Pastel Litepaper

Jeffrey Emanuel, Anthony Georgiades, airk42

January 7th, 2021

Contents

1 Introduction **2**

2 Market Opportunity & Economic Rationale **2**
2.1 The Art Market . . . 2
2.2 High-End Contemporary Art . . . 2
2.3 Eliminating Intermediaries . . . 3
2.4 Blockchain Can Democratize the Market . . . 3
2.5 Crypto-Currency as a Solution . . . 4

3 Current Alternatives and Competition **6**

4 Core Architecture **7**
4.1 Z-Cash and Cryptographic Primacy . . . 7
4.2 Dash and the Masternode Concept . . . 8
4.3 Novel Python Code Base . . . 9

5 Key Features **9**
5.1 Off-Chain Storage . . . 9
5.2 NSFW and Inappropriate Content . . . 10
5.3 Duplicate Detection . . . 10
5.4 Other Critical Features . . . 11

6 The Crypto-Economics of the Token **11**
6.1 Economic Role of Masternode Operators . . . 12

7 Tokenomics and Emission Schedule **13**
7.1 Initial Fork and Distribution Mechanism . . . 13
7.2 Coin Distribution and Post Fork Tokenomics . . . 14

8 Feature Pipeline and Future Roadmap **15**

1 Introduction

We introduce **Pastel**, an open-source, decentralized system which allows artists to register "provably rare" digital artworks on a Bitcoin-like blockchain, while also allowing art collectors to purchase these artworks and "trustlessly" trade them among themselves without reliance on a central authority. The resulting rare digital artworks can be thought of as continuing the long tradition of limited edition art prints such as those sold by art galleries, often in sets of 10 individually numbered pieces.

Unlike such "physical world" prints, rare digital artwork–when implemented correctly using a secure cryptographic digital signature scheme and a robust "near-duplicate" image detection scheme–offer the digital art collector a high degree of certainty in determining the authenticity and provenance of a specific artwork registered in the system. At the same time, rare digital artwork allows artists to directly access and trade with their patrons, without an art gallery or dealer taking a huge slice of the value. Furthermore, rare digital art collectors can trade among themselves using an integrated, decentralized art marketplace at a minimal cost in terms of fees, providing low-friction liquidity to a notoriously illiquid and fee-ridden traditional art market.

2 Market Opportunity & Economic Rationale

In this section, we discuss the opportunity for the Pastel project in the context of the global art market. Current processes are filled with inefficiencies, and it has become abundantly clear that decentralization improve markets. In particular, the advent of digital technology–especially the ability to make an exact "bit-for-bit" copy of a digital file–has changed the underlying assumptions that have historically guided art market participants. The inability of traditional art markets to adequately respond to these technological challenges has paved the way for innovation through a self-contained, decentralized platform.

2.1 The Art Market

The global art market exceeds $50 billion dollars per year. While much of that value is dominated by a few high-priced sales at auction of famous historical works that can exceed hundreds of millions of dollars, the size of the contemporary art market, as measured by using global auction revenue, is close to $2 billion annually (Source: artprice.com). In addition, the contemporary art market employs many thousands of individuals around the world, from the artists themselves to their assistants, art dealers, gallerists, art advisors (who advise collectors), museum curators, publicists, etc.

2.2 High-End Contemporary Art

The "high end" of the contemporary art market is increasingly dominated by a small centralized group of "star" artists, such Damien Hirst, Jeff Koons, and Matthew Barney, who often employ whole teams of assistants to jointly produce their artworks. These studios work closely with the most reputable galleries and collectors, and cultivate social relationships with

important art critics and taste-makers. Without such connections, it is extremely difficult for young artists trying to establish themselves to get enough career traction so that they are able to financially support themselves through their art. Indeed, many young artists face a steep, uphill battle to even have a chance at establishing such connections. And for those who do manage to catch the attention of a gallery or dealer who is established enough to financially support the artist, the price is very high: dealers generally take the majority of the economics, and the additional layers of fees from galleries and art-advisors usually means that the artist is left with a small fraction of the total amount spent by the end buyer.

