Astro

A Market Design Approach to Crypto

rkapurbh@gmail.com

January 2018

1 Introduction

In the time since January 2017, the market for cryptos has seen a tremendous run, with leading cryptocurrencies such as BTC, XMR, DASH, and ETH seeing price rises of 2000%, 3280%, 6710%, and 13230% respectively. Despite this change, the growth in transaction volume on-chain remains fractional compared to its accompanying price rise (see Table 1). Moreover, this on-chain volume data does not even begin to account for the probable inflation of transaction counts through 'mixers' (services that 'clean' money using complex networks of temp addresses) or the influx of first-time issuances to new entrants during the most recent runs.

Table 1: Change in Price vs. Transaction Volume On-Chain

Cryptocurrency	**%Δ Price**	**%Δ Transaction Volume**
BTC	+2000	+17
XMR	+3280	+90
DASH	+6710	+859
ETH	+13230	+2560

Considering only the frontrunner by market cap, BTC, its transaction volume on-chain accounts for a mere 0.85% of its increase in price. More interestingly so, within the same time frame, the volume for BTC on major crypto exchanges increased by 4400% (Table 2), roughly 2x the increase in price. While BTC's volume on-chain may account for real-world purchases, micropayments, mixers, and/or dark pools, the only possible use-case for on-exchange volume is, as the name suggests, coin exchange. Considering the demand for coin exchange far outstrips the demand for on-chain usage it becomes increasingly necessary to evaluate the crypto economy from a design perspective of all its component exchange-based markets: crypto-exchanges, ICO auctions, and the regulatory constraints imposed on the former two. Without getting into the 'Bubble or Not' debate, understanding the underlying market design may very allow us to

explain the events that led to the current run and build upon them for new classes of tokenized assets.

Table 2: BTC On-Chain vs BTC On-Exchange

Medium of Exchange	**%Δ Daily Volume**	**% of Price Change (in $)**
On-Chain	+17	+0.85
On-Exchange	+4400	+120

Market Design is the study of auction theory (i.e. ICOs) and matching theory (Crypto-Exchanges), but more broadly its the development of multi-stakeholder markets with potentially mislaigned incentives. With a reduction in the cost of creating financial instruments due to 'smart contracts' and the introduction of digital incentive through cryptocurrencies, conventional markets (IPO, Stock Exchange, OTC etc) and their incentive structures can be reprogrammed to meet the changing demands of stakeholders.

In our evaluation of the crypto-market we will make a few assumptions, namely, (1) the ordinary retail investor has limited access to high-risk/return investment opportunities and in searching for those opportunities within the crypto-sphere (2) an investor may invest in one of two distinct classes: cryptocurrencies or crypto-assets (collectively known as cryptos); both of which often, but not always, (3) employ the token model as a means of time-bounded digital scarcity in order to provide rent to purchasers.

This year alone the ICO auctions have raised upwards of $5B through new coin purchases, while the daily value traded across crypto-exchanges currently hovers around $50B. Above all, $500B of new wealth has been created seemingly overnight. By way of example, we present three market design decisions as axioms for the overwhelming interest retail investors have shown to the crypto market:

1.1 Borderless

Digital currencies bring the same consequences to money that the Internet enabled for information, with the added benefit of incentive. The two areas where these Internet-like implications are observed include; (1) the use of interconnectivity to establish digital and social networks, so-called network effects, as well as (2) the borderless and permissionless access that allow these network effects to scale at exponential rates. While the former can be analogized to the networked cooperation in the mining ecosystem, the latter reflects a paradigm shift for the use of money by reducing the marginal cost of acquisition/holding and the transaction cost of global transference to near zero. Crypto-exchanges and

ICO auctions have particularly benefitted from these reduced costs as evidenced by Kik's recent ICO that raised $98M from 10,026 individuals of 117 countries. To put that into perspective, 60% of the countries in the world participated in this token sale with an average contribution of about $10k.

1.2 Whale Preventing

The notion of whale prevention stems directly from the consensus mechanisms that govern the blockchains themselves. PoW and PoS both achieve consensus with minimum thresholds of fault-tolerance, 33% and 51% respectively. In order for consensus to work, the idea of massive wealth inequality cannot. This ethos manifests itself in the functioning of most cryptocurrencies and crypto-exchanges as well. The inherently fractional nature of cryptos allows for micro-investments while the 24/7 nature of both on-chain and on-exchange orders make cryptos time zone non-restrictive. Of late, such whale prevention tactics have also been adopted by ICOs through pre-programmed caps on investment, vesting 'smart contracts', and most recently Vitalik's Interactive ICO.

