phenomenon while promoting long-term sustainable price stability. Moreover, Paycoin™ introduces Prime Controllers™, distributed high-staking transactional processing nodes that can be acquired temporarily via an algorithmic bidding system. Prime Controllers™ automatically adjust the creation rate of Paycoins™ in response to real market demand, creating long-term stable valuations, dramatically lowered transaction times over legacy cryptocurrencies, all while also creating a lucrative environment for market-maker investments in the currency.

Paycoin™ is the first cryptocurrency to employ a HybridFlex blockchain, expanding on the work of Satoshi Nakamoto, in order to produce a light, efficient, highly-secure blockchain, accessible to nearly all internet connected devices. The HybridFlex model produces a cryptocurrency that offers ease of consumer adoption and use, ease of infrastructure support, while also facilitating large-scale investor entry into the cryptocurrency industry; Augmenting the creation, management and deployment of a competitive global payments and commerce system.

Table of Contents

1 What is Cryptocurrency?

Cryptocurrency is a digital monetary unit (coin) that utilizes public key cryptography to secure and perform anti-counterfeiting functions embedded within the currency unit. Public and private keys are used as entries to form a public ledger, called a “blockchain,” in order to prevent simultaneous ownership, or spending, of a monetary unit by one or more individuals.

Cryptocurrency’s network cryptography techniques are cited as the first solution to the “double spending problem” in computer science.

As an achievement in both technology and commerce, units of cryptocurrency represent scarce digital resources. Unit valuations are determined by semi-consensual supply and demand forces within marketplaces, rather than valuations backed by other commodities, such as silver or gold bullion. Moreover,since cryptocurrencies are neither created nor controlled by external central bank authorities, these external authorities are equally unable to influence their valuations. Monetary policy of cryptocurrency — forces that promote inflationary or deflationary effects on money supply — are controlled by algorithmic functions, rather than by the judgment of individuals.

2 What is Proof of Work?

Proof of Work (PoW) is a protocol used to secure transactions and issue newly created digital coins to individuals.

Cryptocurrency relies on a distributed network of nodes reaching consensus on the legitimacy of individual transactions. A coin can only belong to one address (wallet) at any given time. To enforce this, the network creates what is called a “blockchain” public ledger recorded on each node on the network. The blockchain tracks transfers of cryptocoins to and from wallets in order to prevent counterfeiting and double spending. Transactions are executed only when the network agrees that the transferred coins are legitimately and singularly owned by the transactors and that the sending party was the last recorded recipient of said coins. This is performed by validat ing digital signatures against the blockchain by participants in the network.

To prevent third parties from creating false transactions, the network employs a roadblock called “Proof-of-Work” (PoW), wherein nodes on the network must find solutions to difficult mathematical equations before earning permission to edit the blockchain. This, along with the fact that each transaction must reach agreement from the majority of the other nodes on the network means that manipulation of the blockchain requires resources greater than half of the active nodes on the network.

Proof-of-work requires time and energy to perform. What incentivizes individuals to connect their nodes to the network and perform this work of validating transactions are that new cryptocoins are issued to these nodes based on the number of mathematical solutions they solve. This compensation is called the “block reward.” The more work a node performs, the more transactions it verifies, and thus, the more coins awarded.

3 What is Proof of Stake (PoS)?

Proof-of-Stake (PoS) is an alternative protocol to Proof-of-Work (PoW) for securing transactions and issuing new coin rewards to individuals.

Rather than the ability to contribute to the blockchain being granted by supplying to computational power, access to the blockchain is granted by ownership of the cryptocurrency itself; using open wallets connected to the cryptocurrency's network. Anyone with an ownership "stake" in the cryptocurrency has the ability to connect to the network and contribute to securing and processing transactions, while earning newly-issued currency based on this participation.

Proof-of-Stake is considered, by many, as a superior protocol to Proof-of-Work in that it is more environmentally friendly, requiring far less energy and computational power than proof-of-work. This application adds incentive to hold cryptocurrency, greatly encouraging price stability, while also rendering the observed hashing power "arms race," in PoW models, potentially obsolete. This protocol also increases individual participation in the transaction securing process.