2.3 Eliminating Intermediaries

It's not just the art galleries that take a piece of the economics in art market transactions: there is a whole industry of art appraisers, who certify the authenticity and attempt to estimate the value of specific artworks using various methodologies, similar to how a real estate appraiser might value a building. The art industry continues to extract a huge portion of the total value chain in the art market, even for digital artwork.

A buyer who purchases a piece of artwork from a gallery is usually helpless to efficiently sell the artwork without the cooperation of a gallery (often the very same gallery that sold it in the first place), which again comes at a very steep cost in transactions fees and the co-called "bid ask spread," or the difference between buying and selling prices that exist even when artwork is sold from one dealer to another dealer. These frictional costs reduce the incentive to transact in the art market, and the resulting loss of liquidity hurts both artists and collectors.

The art market, in addition to the rare collectibles market (e.g., comic books, baseball cards, etc.), is rife with inefficiencies for both consumers and producers. The people who are actually making the art are getting a fraction of the final value created, and the people who are actually buying the art are also forced to give up an enormous share of the potential profit through the various layers of fees and the lack of liquidity. The reason why collectors put up with this untenable situation is because the art market has *always* worked in this way, and until now, there have been no good alternatives that retain the "reputation backed security" offered by the traditional gallery or retail model.

2.4 Blockchain Can Democratize the Market

While the inefficiencies that exist in the market for physical artwork are not going to change anytime soon, there is no reason why the new world of digital artwork has to be shackled to this inefficient and inequitable system. But before that can happen, the world needs a decentralized, *trustless* mechanism to fulfill these same core functions of the art market that are currently provided by galleries and experts. Why must it be decentralized? In short, no one is going to trust a centralized network with something as important as high-end (or even low-end) artwork or valuable rare collectibles. What artist in their right mind would want their art to be held hostage in some "closed-garden" environment controlled by a corporation or government?

In a fully decentralized peer-to-peer system such as Pastel, where all of the software is open-source and anyone can freely purchase the coins required to "host" the network (i.e.,

to run a Masternode) so that it can serve users, the community is never faced with this problem. If the original Pastel developers were to abandon the project for some reason, anyone (say, an artist or art collector) could carry on the operation of the system. The essence of a decentralized system is that no one is in control, which gives individual network participants a degree of freedom and power that is simply unavailable in a centralized system; centralization means that users must act passively, with no control over their own destiny.

This is what gives us at least some chance to fulfill the implied guaranty of our proposed system: that it will securely store users' artworks "forever". After all, any owner of a large number of artworks registered on the network would have a personal motive to continue running the Masternode software, even if doing so would otherwise be financially undesirable. And a new group of leaders from the outside could become "activist" and publicly announce that they are going to "take over" the system; if these outsiders can make a compelling enough case that a majority of Masternode operators are convinced to give them a chance, no one can stop them– even the original Pastel development team.

2.5 Crypto-Currency as a Solution

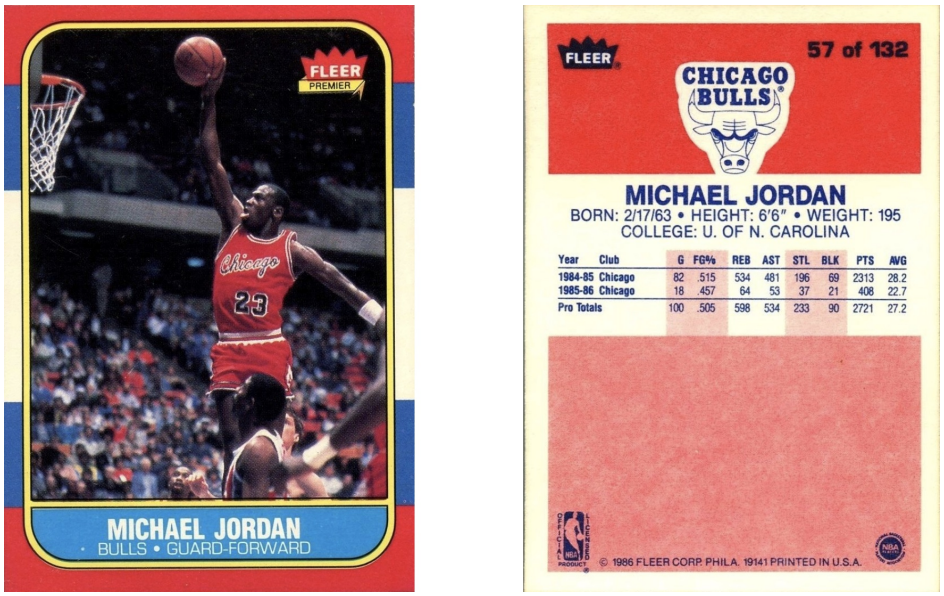
What if there were some way to give the fans of an artist a way to support the artist financially, while still deriving some tangible value themselves from the transaction? That is, if instead of simply giving a donation, the fan could receive something in return for their support?

