The Value of App Coins

An open source analysis of App Coins, as a technical and economic means of price discovery, forms of expression, community building, and a model for rewarding actors that perform quantifiable valued added behaviors. Pull requests to improve the content, references, and claims of this whitepaper are welcome.

Authors:

David A. Johnston - https://github.com/DavidJohnstonCEO

Joel Dietz - https://github.com/fractastical

Ron Gross - https://github.com/ripper234

With input from:

Peter Todd - https://github.com/petertodd

David Irvine - https://github.com/dirvine

Jeremy Kandah - https://github.com/jkandah

Sam Yilmaz - https://github.com/Onat

J.R. Willet - https://github.com/dacoinminster

Tom Ding - https://github.com/toysrtommy

Introduction:

This white paper seeks to put forth the economic and technical reasons that the digital tokens known as **can develop a value in the market and maintain their value over the long term, should their associated application gain adoption by users. App Coins can be implemented for solid technical or economic reasons. However projects should think carefully about their particular application and evaluate if there are compelling technical or economic justifications for the creation of an App Coin or if a for-profit business model may be better suited than a crowdsale model involving a pre-sale of the tokens that gives access to the services.**

Definition for App Coins:
App Coins are defined here as tokens that are native to Decentralized applications that have a digital token associated with their use or monetization. For a more general description of what a Decentralized Application is (outside of the economic and technical discussions below about the value of their digital tokens) see this white paper (https://github.com/DavidJohnstonCEO/DecentralizedApplications) and wiki entry.

Table of Contents:
==========

Section One: When Does an App Coin Model Make Sense

1. Centralization or the Requirement of Trust is Unacceptable

2. It Implements Functionality That Bitcoin CanNetwork StrengthNetwork StrengthNETWORK EFFECTS AND COMPETITION: An Empirical Analysis of the Home Video Game Industrystrong evidence that network effects are asymmetric between the competitors Where the term is defined as (the marginal impact of a unit increase in network size on demand).

An example of this is the Apple OSX operating system which for a long time had a much smaller network size effect, however, due to a higher network strength was able to overcome this and attain a much higher market share of operating systems in recent years. As shown in this graph of U.S. Apple Market Share over time.

Where this higher level of affinity for an application can be reinforced with ownership of an App Coin this effect can offer the App Coin an advantage over a system that uses Bitcoin for the same features.

Could be further breakdown to (a) increasing barrier of exit and hence increasing emotional ownership (b) boostrapping a network. The hardest part of any new network is always cold start problem, i.e. psychological resistance / inertia of adopting new things. AppCoin model leverages another human tendency , i.e. speculation and economic incentive, to overcome the inertia and reward risk taking.

###5) Freedom of Expression and Association Via an App Coin

During his keynote speech at the Bitcoin Expo 2014 in Toronto titled Andreas Antonopoulos makes the argument that App Coins will continue to multiply until everyone has such a token. He discussed thinking of currency as an application then thinking of currency as a means of expression.

This creates a situation where if a community wants to use a token to express a certain set of principles then that token will have a value to those that wish to identify or express those principles to others. This is evident in the different alternatives to Bitcoin that now exist.

####Example A. Choice of Monetary Policy
App Coins can serve as an expression and an implied voting for certain economic theory / monetary policy. Traditionally, you have something like USD controlled by Federal Reserve, that adopts dynamic economic policy but with certain tendency (e.g. Keynes) based on committee and specific economic situation. Then, you have Bitcoin, which adopts a fixed monetary philosophy. This has given rise to a competitive environment where many competing economic theories expressed in the form of algorithm - e.g. speed of new coin mining, inflationary or deflationary policies are being created with new coins. Some people decide to hold HayekCoin over FEDCoin because they subscribe to its monetary policy and believe it will hold value better in the long-term. And conversely those that decide to hold FEDcoin because they subscribe to its inflationary monetary policy and believe it will drive consumption are equally free to do so. One could imagine a whole varity of politics, ethics, economics and other beliefs that can be quantified and held as an identity in a Coin.