The concept of "stake" creates a barrier to entry for bad actors, who may try to attack the payment system. In order to participate in the processing and rewards of a proof-of-stake currency, an individual must hold a portion of the currency. This, by its very nature, makes attacks more expensive as coins are not reusable for other purposes, whereas in a Proof-of-Work coin, resources could be used in a self-serving manner, being redirected towards multiple coins and tasks. HashCoin™ leverages this "skin-in-the-game" concept with its tiered controller network and exclusive barrier to entry for "Primary Node" operators.

4 Why release a New Coin?

Cryptocurrency is shifting the economic paradigm. By introducing blockchain technology, and proving that digital scarcity is possible, cryptocurrencies, and the networks that process them, have formed a proof-of-concept that, decentralized digital money can provide a value proposition that has never before been contemplated in global commerce.

However, as legacy cryptocurrencies age, it becomes increasingly clear that these coins' networks face enormous challenges in promoting price stability, maintaining decentralization, and ensuring ease of use, all of which severely hinder adoption.

To date, all cryptocurrencies have failed to achieve mainstream adoption due to their inherent shortcomings.

Paycoin™ changes this for the first time. It carries with it the most compelling features of existing cryptocurrencies, while making key advancements necessary to produce a coin network that is fast-transacting, safe and secure, decentralized, and favors price stability over speculation; a currency highly suitable for global adoption.

Paycoin™ is unique among cryptocurrencies in that its Initial Coin Offering (ICO) creates the world's first Coin Adoption Fund (CAF), a multi-tier, organized strategy for increasing global adoption. The CAF is divided into three equally sized budgets; (1) funds for promoting adoption with APIs, plugins, and apps; (2) funds for maintaining a fiat exchange, providing the necessary liquidity for merchant adoption, and; (3) funds for developing proprietary hardware to distribute to miners at cost.

In addition, Paycoin™ also introduces Prime Controllers™, which incentivize large

4 Why release a New Coin? *(cont.)*

investment interests to participate actively in the Paycoin™ network, removing bad actors or non-performing peers, promoting long-term price stability, and dramatically increasing transaction speed over legacy cryptocoins.

The rationale behind the creation of a new coin is simple: Existing cryptocurrencies use legacy platforms which are currently facing increasing problems in the areas of price stability and adoption. A new coin that solves these issues is poised to bring the benefits of cryptocurrency to the global marketplace; that is what Paycoin™ achieves.

5 Technical Coin Specifications

5.1 PoW

5.1.1 Proof of Work Time Period

The Paycoin™ PoW mining phase will last until the initial allotment of coins needed, are mined. In this proof-of-work phase, any miners wishing to participate in mining Paycoin™, will be allowed to commence mining.

During the proof-of-work phase the "thermodynamic, reverse corollary, difficulty algorithm" will dictate a 12.5 million coin mintage limit[1]. Of the initial 12.5 million coins minted an allotment of approximately 5.5 million coins will be distributed to the Initial Prime owners and those who participated in an initial Paycoin™ acquisition program. As the difficulty rises, the reward will inversely correlate, seeking an equilibrium between the amount of work accomplished to process transactions, and the reward structure accomplishing the work. Difficulty re-targets every block, with a block time of 1 minute. In this phase the initial 50 Prime Controllers™ will be deployed . The Paycoin™ network will utilize a five-network-confirmation protocol, versus a 51% consensus of the Prime Controllers™, to generate new coins, while the network of Prime Controllers™ is deployed in preparation of the Proof-of-Stake phase.

[1] As several Prime Controllers™ have already been reserved a portion of coins equal to those reserved will be allocated to the first set of Controllers™ coming online prior to the first network auction.

5.1.2 Growth-Protected Reward Scheduling

One of the complications of a fixed-supply, closed-currency system, with a declining block reward schedule, utilized by other cryptocurrencies, is the eventuality of predictable mining network disruptions and distortions, during each mining profitability modification that occurs instantaneously.

Paycoin™ provides a solution to this sudden block reward halving: A "Growth-Protection" reward scheduling system, derived from thermodynamic, closed systems, exchange of energy. This equation establishes a leading and trailing baseline, from which a gradually declining block reward can ensure a consistent supply of currency, being introduced into the closed system.