We believe that rare digital artwork, implemented correctly on a decentralized blockchain, offers an optimal solution. By giving the collector the ability to transfer value directly to the artist with minimal fees–that is, by the allowing the collector to purchase one of the rare "copies" of the artwork offered for sale by the artist, using an integrated, decentralized asset exchange– that we can offer a far better way to create a mutually beneficial exchange between artist and collector. Savvy collectors, who have a good eye for talent and their "finger on the pulse" of popular tastes, could find an artist just starting out with few fans, and inexpensively purchase one of say, 10 limited editions of one of the artist's digital artworks. If that artist were to later become a huge celebrity, with thousands of fans (after all, some of the biggest celebrities today got their start from humble origins on social media), then it's easy to see how such early artworks could appreciate in price dramatically– say, from $4 to $100.

The scenario outlined here is exactly analogous to a knowledgeable basketball fan deciding in 1986 to purchase a box of baseball cards in order to acquire 10 copies of Michael Jordan's rookie card, shown in the figure above. Such cards now fetch as much as $2,000 in the market. Although there is generally no reward for being an early fan of an artist who goes on to later mainstream success (other than the satisfaction of seeing one's tastes vindicated), in our proposed system, a fan can actually benefit financially, thus creating a symbiotic relationship between the fan and the artist:

- The fan either gives coins to the artist in return for the artwork (which the artist can sell for Bitcoin on an exchange) or purchases the artwork in a secondary market transaction from another user. Thus each purchase financially benefits the artist, either by directly transferring value to the artist or indirectly by increasing the market demand and price for the artist's works on the network.

Figure 1: Michael Jordan Rookie Card (Source: *the Fleer Corporation*)



- The fan now owns a liquid asset, denominated in a crypto-currency which can be converted into Bitcoin (and thus ultimately into any fiat currency), the value of which depends of the success of the artist. Thus the fan or collector now has a vested interest in promoting the works of the artist, since the artist's future success directly benefits the collector in the form of a higher market price for the artist's works.

The key advantages of rare digital art, and why it is such a potentially transformative force in the way art is collected and created, include the following:

1. Since the art exists in digital form (i.e., as information), **the costs to create it and distribute it are much lower than with physical artwork**.

2. The use of secure cryptographic methods allows rare digital art to **solve the problem of establishing the authorship and provenance of a given artwork**, which has plagued the art market for centuries.

3. By integrating the payment and trading aspects of art collecting into the very same blockchain that acts as the registry for that artwork, we greatly **reduce the need for extensive intermediation in the form of galleries, dealers, and payment processors.**

4. By giving a new way for "casual fans"– that is, non-wealthy consumers who enjoy the works of an artist– **to financially interact with their favorite artists through efficient micro-payments, rare digital art enables new ways for artists to support themselves** instead of using services such as *Patreon* or *GoFundMe*, or by taking on contract work for hire that they do not own.

3 Current Alternatives and Competition

The use of blockchain or distributed ledger as a registry for artwork is not a novel concept. However, no existing project has solved the particular challenges that arise in developing an art registry system that can work reliably and securely in a truly decentralized way. Existing projects such as PepeCash/Rare Pepe, which briefly reached a valuation of $90 million in early 2017, established that there is market interest in rare digital artwork. Yet PepeCash is far from decentralized; although the details of the artworks and their ownership are stored on the Bitcoin blockchain (by means of the *CounterParty* protocol), the registration process to create a new artwork relies on contacting the creator of the project, Mike, who unilaterally decides whether to allow the registration using criteria such as the perceived uniqueness or originality of the submission (e.g., you can't register a "Simpsons" Pepe because someone already did that).