1.3 Liveness

In traditional financial markets, institutional investors compete, often with an edge, on one of two fronts: (private) information or speed. With the permissionless transparency of the Blockchain, information is produced constantly, publicly, and in realtime. Additionally, the entire information lifecycle of cryptocurrencies from their creation in open-sourced git commits, their deployment including soft/hard forks, all the way to their usage on-chain can be publicly accessed in realtime. This realtime public access (liveness) makes 'whale' frontrunning and competition on 'insider information' near impossible or at the least, very difficult. By democratizing this notion of private information and minimizing latency in the production of information, we should observe that prices reflect the strong form of the efficient market hypothesis, i.e. prices reflect all public and private information preventing anyone from earning excess returns on the market itself. Though in reality, this is not the case.

With the strong correlation of BTC to the entire crypto-market (centralized market exposure), flash ICO auctions propelled by 'gas', and coordinated Pumps and Dumps both on-exchanges and from open ICOs to exchanges, it becomes evident that in certain ways the existing crypto market has its own share of market failures. To correct these market failures, we present an end-to-end (ICO to Exchange) closed information system with novel data streams built upon a crypto-asset class that remains consistent with the above 3 axioms.

2 The Basket of App-Assets

Investors in crypto today bear significant market exposure (systematic risk). With significant cryptocurrency performance correlated (see Table 3) to one 'market peg,' the market suffers from a single point of failure. Strong correlations and accompanying lack of intrinsic value (common to all currencies) create market instability, i.e. unbounded upside and downside. This market instability hinders the creation of a number of crucial financial instruments, including, store-of-value currencies, stable hedges, uncorrelated crypto-collateral, and a multitude of derivative products.

Table 3: BTC 90-Day Correlation Matrix

	ETH	**LTC**	**XMR**	**DASH**	**ZEC**
BTC	0.31	0.46	0.45	0.26	0.36

The p-values above are computed from the log-returns of volume-weighted average daily prices over 90 Days. $0.1 \leq x \leq 0.3$: Weak positive correlation.$0.3 \leq x \leq 0.5$: Moderate positive correlation. $0.5 \leq x \leq 1$: Strong positive correlations

Most attempts at creating market stability focus on building non-volatile uncorrelated cryptocurrencies. These 'stable coins' fall into one of two categories : pegs or multi-coins. Pegs set fixed exchange rates to external stores-of-value that have existingly liquid markets (fiat currencies, precious metals, energy). For the fixed exchange rate to work in practice, the creators host a fractional reserve for the store-of-value. As such, investing into pegs provides no crypto upside with potentially centralized default risk. Multi-coin models avoid the overhead/risk of fractional reserves by simulating the expansionary and/or contractionary effects of monetary policy by making use of multiple separate coins (see Basecoin). In practice, of course, the added complexity of additional coins and the tradeoff of a reserve-based guarantee make multi-coins just as susceptible to speculative runs as most cryptos (if not more so).

One solution to the instability problem is diversification, i.e. investing cryptocurrencies in distinct classes of crypto-assets, each of which brings exposure to its own idiosyncratic risk (breaking crypto correlation). This works in opposition to the 'no intrinsic value' feedback loop of investing cryptocurrencies into themselves (read altcoins). Cryptocurrencies can derive value from their purchasing power of bundles of crypto-assets, similar to how fiat currencies derive value from their global purchasing power. If these crypto-assets belonged to highly liquid fiat markets, their purchase would be the equivalent to a fiat exit (being out of the money, so to speak). Moreover, these assets must have some notion of intrinsic value yet still remain borderless, live, and whale preventing.

2.1 Digital Assets & Monetizing the Web

Digital assets, like CryptoKitties, demonstrate the 3 crypto properties but lack the intrinisic value to make suitable (non-speculative) investments. Conversely, the more generalized form of digital assets that is internet-software (networked applications) often provides quantifiable tangible value to some subset of internet users while still remaining consistent with crypto properties. This tangible value, although quantifiable, is difficult to capture and monetize in the one-size fits all business model of the 'free' internet: advertising. The advertising model disproportionately benefits internet businesses at scale while disproportionately hurting the ones that are not. By way of example, according to a recent PWC report, approximately 75% of all internet advertising revenue is controlled by 10 companies. This has been the case for the last decade.

Arguably one of the most important use-cases of cryptos, as they exist today, is to capture the uncaptured value exchanged on the internet, across all levels of scale. The $500B of new cryptocurrency wealth can pay for this value in exchange for crypto-assets that tokenize the digital services that encapsulate it. In order to tokenize digital services while guaranteeing reliable ownership of the underlying value, we create digital equity-backed tokens (DEBT), the world's first global asset class. If in time networked software penetrates all businesses (read: 'software is eating the world'), then this uncaptured value may represent a portion of global economic activity or at least a large portion of internet activity. Thus making internet-software and the businesses that provide it one of the most valuable asset classes of our time.