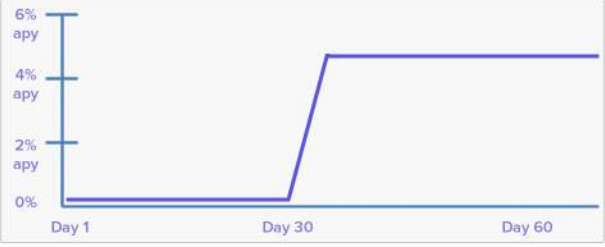
This Growth-Protection block reward schedule system protects against the rapid deflationary effect (block halving) on the currency, that occurs over the duration of the coin's life. The miner who mines the final block, will receive a proportional block reward that is derived over the existence of the Proof-of-Work stage, in relation to difficulty of the mined block.

5.2 PoS

Coin holders who maintain an online node and continiously participate in the Paycoin™ network by verify transactions and enabling advanced blockchain features are rewarded with Staking.

For a coin to be eligible for staking, it must exist in a single, active wallet node for 30 days or longer. This is determined by a variable that records time a coin exists within a wallet. Once a coin is transferred from one wallet to another, this variable resets. Coins that have matured to 30 days generate a stake of approximately 0.4%[2] each month[3].

Figure 5.2.1 - Paycoin Staking



5.3 Transaction fees

Paycoin™ transaction fees are based on the type, amount and size of the transaction being sent. Both one-to-one and many-to-one transactions will have an associated fee deducted from the receiver. For one-to-many and many-to-many transactions, the fee will be paid by the sender. This reduces end user confusion, while supporting consumer to merchant spending activities, with a known and understandable transactions model. Transaction fees will initially be distributed to all of the Orion Controllers™ exclusively (See Section “Orion Controllers™”). Fees are designed to be negligible, but sufficient to, prevent blockchain spamming and attacks. Transactions which send an amount less than the fee amount will be rejected as invalid, and returned to the sender[4].

[2] Tthe overall node stake is equivalent to 5% APY with monthly stake periods.
[3] Month is relative to a normalized number of days not to a calendar month. The number of days in each staking period is ~ 30.4375 calculated as 365.25 days divided into 12 equal periods.
[4] As an additional measure to prevent network abuse addresses sending many micro transactions smaller than the network fee will be declined processing by the network and destroyed.

5.4 Blockchain Features

5.4.1 Hybrid Flex Blockchain

With current implementations of crypto-currencies, in order to create near-instant verification of transactions a system must lower the block generation time, having the effect of greatly increasing the number of orphaned blocks, and therefore decreasing the overall stability of the blockchain. Paycoin™ provides a new solution to this block time versus stability dilemma, with a network of highly connected and capable Prime Controllers™, while also reducing blockchain bloat with the new HybridFlex Blockchain.

HybridFlex Blockchain provides archival and final confirmation of all balances, enabling new Paycoin™ nodes to participating on the network, immediate access to the current HybridFlex Lite Blockchain Ledger. New nodes are able to download the "lite chain" containing only the period's most recent balances and transactions; updating new transactions as they appear. The HybridFlex Blockchain also enables transactional messages and an extensible blockchain API.

During each consolidation, or Flex interval, a list of ledger balances is written to a new ledger that contains only current balances and recent transactions. All blockchain history is maintained in the full chain on Prime and Orion Controllers™. Wallets, Mobile Apps and Merchants can download the smaller Flex Blockchain preventing wait times during the process of synchronizing balances.

5.4.2 Immutable Transactions

Since their introduction, inherent design flaws have hampered their adoption and usability. To complete a transaction, all parties in the agreement must wait for outside confirmation, through a blockchain, for the validity of the transaction to be accepted. This vital step, in the exchange of monetary units, can take between 10 and 30 minutes to complete with today's merchant-accepted cryptocurrencies.

Paycoin™ solves this inherent flaw by introducing Transactional Immutability into the backbone of the currency. Paycoin™ Transactional Immutability places a transactional lock on a transaction, which is broadcast immediately, network-wide, to gain consensus before being packaged into a block for later confirmation. This allows the Paycoin™ network to process a transaction within seconds.

One-to-One Payments (Transactions) Process

1) A Node (wallet or merchant) broadcasts a transaction on the network
2) The closest Prime Controller™ verifies transaction validity
    a) If the transaction is not verified by this Prime Controller™ the transaction is rejected and a rejection message is broadcast.
3) The processing Prime node temporarily locks the transaction and broadcasts a verification request to it's adjoining nodes who verify and do the same.
4) Transaction balance is verified by a majority consensus of the Prime nodes.
    a) Response is sent (TX Success/TX Denied)
    b) Nodes spread TX to gain consensus
5) Upon consensus all nodes write the transaction into the current block being solved.