Furthermore, the advent of non-fungible tokens (NFTs) has increased both awareness and demand for rare digital assets. NFTs indeed offer certain advantages for both creators and speculators alike - interoperability across ecosystems increases tradeability and liquidity, while token standards like ERC721 promise provable scarcity. However, NFT platforms face certain challenges. For one, with interoperability comes reliability - NFT platforms and token standards are largely beholden to their underlying infrastructure, such as Ethereum or Tron. In the case of Ethereum as an examplee, increased network traffic, which might be a product of heightened NFT demand or driven by the use of other services on the network, can drive transaction fees to a point in which it becomes economically in-viable to purchase a single piece of art. Additionally, none of these frameworks offers a self-contained system which can provide the network sophistication to detect against near duplicates or protect the system from NSFW.

In short, other existing "art on the blockchain" projects put far too low of an emphasis on decentralization and security. They attempt to solve problems through heavy-handed, blunt approaches that make them unattractive for serious artists and collectors, and generally introduce huge amounts of centralization through human-managed moderation that is subject to subversion.

Even if these competing projects didn't suffer from such "show-stopping" flaws, they are inherently less ambitious and powerful than what we are attempting to do in the Pastel project: we are leveraging the latest advances in machine learning, as well as novel contributions from the Pastel project, to remove the human element from the equation to the greatest degree possible.

We are building a system in which machines can coldly and objectively evaluate which images should be prevented from being registered–say, because they contain child pornography, or are "rip offs" of existing registered artworks. We are building a system where anyone can, without permission or authorization, create original digital artworks using the tools of their choice, and submit these for registration without any individual person or entity being in a position to impede them. And we are building a system where the actual art files are stored in a robust, decentralized way, and where registered artworks can be freely traded in a completely trustless way. Perhaps most importantly, we are building a system in which anyone can help *run* the network themselves by purchasing a sufficient number of coins so that they can setup a machine as a so-called Masternode, described more fully below.

4 Core Architecture

From the beginning, the primary design inspiration for Pastel has been Bitcoin, which strikes an ideal balance between security and functionality. While Turing complete blockchain projects such as *Ethereum* obviously have more built-in functionality, this expressive power come at a great cost in terms of security and reliability. The fact that one of the core developers of Ethereum managed to lose hundreds of millions of dollars worth of coins because of a software bug in a multi-signature wallet shows that such a system is too complicated to reason about effectively even for the most advanced users.

Just as Bitcoin focuses exclusively on the narrow problem of how to make ideal "e-gold," and optimizes for this single use case in the simplest way possible, our goal with Pastel is to build only the functionality required to efficiently and securely provide the services we need for the specific use case of rare digital artwork on the blockchain, rather than being all things to all people and use cases. At the same time, many of the techniques and approaches we use for rare artwork would apply equally well to other types of files, which we discuss further in a later section.

As such, we wanted our base layer– the foundation on which our project is built–to be Bitcoin. By using a familiar, well-tested foundation, we can ensure that the most basic functions of a crypto-currency network–the secure transfer of coins among users in an immutable ledger–is beyond reproach. However, rather that use Bitcoin Core as the starting point for the Pastel code base, we have instead selected to build on top of *Z-Cash*.

4.1 Z-Cash and Cryptographic Primacy

The Z-Cash project is a direct fork of the Bitcoin code-base (albeit an outdated fork) which makes only very modest changes to the key parameters of Bitcoin:

1. **Proof-of-work algorithm:** Z-Cash uses *EquiHash*, rather than the *SHA-256* hash algorithm used in Bitcoin.

2. **Average Block Time:** Z-Cash has a 2.5 minute block time, versus 10 minutes for Bitcoin.

3. **Emission Schedule:** Z-Cash makes minor changes to the initial rate of distribution of coins early in the network's evolution, but essentially sticks to the same 21 million coins and distribution schedule as in Bitcoin.

4. **Difficulty Retargeting Algorithm:** Z-Cash uses a different mechanism for adjusting the difficulty of the proof-of-work in response to observed changes in the network's hash rate designed to be more stable.