####Example B. The Decentralization Community
Some users are highly concerned with the that taking place in the mining market of bitcoin due to ASICs and as a response to that concern different communities have adopted scripting algorithms for mining of coins that are more ASIC resistant and thus in their minds preserving of .

####Example C. The Proof of Stake Community
For those users concerned with the use of large amounts of electricity in the mining process, the alternative use of has emerged as a low energy alternative was to maintain consensus in a trustless ledger system.

####Example D. The Privacy Community
For those user concerned with anonymity and privacy of their transactions alternative systems have emerged with their own

coins to serve this community.

####Example E. The Charity / Tipping Community

For those that identify with a more light hearted and charity oriented view of currency, alternative systems that make tipping behavior and crowdfunding of fun initiatives have emerged to serve those users.

###6) Preference for certain Economic philosophy thru AppCoin

Choosing a certain coin could also reflect preference over a specific economic theory. Traditionally, you have something like USD controlled by Federal Reserve, which adopts various economic philosophy over time (e.g. Keynes) based on decision of commitee members. Then, you have Bitcoin which adopts a fixed deflationary policy; so are most altcoins. In fact, many BitCoin fans promotes bitcoin heavily because of its deflationary nature.

In future, it's likely that many more AppCoins could adopt different economic theories, in the form of algorithm - e.g. a BernankeCoin could adopt an expansionary strategy where new coin mining rate dynamically adjusted to CPI data, or even allow manual intervention to mint more coin upon voting by stake of coin. As such, some people may prefer to hold BernankeCoin over BitCoin, at least for that specific app, because they subscribe to its economics philosophy and believe it encourages more economic behavior and beneficial to the app ecosystem.

###7) New mechanisms of price discovery and adjustment

One important use of creating a new currency is discovering and adjusting price for a product/service previously of unknown value. However, one might ask, how is that different from denominating in USD or BTC, then let service provider(s) compete and adjust price based on market reaction?

We'll discuss below why denominating in a new currency enable different forms, sometimes more effective, of price discovery:

####7a: Price discovery through initial public offering

Public offering for a specific product (whether initial, or multiple rounds) provides a unique and, often very effective, mechanism to discover price for a product in a short period. It also builds up marketing buzz around the product -- where branding and the initial network that it bootstrap could also be an important part of the value, yet this is only possible thru creating a new specific AppCoin, as opposed to reusing an existing currency (which has a larger pool of use cases by definition, and its value is inevetiably a function of multiple applications)

####7b: Demand-driven one-way price discovery
Price discovery is a two-way negotiation process between supply and demand.
However, one side always takes the first move.

Traditionally, when a currency is more established (like USD), the suppliers adjust its price dennominated in that specific currency, e.g. decrease from $15 to $10 if sales is decreasing.

On the other hand, creating a new AppCoin allows the reverse discovery process, i.e. a certain feature of the AppCoin Network could be pegged at a fixed rate against the AppCoin, e.g. 1 SafeCoin for 1G storage. Then the demand (buyer) would bid on e.g. USD:SafeCoin price to decide its actual value of that 1G storage.

This could become a more efficient process for some product, as pricing signal are manipulated directly by buyers rather than relying on supplier to act (which happens when they don't find enough buyers, a lagged signal). This mostly apply to a highly standardized & commoditized service, where all suppliers's service are equivalent in price (e.g. 1G storage is always 1 SafeCoin) and earn same income, hence no one gets a premium. Many decnetralized applications -- Tor, File storage, computational power, even BitCoin itself (where miner gets compensated at a fix BTC rate) all easily fall into this category.

On the flip side, this does create the reverse lag of pricing signal on the supply end. E.g., when SafeCoin go below a supplier's storage cost, some suppliers may leave the network (worse, many at same time). Of course, assuming same demand, users discover that storage become unavailable, they'd bid up the SafeCoin price, which encourages new suppliers to join the network. But there'd be a lag.

###8) Establishing a new unit of account
Every type of currency, esp. those well established ones like USD or BTC, people usually has a commonly used unit of account (e.g. 1 USD, or 1 Bits) and direct psychological association of its value (e.g. 0.1 USD "feels" a small amount of money).