5.4.2 Immutable Transactions *(cont.)*

Pseudo Proof of Concept Code:

```
PrimeController::TI_Sent_Transaction() {
    TI1 = POWHash (nBlockHeight ~ Proof-of-Transactional-Viability(nth) );
    TI2 = SHA256( TI1 ) * Difficulty(n);
    TI3 = Return ( TI2 - PrimeController( directive ) );
    return TI3;
}

PrimeController::TI_Locked_Transaction() {
    TILT = PrimeController.TI_Sent_Transaction();
    if ( TILT = PrimeController(Verified_Transaction( mrch ) ) {
    BlockConfirmation = true;
        }
    }
}
```

This immediacy of transactional verification enables Paycoin™ to maintain a streamlined and efficient blockchain with periodic self-reconciliation and archival capabilities while not sacrificing transaction speed, transparency, stability or size of the full blockchain.

5.4.3 FundSafe

MultiSig (Multiple signature) wallets are becoming more and more common, while being the needed defacto standard. Paycoin™ adds to this security measure by introducing FundSafe on chain wallet locking. Web services can be built upon the blockchain locking system, allowing for users to lock and unlock wallet addresses using additional authentication mechanisms. User friendly locking systems can then be used, such as two factor authentication (2FA), utilizing temporal tokens, mobile devices, or biometric signatures, making off-chain cold storage obsolete.

5.4.4 Extensible Blockchain (EBC)

Paycoin™ features an "Extensible Blockchain" with "HashCodes" allowing for any number of extended capabilities, services and products to be built on top of the Paycoin™ network. The HashCode message space contains a one-way algorithmic hash of a message, file or receipt. Merchants can easily build upon this capability and send daily batch messages, which are one-to-many transactions, containing hashed copies of customer receipts. This allows merchants to build websites that interact with the Paycoin™ blockchain, to display verifiable receipts and purchase histories to customers. Customers can view, through trusted applications, the compared value of a receipt and it's HashCode to verify it is unchanged. This also applies for on-chain smart contracts, advertising Pay-Per-Impression and Pay-Per-Click micropayments, Remote Peer-to-Peer Sensor networks with verifiable metrics and return payments, Proof-of-Concept claims, as well as many currently undeveloped services and uses for the additional message space. While this is inherently similar to that of other cryptocurrencies, we have structured the HashCode system to work in a scalable and future-ready implementation of the HybridFlex blockchain technology.

5.4.4 Extensible Blockchain (cont.)

5.4.4.1 Proof of Concept Claims

Allows for sending a transaction of an arbitrary amount containing a HashCode message to record an idea or text, marking the original date and time of the idea in the archival blockchain. This is a novel idea within other blockchains, however the current implementations are not user-friendly. API's can be built to query the Paycoin™ Network to allow websites to interact with the blockchains Proof-of-Concept database.

5.4.4.2 Time based contracts

Using the hash message space, FundSafe and FundSwap, with expiring dates' contracts and agreements, can be written between multiple parties with escrows, signing and timed funds release with backup fund return for contract cancellations.

5.4.4.3 Smart Property

Tying a physical device's UID to a hashed message within the blockchain. Physical property can be tagged to an owner and ownership can be transferred via the blockchain, so a true owner of an asset can be cryptographically verified.

5.4.4.4 Advertising Micro Payment System

Using the message space of the HashCoin™ blockchain, one can send a payment to apply as a provider, on an advertising network, enclosing a copy of the unique referral code. Providers can send back payments on a regular basis for clicks, impressions, conversions, affiliates, signups or any other measure.

5.4.4.5 Crowdfunding

Crowdfunding companies can use the block-chain to remove relance on "trusted" third-parties. Donors/Backers would be able to verify the recipients of all funds sent on the platform. The funds could also be returned if funding targets are not met. In effect, crowd-funding failures could be eliminated on a blockchain platform using Time Based Con-tracts.

5.4.1 Voting System

Votable items theoretically could be anything from contract negotiations to code changes in the codebase for Paycoin™. Additional architecture may be needed to accomplish a custom voting system. A Vote passes when a majority of Prime Controllers™ cast an affirming vote within the established voting time-frame. Moreover, Orion Controllers™ can vote on specified changes or override ties in Prime Controller™ voting. Each Orion Controller™ casts a vote equal to their wallet balance (coin stake). The total votes are counted, and a two thirds majority wins. If an actor does not vote, the network disqualifies the candidate and the null vote is removed.