But the primary change made by Z-Cash is the introduction of *Z-SNARKS*, a powerful cryptographic scheme for facilitating on-chain transactions (known as *shielded transactions* that are nevertheless invisible to other network participants, who cannot determine the identities or amounts involved in such transactions. Although the cryptography involved in Z-SNARKS is relatively new, the method has been extensively peer reviewed, and is based on proven cryptographic concepts.

While a discussion of how Z-SNARKS work is beyond the scope of this document, we will briefly remark that we are employing the same "Trusted Setup", or initial set of security parameters, as the Z-Cash project uses. The key generation ceremony used for Z-Cash has been extensively documented elsewhere (See X, Y), and a detailed review of the steps taken should convince even a skeptical observer that the methodology employed was sufficiently rigorous to ensure the overall security of the scheme.

4.2 Dash and the Masternode Concept

Of course, one obvious limitation of Z-Cash is that it has no support for the Masternode concept, which is a cornerstone of the Pastel architecture. Thus, the next key layer of Pastel's architecture is the core Masternode code from the *Dash* project, which pioneered the idea in its 2014 introduction. This code, which, like the Bitcoin and Z-Cash code, is primarily written in the *C++* language, was (after being slightly simplified and modified) carefully transplanted into the Z-Cash code base, thus producing a novel combination: a Masternode based crypto-currency with full support for Z-SNARKS. Although there are dozens of Masternode crypto-currency projects based on the Dash code base, most of these are close derivatives or "clones", and none offer the kind of "step change" increase in functionality at the level of shielded transactions.

However, DASH contained many elements that were complex and unnecessary for the functionality of the Pastel project. For example, Dash services such as *InstantSend* and the questionable *PrivateSend* were completely removed, leaving the core skeleton of the Masternode architecture: the selection of the "winning" Masternodes that will receive the next share of the block reward, and the essential code for checking that Masternodes control the required number of coins and that they respond to pings at their announced IP addresses. Despite some valid criticisms about its initial distribution, the Dash network has a proven track record of security, and the code has demonstrated that it does the essential functions required.

One element that has been added to this core C++ layer is a new Masternode voting system. In this system, any Masternode can submit a ticket requesting payment from the network in return for some service, or to be reimbursed for valid expenses incurred in the creation of new functionality. This ticket includes a text field which could contain, for example, a link to a PDF file describing the purpose of the request; for instance, the PDF might detail the listing cost with an exchange, and the submitter of the ticket would try to convince a majority of the other Masternodes to vote in favor of the proposal. In addition, the ticket will include the Pastel blockchain address at which the submitter wants to receive the funds if the ticket is approved.

A total of 5% of the Pastel mining block reward will go towards payments to such addresses (i.e., to the Pastel *Growth Fund*, assuming that they win enough votes using the voting system. In order for a ticket to be approved, it must be voted on by a sufficiently higher number of MNs so that a *quorum* is available– a minimum number below which a vote is invalid. If the quorum is met, then elections are based on a majority vote. Submitted requests arrive in a queue, and are entered into circulation among MNs as part of a list of potential recipients of funds, so that each MN can vote on whether they approve or disapprove of the submitted request. Assuming a ticket is approved, the payments will will

be sent in the form of *coinbase* transactions, similar to how mining rewards and Masternode rewards are paid out by the network. If the requested amount exceeds the amount of the next 5% payment, then the ticket continues to remain outstanding until it is fully paid the originally specified number of coins.

4.3 Novel Python Code Base

The higher-order functions of the Pastel network–namely, those which operate by means of ticket files written to the blockchain (e.g., artwork registration tickets, artwork trading tickets, identity establishing tickets, etc.)– essentially "piggy back" on the core blockchain functionality of Bitcoin/Z-Cash by using these transactions as "dumb storage."

Just because a ticket file has been written to the blockchain by means of these special coin transactions, it is not necessarily deemed to be valid by Masternodes: first, the ticket file must be carefully and independently reconstructed, parsed, and validated by each Masternode. Once validated, the Masternodes must act on the basis of these tickets, performing a variety of specific services in coordination with other randomly selected MNs.

All of the computer code to facilitate these operations are implemented in the custom *Python* system developed for the Pastel project. The code is written in a modular way, with various utility and other classes to reduce code redundancy. It is also fully open-source, with the updated contents available to anyone around the world through *GitHub*.