Yet sometimes it's important to manipulate that perception in commerce -- esp. enabling "micro" transactions that fall below psychological threshold. Adding an extra layer of currency conversion, we're really cognitively abstracting the true value of the service away from the user, and making them less sensitive to its underlying cost/price.

Look at example of FavorDo, an app that allow people to ask for favor and help each other in a social network, with economic reward attached. When you ask for your friends of friends for favor with 50cents attached, people feel very little motivation to help or, worse, insulted. Yet, when you abstract it to 5000 FavorCoins (where the market value of a FavorCoin is really 0.0001), that might fare better.

Airlines mile rewards (e.g. it's not obvious what does 3000 miles really worth) and Doge Coin tipping, are similiar examples.

####9 Enabling (more) pre-sale of goods / service
Holding Currency is like holding on to generic futures of undetermined service, when it comes to AppCoin they're usually a more specific type of futures. E.g. SafeCoin is a futures for some undetermined storage / computation power.

People like choices. The liquidity and flexibility of AppCoin could encourage people to purchase (more of) these currencies, more likely than they would if you ask them very specifically to decide on X gigabyte of storage which they may not need right now.

SECTION TWO - Comparison of App Coins to Bitcoin
==========

###1). Why There Is A Need For More Than Just Bitcoin

Some in their analysis of App Coins think anything can be done with Bitcoin, when in reality only a very limited set of transaction types are possible in a fully decentralized way.

###2). Transaction Costs

Bitcoin reduces transaction costs for *specific* types of transactions. For instance it greatly reduced the cost of getting reimbursed for my expenses in the past few weeks - an employer was able to send funds from Israel to Canada in just a few minutes with total fees around 0.5% including the process of selling the bitcoins. Compare that

to the multiple weeks I'll have to wait for my cheque from the BBC to clear, along with about 5% fees.

But Bitcoin in its current form simply cannot lower costs for other types of transactions. For instance sending money with provably strong anonymity isn't yet possible in a decentralized way - the (future attempts to do this using Bitcoin are under development) App Coin Zerocash can do that because the underlying technology supports that type of transaction. Andrew Miller Infrastructure" is perhaps not the best argument for why forking App Coins is infeasible. Infrastructure in a decentralized environment, run by open source software, can be recreated instantly just the same way the software itself can. What can't be recreated is the social consensus, and we've already agreed that network effects reduce transaction costs by providing for more liquid markets. Having said that social consensus can change. Markets can be convinced by allegations of fraud and unfairness, or simply higher costs; this is a big part of why I think Mastercoin and similar systems must be interoperable with each other, and only require use of the App Coins for valid, justifiable, technical reasons.

An interesting thing you can point out here is how with the Zerocash App Coin the number of users directly relates to the size of your anonymity set - use a less popular fork and you're not as anonymous.

There is however a big gotcha with these arguments: converting the App Coin to/from Bitcoin can be highly efficient. If users only need to hold a given coin briefly to do whatever the application requires the velocity of the App Coin will be high and potentially demand low. Like the transaction costs, whether or not this matters is a case-by-case thing.

SECTION THREE - Comparison of the Different Consensus Systems
==========

###1). Zero Knowledge Systems

The "dark horse" is **(zk-SNARK). If you haven't heard of the term, basically they let Alice prove to Bob that she ran some specified computer program on a set of data, some of which may be hidden from Bob. The proofs are small (hundreds of bytes) and can be verified in constant time in the range of milliseconds. Computing the proofs is reasonable as well. Critically the program a zk-SNARKs proves can also include functionality to verify another zk-SNARK recursively. While this hasn't yet been demonstrated "in** production" it's quite conceivable that all App Coins can be replaced with a single zk-SNARK based system, kind of a hyper-optimized version of Ethereum. Such a system could be itself implemented as an Mastercoin-style embedded consensus system, resulting in "one App Coin to rule them all". Equally, Bitcoin can add such functionality.