5.4.6 Proxy Voting system

Prime Controllers™ wishing to assign proxy votes may do so by allowing their proxies to send a small transaction, assigning their vote in the transaction to another, single Prime Controller™. The Prime Controller™ will then package all the votes into one transaction and submit all the votes at once with multiple hashes being in the URI.

5.4.7 Built in escrow

Trustless transactions are not always ideal for users wishing to remain anonymous or geographically diverse. Leveraging the Prime Controller™ bidding system, Paycoin™ introduces on-chain blockchain escrow for time-based escrows. Two parties can, with the aid of a mutually trusted third-party, send a transaction, with escrow requirements, to initiate a time-based escrow contract. At any time, prior to the expiration of the contract, the third-party can release the funds to the sender or recipient of the contract.

5.4.7 Built-in Escrow *(cont.)*

To set up an escrow transaction, users will send a payment to the network containing a flag for escrow, which will also contain a fixed amount of escrow data. When setting up an escrow transaction on the blockchain, the Paycoin™ network will use the following variables:

- Senders' address
- Expiration Date in unix time
- Second signing key required to release funds
- Recipients' address

To release escrowed transactions either the timer on the escrow must expire releasing the funds back to the sender or the escrow key holder must send a release transaction to the original escrow address.

6 Controller Types

6.1 Orion Controllers

Orion Controllers™ are unpromoted Prime Controllers™ who are willing to dedicate more time in securing the network than standard or lite nodes. They will still receive the normal stake of 5%[5] as does the rest of the Paycoin™ network. However, these elevated operators will be privy to some new privileges and benefits. In order to be an Orion Controller™ you must dedicate more effort than the average Paycoin™ node. In this regard, an Orion Controller™ is similar to other tiered-node concepts. However, Orion Controller™ managers are incentivized beyond the network stake rate for participating in several responsibilities, including:

- Performance of network confirmations and communications;
- Routing system verification;
- Participatation in tiebreaker voting;
- Storing a copy of the full HashCoin™ blockchain (i.e. non-HybridFlex block chain);
- Performing as partial Prime Controllers™ when needed in the unlikely event case of a shortage;
- Acting as a gateway for off-chain API's and services, and;
- Acting as a backbone for third party services utilizing the Paycoin™ block chain.

[5] Orion Controllers™ stake at the standard 5% APY rate on monthly stake periods see (3) for additional technical details on stake rates and time definitions

6.1 Orion Controllers *(cont.)*

In exchange for performing the above responsibilities, Orion Controllers™ are incentivized in the following ways[6]:

- All Orion Controllers™ will receive a proportional share[7] of transaction fees;
- All Orion Controllers™ will receive a proportional share of the bid fees during each Prime Controller™ bid period and;
- All Orion Controllers™ will receive a proportional share of payments and fees sent for advanced blockchain features, such as Escrow, Wallet Locking, HashCode messaging.

Orion Controllers™ have the exclusive right to bid on open Prime Controller™ slots and be promoted to Prime Controllers™ if they win.

6.1.1 Initial Orion Controller™ Distribution

Upon launch, any qualified node will be able to operate as an Orion Controller™.

[6] Fee distribution to Orion Controllers™ may shift at times when new coin production is limited.
[7] The per Controller™ share is determined based on network participation and total coin stake owned.

6.2 Prime Controllers

Prime Controllers™ on the Paycoin™ network are the backbone of the system, which enable Transactional Immutability to occur and be confirmed, within a near-instantaneous response timeframe. Controllers exist in the peer-to-peer network to supply the computing power needed for transactional locking that occurs as part of the Transactional Immutability capabilities of Paycoin™. These Controllers interact with Paycoin™ Orion Controllers™ for consensus and verification of transactional blocks.

6.2.1 The Hard Problem of Quantity Theory

For a currency to achieve stable prices, relative to other goods, the supply of currency must increase as demand for the currency increases. Achieving a dynamic relationship between supply of coins and demand of coins has been an unsolved problem in cryptocurrency.

Existing cryptocurrency algorithms define currency creation rates globally by arbitrary parameters irrespective of demand. Economic Quantity Theory deems that, for a currency to achieve long-term price stability, the creation rate of currency must adapt to real-time demand for the currency. In short, if demand for a currency remains constant, then increasing the supply of currency rapidly will result in a reduction of value in the currency. However, if demand for a currency increases the supply of that currency must also increase proportionately, to ensure a stable value.