5 Key Features

Instead of attempting to serve as a universal platform for building decentralized applications, the Pastel project focuses narrowly on rare digital assets (art, videos, music, etc.), with the single goal of optimizing the various engineering and security trade-offs for this one application. We believe in building the project upon a sturdy foundation of proven, peer-reviewed technologies wherever possible, although in some cases, we had to invent new technology that did not exist previously. With the exception of these innovative features, the primary contribution of Pastel is in how it combines these existing technologies in innovative ways, while carefully designing the economic incentives of the network so that the optimal behavior of network participants is to act honestly and in a way that is productive for the performance and security of the network.

5.1 Off-Chain Storage

A system like the one described above, while secure, is not complete as an integrated digital art registry. That's because it leaves out the storage of the artwork itself, which is obviously a critical aspect of visual art. What is needed is an additional *off-chain storage system*, in which the original, high-resolution image files can be safely stored in a fault-tolerant, redundant, and decentralized way, so that they are always available to authorized owners– even in 10 years from now, and all without a centralized party or service underpinning the system. Pastel addresses this challenge through the use of a novel distributed file-storage layer via the use of rare chunks and LT encoding as described in our Whitepaper.

5.2 NSFW and Inappropriate Content

Of course, storing the artwork image files "off-chain" is just a starting point; there are several other features that we believe are critical to a successful decentralized art registry. The first of these is a way to reliably prevent offensive or illegal content from being registered on the network in an "active" way, rather than responding passively through moderation when such content is identified by network participants. While this may seem like a questionable or "prude" feature, it is in reality quite serious: other decentralized networks, such as FreeNet, are notoriously plagued by child pornography and other illicit content. Not only are such uses of the network morally repugnant, they also introduce real legal risk to the owner of the computer on which the content is stored.

While determining if a candidate image is pornographic or otherwise "NSFW" is very challenging, recent advances in machine learning have led to open-source models that have been trained on millions of sample images. Pastel uses a pre-trained *TensorFlow* model from Yahoo's *OpenNSFW* project to evaluate every submitted art image file; the model assigns a score between 0 (definitely not NSFW) and 1 (definitely NSFW). By insisting on a relatively low score, we can ensure that the majority of inappropriate content will never be permitted on the network. While this is in effect a form of censorship, and will likely lead to the rejection of artworks that would otherwise be considered by a human observer to constitute "acceptable art" (such as a tastefully done nude scene), we believe that this sacrifice is well worth it to establish a baseline level of confidence in the nature (and legality) of the stored image content.

5.3 Duplicate Detection

Perhaps the most technically challenging feature required in any decentralized art registry is some form of *near-duplicate image detection*. The idea here is that we only want original works to be registered on the network. That is, if a particular image is registered on the network, then we don't want to allow another user (or even the same artist) to register a "near-duplicate" image. If we were only concerned about an exact bit-for-bit duplicate of the original image file, we could simply use a file hash, and insist that this be unique. But a file hash is brittle: if you take an existing registered image and change only the upper left pixel, for example, the entire hash will change. What we want is the exact opposite: a *robust* image fingerprint– one that is stable in the face of superficial changes. That is, we want a way of identifying or characterizing an image that is robust to various transformations to the original image, which might include:

- Cropping, scaling, or rotating the image.
- Adjusting the color, contrast, brightness, or "curves" of the image.
- Adding random noise or dots to the image.
- Applying any sort of image filter, such as those included in Adobe's Photoshop software package; for example: blur/sharpen, edge-detection, inverted images, non-linear image warping filters such as Spherize or Twist, etc.

Put differently, we want a duplicate detection system that can react similarly to the way a human observer could in determining if two images are "related"; that is, if an average person could reliably determine that a given image is "excessively derivative" of an existing registered image, then we want our automated system to reach the same conclusion. The ideal system would reject a high percentage of true duplicate works while allowing through the vast bulk of truly original works. The greatest challenge are those artworks on the boundary line– similar to an existing artwork, but different enough that they are not clearly "duplicates" according to our chosen criteria. For this problem, Pastel has developed a novel and innovative duplicate detection framework, which leverages advances in machine learning technology as well as the creative application of classical statistical techniques, which we explain in more detail in a later section.