###2). Hybrid Systems

A more near-term competitor might be hybrid systems that have both centralized and decentralized aspects. Colored Coins is a good example: you can offer to sell Colored Coins for bitcoins atomically in a completely decentralized fashion (4) with honest pricing and market depth, but can't offer to buy Colored Coins for bitcoins because Bitcoin does not understand the Colored Coin protocol. However you can of course have a centralized exchange perform that task, and you can use a variety of techniques to keep that exchange honest. (similar to the techniques to keeping off-chain tx providers honest)

The regulatory uncertainty surrounding blockchain-issued assets will likely prove to be a major "transaction cost" in the form of counterparty risk. But with hybrid systems you can have a decentralized layer to fall back on if any given exchange fails, giving assurance to users that replacements will pop up sooner or later. Centralized systems push down transaction costs in other ways and can provide speeds that decentralized systems just can't, so the net effect may be that the simpler hybrid systems, without an app coin, have the advantage for many applications. There is at least one player in the Colored Coins space that is looking at implementing this model. Equally chaum token using fidelity bonded banks (5) concept is a hybrid system that potentially competes with Zerocash.

Conclusion
==========

It's entirely possible that if you simply create an App Coin as a way to get money there is no purpose or value attached to that coin. Although calling them necessarily "fradulent" is going too far, there's a strong need to define the value of App Coins.

In this paper we have established many use cases where App Coins provide clear value. These cases include the benefit of having users as investors, increased network effect strength, presale of a token for fundraising, and various incentivization strategies that are missing in the world of mainstream investment. All of these point to the fact that App Coins can be valuable to both the people creating a project and those obtaining the coins.

That said, it is always worth considering App Coins in light of alternative strategies like crowdfunding efforts or simply creating a for-profit business. There is no single right answer and there are advantages to each approach depending on circumstances, technical requirements and economic motivations.

References
==========

1) http://cs.umd.edu/~amiller/permacoin.pdf

2) https://github.com/petertodd/timelock

3) http://twister.net.co/

4) [Bitcoin-development] Decentralized digital asset exchange with honest pricing and market depth, Peter Todd, Feb 9th 2014, http://goo.gl/ys5iXE

6) NETWORK EFFECTS AND COMPETITION: http://goo.gl/gIWWLJ

7) The Future of Crypto Currencies by Andreas Antonopoulos http://youtu.be/SHrjs7VkSGU

8) U.S. Apple Laptop Marketshare Graph http://goo.gl/sVlzGE

Appendix Case Studies
==========

See [reddit.com/r/whyxhasvalue](http://www.reddit.com/r/whyxhasvalue/)

1. [Why Mastercoins Have Value](https://github.com/mastercoin-MSC/spec/blob/master/WhyMastercoinsHaveValue.md)
2. [Why Ether Will Have Value](https://docs.google.com/document/d/1yh88h6FRAiB9-1_G0xlz2pvDN1Xo7o376xLkGksLLpg/edit)
3. [Why Counterparty XCP Has Value](https://docs.google.com/document/d/1rtzporRd-gSWf-H1wvrxdKxqXyr1SwXGzUzFztlBFM8/edit?usp=sharing)
4. [Why MaidSafeCoins Have Value](http://blog.maidsafe.net/2014/05/14/the-economics-of-safecoin/)
5. [Why SWARM Coins Will Have Value](https://docs.google.com/document/d/1UWE4s5mIwCaO3W7hqpd5d392QyUN

jsa1j5H2OeIUq5c/edit)
6. [Why LTBCOIN Will Have Value](https://docs.google.com/document/d/1r9D3pfv3sbqrNYvTIkRk2cEMEKegTBedVNKjeG6kDc4)
7. [Why API Coins Will Have Value](https://github.com/DavidJohnstonCEO/APINetwork/blob/master/README.md)
8. [Why Ripple XRP Have Value](https://ripple.com/partners/)
9. [Why Permacredits Have Value](https://docs.google.com/document/d/12JZqif8nO-hakiBp82UcEdomkorjVEm_I-VTfXu5WA0/edit)

TODO:

1. Why NXT Have Value
2. Why Rivetz Will Have Value
3. Why DERPA Coins Will Have Value
4. Why Storj Will Have Value