Prime Controllers™ employ an algorithmic

6.2.1 The Hard Problem of Quantity Theory *(cont)*

process that quantifies demand and allows the supply rate of Paycoins™ to adapt to changes in demand. Prime Controller™ wallets stake at a much higher rate than other wallets. As demand for HashCoin™ increases, it follows that demand for Prime Controllers™ will increase in response. This demand is measured by increasing bids for Prime Controllers™, during their bidding phases, as they become available. As Prime Controller™ bids increase, the number of Paycoins™ entering higher staking wallets increases. This means more coins stake at a higher level and thus the creation rate of Paycoins™ increases in response to the increase in demand. The opposite holds true as well, for times when demand decreases.

Prime Controllers™ are a mechanism that allows a cryptocurrency's creation rate to adapt to market demand in real-time, in order to produce self-stabilizing currency value.

6.2.2 Prime Controller™ Functions

The Prime Controller™ serves multiple purposes in its goal of protecting the integrity of Paycoin's™ network including:

- Performing the archiving functions on the HybridFlex Blockchain;
- Providing reconciliation instructions for the blockchain to Orion Control lers™;
- Performing as the first entry point of a transaction into the network (border security, if you will), thereby verifying that no illicit transactions hit the open network, (i.e. double spend checking);
- Participate in voting on any code changes and/or possible forks to the blockchain, and;
- Prime Controllers™ have the exclu sive right to perform inter-blockchain cold storage functions[8].

In exchange for performing the above responsibilities, Prime Controllers™ are incentivized by the following:

- Stake rate of 5% on all funds locked in the winning bid address[9];
- Ability to participate in an aggregate stake;
- Voting rights to proposed changes in the codebase, and;
- Receive a proportional share[10] of all advanced blockchain feature payments including FundLock, Bidding, HashCode Messaging and Escrow when coin creation becomes limited.

---

[8] Inter-blockchain cold storage is
[9] Prime Controller™ stake rate is 5% of all locked bid funds as a six month yield with the stake paid daily.
[10] Proportional share is a weighted value based on network participation and total coin stake.

6.2.3 Prime Controller™ Eligibility Requirements

Prime Controllers™ are the backbone and core of the Paycoin™ network. To keep the network as an open peer-to-peer network while maintaining the integrity of the backbone, Prime Controllers™ require a strong commitment to the coins success. The amount of network stake, required to promote an Orion Controller™ to a Prime Controller™, will provide a disincentive to any illicit party, acting alone or in conjunction with others, to affect a negative impact on the Paycoin™ network. This unique stake requirement adjusts dynamically as the network scales up or down, creating a globally scalable, near-real-time commerce network.

In addition to the exclusivity and strong a large stake in the coin, Prime Controllers™ are required to meet certain minimum standards. Orion Controllers™ must meet the following overall requirements to bid on a promotion to Prime Controller™:

- Passing a Transaction Per Second test which consists of
  - Random Connected Node latency,
  - Disk throughput requirements,
  - Minimum number of processed transactions processed,
  - Minimum # of Connected Nodes,
  - Maximum time since last broadcast received.
- Hold a funded wallet on the Orion Controller™ meeting the current minimum bid amount for a Prime Controller™[11].

[11] The minimum initial bid to promote an Orion Controller™ is equal to one half of total number of coins in existence divided by the total number of Prime Controllers™ required by the network.

6.2.4 Prime Controller Availability

The network continuously analyzes transactions per second, and aggregate node performance to dynamically adjust the required and available number of Prime Controllers™. There are two instances whereby Orion Controllers™ may bid to be promoted to a Prime Controller™:

- During the Prime expiration window, which initially occurs every 6 months, all Prime Controllers™ positions will be available for bid;
- At any time the Paycoin™ network ejects a bad actor, individual Prime Controller™ slots will be available for bid:
  - When needed a vote can be initiated by any Prime Controller™ on the network to reject a Prime Controller™ from the network for illicit acts or under performance.
  - The network can automatically reject and demote underperforming Prime Controllers™ (See the section titled "Prime Controller™ Scaling for details).