5.4 Other Critical Features

We describe the core architecture and key features of Pastel in more detail in our WhitePaper, certain of which include:

1. Pastel Digital Signature System
2. Pastel ID and the Reputation Tracking System
3. Artwork Registration Worfklow
4. Masternode Messaging System
5. The Blockchain Ticketing System
6. Off-Chain Storage System
7. Artwork Collecting and Trading Workflow
8. Piracy and Unauthorized Usage
9. End User Experience for Collectors
10. Serving Metadata and Thumbnail to Userse

6 The Crypto-Economics of the Token

The single most important benefit of a Masternode system is that it provides an answer to the question: *"Why would anyone want to hold this coin over the long term?"* The response to this question is ultimately what determines the market value of a crypto-currency network.

The problem with the majority of existing crypto token assets is that they utterly fail to answer this key question, and instead fall into what we can call the "Chuck-E-Cheese dilemma." This term is based on a comparison to *Chuck-E-Cheese*, a chain of arcade and pizza stores popular in North America that forced customers to pay for arcade games using the company's own proprietary tokens instead of regular (USD) coins, as illustrated in the

following figure. If one considers the incentives of a parent hosting a child's birthday party, the parent wants to purchase only the minimum number of coins required to get through the party, and then wants to get rid of the remaining coins at the end.

Figure 2: Chuck-E-Cheese Tokens (Source: *forums.collectors.com*)

That is to say, no one would rationally choose to hold on to these tokens over the long term, since there is absolutely no benefit to doing so– only downside, in the form of reduced liquidity, since the tokens are useless anywhere besides that particular store, and if the company were to go bankrupt, the tokens would be as worthless as a *Circuit City* gift card (to name another defunct retail company). Any token that follows this basic structure– and unfortunately, this category describes the vast majority of "ERC-20" tokens that have been launched on the *Ethereum* platform– will have its fundamental value limited by the average value of transactions on the network at a given time.

In the case of the arcade company analogy, this value might be approximated by some discount to the equivalent dollar value, over a given time period, of all the games played in its stores if they instead required regular coins rather than proprietary tokens to play. That is, **the value of the coins are limited by the marginal utility value of the network**. This creates a "prisoner's dilemma" problem, in which users are motivated to hold the token for the shortest time possible, since others will come to the same conclusion and race to sell first, similar to how consumers tend to behave in hyper-inflationary economies such as Venezuela or Zimbabwe.

6.1 Economic Role of Masternode Operators

Masternode operators, who invest an up-front amount of capital (i.e., the coins required to collateralize and operate a Masternode) in return for the opportunity to become part of the network, just as a new franchise operator gets to be part of a network of stores. And just as the new franchisee has a series of obligations to the franchisor– for example, they must serve only the products specifically permitted in each region by the corporate parent, and they must maintain certain minimum standards– the new Masternode operator must perform a series of obligations when called upon by the rank ordering process, which include:

- The parsing and validation of submitted blockchain tickets.
- The application of NSFW and duplicate content detection.
- The preparation of the image files for insertion in the off-chain storage system.
- The facilitation of decentralized trading of registered artworks, with the MNs acting as brokers on behalf of users.

Put differently, the Pastel project provides the prospective Masternode owner the opportunity to participate in the rewards and work involved in actually running the network. It gives them the authorization, or "license," to be allowed to be part of the system, and it also provides the tools required for a non-technical user to fulfill all of the actions expected by other users from a properly functioning Masternode. The Pastel software gives the Masternode the software tools required to, for example, automatically determine if a newly submitted candidate artwork is a near duplicate of an existing artwork– a challenging problem that until recently had no good open-source solutions– all without the manual intervention of the Masternode owner, who can essentially "earn money while they sleep" as their computer slavishly follows the procedures encapsulated in the Pastel computer code.

7 Tokenomics and Emission Schedule

7.1 Initial Fork and Distribution Mechanism

We humbly submit that the *Animecoin* project serves as the parent coin for the Pastel fork, as it possesses desired attributes identified for a fork. Animecoin, also known by the symbol ANI, was originally announced on the well-known *bitcointalk.org* web forum on January 19th, 2014– fairly early compared to the vast majority of the roughly 2,000 crypto-currencies in the market today. Animecoin was intended as currency "for the anime community"; although this questionable goal was never reached (why would they need their own coin instead of Bitcoin? What functionality did it provide?), the coin was nonetheless enthusiastically adopted by hundreds or even thousands of users, many of whom were computer game fans who simultaneously had an interest in crypto-currency and anime as well as a powerful GPU for use in 3D games. As a result, the coin was widely distributed over an extended time period.

While a detailed description of the technical aspects of ANI are beyond the scope of this document, the Animecoin software is essentially a Bitcoin clone (as of late 2013) with a 30-second block time instead of Bitcoin's 10-minute block time, and using the "modified Quark" hashing algorithm instead of *SHA-256* as in Bitcoin.

In order to deal with this problem, we conducted a modified fork procedure in which distribution of the forked coins is not automatic: rather, holders of the parent coin (i.e. ANI) who were interested in participating in the fork were required to signal their desire to participate. In this way, the project obtained a confirmation of the true number of "marketable" existing coins in the fork.

Any coins that have been lost through dead hard drives and other causes thus did not receive an allotment of the new Pastel coin. Furthermore, coins belonging to wallets in which

we were unable to conduct adequate Know Your Customer (KYC) review or that were held by the now defunct Cryptopia exchange were unable to participate. More importantly, old users of ANI, some of whom might have large balances, but who have not kept on top of developments with the project, were also left out. Although this is arguably unfair to such unwitting users, who would normally participate in a fork even if they didn't know the fork was happening, not taking any such precautions creates an uncomfortable amount of risk to early adopters. Suppose such a "legacy whale" were to appear, who only recently found out that the old "worthless" coins are now worth thousands of dollars. If such a user is being economically rational, they should not cause the price to plunge by indiscriminately selling as quickly as possible, since this ultimately reduces the value of their own coins. However, such irrational behavior is commonplace in practice, and seems sufficiently grave so as reasonably lead to the compromise outlined above (i.e., the requirement for a contemporaneous ANI transaction to signal intent to participate in the fork).

7.2 Coin Distribution and Post Fork Tokenomics

- **Initial Circulating Supply:** Approx. 10.5 Billion PSL
- **Total Supply:** 21.0 Billion PSL
- **Initial Block Reward:** 6,250 PSL / Block
- **Reward Distribution:** 5,000 PSL for Miner and 1,250 PSL for Masternodes
- **Emission Decay:** Reduced by 50% very 840,000 blocks

Initial Supply: As of the fork date (January 1, 2021), the initial coin supply will be deemed to be half-way distributed, so that roughly 10.5 billion coins will be outstanding on day one; these coins will be proportionately owned by all the ANI holders who signaled interest in participating in the fork event. Since we know the precise number of qualifying coins that will participate in the fork, we can compute the appropriate ratio to apply in crediting each balance with the new Pastel coins which in this case is 95.0 to 1.0.

Emission Schedule: From then on, the coin emission schedule is set to match that of Z-Cash, which is closely modeled on the Bitcoin emission schedule. For comparison, Bitcoin block reward began at 50 BTC per block, with a new block every 10 minutes. Because the Pastel max supply is 1,000x the size of the BTC max supply, we must multiply this by 1,000. We chose an initial block reward of (50*1,000)/8, or 6,250 Pastel per block to emulate the emission schedule in Bitcoin. This block reward is thus reduced by 50% every 840,000 blocks or 4 years.

Total Supply: To facilitate art transactions that do not result in a comically small number of coins, we have elected to model the Pastel coin distribution on Bitcoin, but instead of using 21 million as the total, we instead use 21 billion, at some slight loss in expressive power in that each resulting coin will not have as many decimal places of precision as in Bitcoin. This way, a user can talk about purchasing an artwork for hundreds or thousands of coins, instead of 0.002 coins or similarly inconvenient numbers.

8 Feature Pipeline and Future Roadmap

Feature Pipeline:

- Loaded PoW
- SPHINCs Quantum Resistant Signatures
- The Use of Steganography to Encode SPHINCs signatures as QR Codes in Images

Roadmap:

- **Q1 2021:** Exchange Listing
- **Q2 2021:** Launch Web-Based Application
- **Q4 2021:** Support for various files (videos, audio, gifs)