6.2.5 Prime Controller™ Consensus

Prime Controllers™ must be able to reach an expedient majority consensus regarding transactions that are submitted to the network. The communications protocol between Prime Controller™ nodes will include a linearly growing signed package until a majority of votes is reached. At the instant of majority consensus, the transaction will then be written to the blockchain, and signed using a hash of the consensus vote signatures.

6.2.6 Prime Controller™ Bidding Process

When Prime Controller™ positions become available, the bidding opens automatically by broadcasting the number of open slots, a bid address and an expiration date. Bidding is performed by making a bid payment to the blockchain from a wallet stored on an Orion Controller™. This "bid packet" will contain the "Controller's Transactions Per Second (Eligibility) Report," and will be sent as a payment of 50 Paycoins™ from an address containing the users bid amount. The amount must match the minimum required bid11 after deducting the bid payment. At

6.2.6 Prime Controller Bidding *(cont)*

any time during the open bid period, the bidder may increase the locked wallet balance in order to increase their bid.

At the end of the bidding period the number of Prime slots available are awarded each based on the highest bids. When multiple Prime Controller™ positions are available bids are calculated using the following method:

- Each bidder sends a bid fee[12] equal to the current bid fee , initially 50 Paycoin™, to the bid address mul tiplied by the number of prime con trollers™ requested;
- Perform 2 rounds of bid assignment to determine the winners,
  - Round 1: Assign by total bid and drop any non-winning bids,
  - Round 2: Starting from the highest total bid, recursively split controller bids into [totalBid/(requestedPositions-n)] amounts until each multi-bid is greater the lowest winning bid.

All remaining bid addresses are unlocked. All bid fees paid are distributed amongst existing Orion Controllers™.

6.2.6.1 Leveraging Inter-Blockchain FundSafe

The auction process leverages HashCoin™s built into a FundSafe mechanism authorized by the Prime Controllers™. Funds are locked in a non-spendable state for the duration of ownership of the Prime Controller™, thereby protecting the integrity of the controller, even if private keys are compromised.

[12] The bid fee is 2,500 Paycoin™ divided by the total number of prime controllers required by the network.

6.2.6.2 Incumbents and tie breaking

As with any vote or auction, there are chances for a voting deadlocks to occur, when Orion Controllers™ bid for a slot to become a Prime Controller™. In order to resolve these ties automatically, the following tie-breaker rules will apply:

- Where an existing Prime Controller™ and an Orion Controller™, the incumbent Prime Controller™ will win;
- In the event of any tie, where the bid amounts are equal, the bid confirmed earliest on the network will win, and;
- In the event of a voting deadlock, neither bidder will win, and the Prime Controller™ slot will be removed.

6.2.7 Prime Controller Scaling

In the event of a network failure or slowdown, the Paycoin™ network will increase the required number of Prime Controller™ slots for the next round. During each round of scaling, certain Prime Controllers™ may be automatically removed from active status and blocked from becoming a Controller again. Features of the mid-term and end term scaling include:

- Automated Prime Controller™ ejection for downtime and lag;
- Transaction per second measurements and network requirements, and;
- Network average transactions per second and low-performer rejection.

7 Conclusion

Cryptocurrency is a young, disruptive technology that offers easier, faster, and more secure transacting between individuals and merchants than any payment technology to date. However, all existing cryptocurrencies have failed to achieve an adoption path leading to mainstream use. Even the most popular cryptocurrencies are accepted by fewer than 1% of all global merchants.

Conventional online payment solutions such as credit cards don't just put consumers at risk of identity theft and merchants at risk of fraud - they are costly even when used under ideal conditions. These payment systems cost consumers and merchants between 2% and 10% per transaction. Cryptocurrency offers merchants an alternative to these methods which eliminates these fees, potentially saving merchants across the globe tens of billions of dollars, annually.

Withso much potential upside, many find it difficult to understand why merchants have been slow to accept legacy crypto-currency payments.

The answer largely is price instability, which threatens business' profitability. Daily price fluctuations of existing cryptocurrencies exceed the transaction fees for conventional payment systems, inhibiting cryptocurrency's benefits over these systems.

Paycoin™ improves upon existing coins by producing an decentralized network structured to promote price stability, fast transaction times, and rich features for merchants and consumers. Prime Controller™ Hybrid-Flex Blockchain, and Transaction Immutability incorporate the latest in cryptography and economic theory to produce a digital currency aims to bring cryptocurrency use to a global audience.