2.2 App-Assets

In tokenizing the equity of digital services for crypto exchange, we must avoid the trap of using cryptos to invest in highly liquid fiat markets : think AAPL, GOOG, FB. In order to capture future value and avoid the liquidity problem above, the class of internet-software companies we tokenize will be limited to private software startups (starting with the Mobile App Store). Startups provide the same potential trajectories as existing cryptos while avoiding the asset correlation problem due to the idiosyncratic risk taken on by potential investors. Moreover, early-stage private companies exist in illiquid fiat markets that could highly benefit from the newly generated $500B of crypto wealth.

2.2.1 Cryptos and Apps

A comparison of the Mobile App Store and Crypto Market reveals interesting similarities. Many retail investors have turned to crypto due to a lack of high risk/return investment opportunities to place small-medium amounts of cash in. As we know, these high risk/return trajectories are most consistent with

those of early-stage investments. Using App Store rankings as a proxy for app risk/return (see Table 4), notable apps analyzed over the course of 1-week have been shown to move upto 89 places on the IOS app store and upto 23 on the Google Play Store. These movements, as observed below, are consistent with those of existing cryptos.

Table 4: 7-Day App Ranking Volatility

	App Store Δ in Ranking	**Google Play Δ in Ranking**
Duolingo	89	5
Venmo	36	23
Lyft	34	13
Linkedin	25	20

These values reflect cumulative change in ranking over the course of a week. Not the maximum uni-directional change (either upwards or downwards)

Besides these potential trajectories, cryptos also share a fungibility/likeness with one another. This likeness can refer to the similar ways in which they are transferred, decimalized, or produce new information (txns, block size, block time etc). Similarly, apps also demonstrate 'likeness' that cryptos do through shared ui components, user reviews, version numbers, and sometimes rankings.

Furthermore, the market cap of the entire mobile app market is currently around $3T, while the crypto market cap is $500B. Cumulatively apps generate 50.52% of all internet advertising revenue, which disproportionately favors the 10 largest companies. Yet most app companies are private and lean (approx 1-50). These apps require new business models (like the token model) to continue to survive in the whale favoring environment.

2.2.2 Token Model

The token model can serve as an alternative business model to help small apps compete with the whales who control most of the advertising revenues generated by the app store. The model refers to the use of tokens as a value store, while leveraging the tokens native properties of transferability, fungibility, and interoperability with other software systems and/or tokens. Currently, the token model has largely served as a vehicle for ICO investment into promising blockchains. Here are a few variations of the model that may be particularly useful for app startups:

1. Vehicle for ICO equity investment and value-based token exchange (i.e. exchanging one startup's equity for another).

2. Liquidity provider to startup equity owners (including founders, investors, and employees).

3. Stable in-app currency that can grant access to new features and/or beta test new services. Ownership of currency can also be used as a proxy for voting rights for new features, company governance, & software updates.

4. Vehicle for repurchase agreements between any combination of users, investors, or the company. For instance, a startup can ICO a token to fund a new feature. These tokens can then be repurchased by users who download/use the new feature (i.e. paying back the loan). BNB uses such a mechanism as a proxy for its quarterly earnings (proof of burn).

5. Vehicle for in-app betting and predictions. Especially useful with gaming apps or apps with an inter-connected competitive element.

2.2.3 Data Model

In tokenizing and trading crypto-assets, the market needs an efficient marker through which to evaluate these assets. While blockchain-based cryptocurrencies provide a slew of fuzzy data (txn count, gas price, contract info etc) through their open interface, the app-store is limited to three data funnels: app updates, user reviews, and store rankings (not always available). Each of these data streams provides minimal info on day-to-day user value and remains difficult to use for inter-app comparison. While metrics such as MAUs or DAUs would be useful in estimating tangible user-value, it remains noncompetitive for apps to display these figures publicly. Considering this dilemma, we develop 3 'live' data streams that allow investors to approximate user-value of any digital asset while still remaining too fuzzy for potential competitors to gain an advantage off of. The data streams are:

1. **Storage:** in GB

2. **Bandwith:** in Mbps

3. **Compute:** in flops

These 3 data streams effectively break down a networked computer into its fundamental components. A financial model built on any combination of these data streams could be used to approximate # of users, usage per user, user response to software updates, impacts of bugs, and many other proxys for present asset value. Additionally, the liveness of these data streams allows app-assets to trade on this information 24/7, much like existing cryptocurrencies.

2.3 Consistency with Axioms

Borderless: Internet Software is inherently borderless and permissionless. The same holds true for the App Store. The only exceptions to this lie in regional variations (like localization of language or service) or use of nation-wide firewalls (i.e. China).

Whale Preventing: We democratize equity by tokenizing and selling private early-stage equity to retail investors. This prevents financial whales from buying up equity in many private rounds before finally 'dumping' the equity on the public (through IPO).

Live: App reviews, versions, and rankings are sources of realtime information generated by the app store. Moreover, we provide 3 additional data streams that are both realtime and continuous: compute, storage, and bandwith.

3 The Exchange & Market Stakeholders

Decentralization is a goal of systems with complex moving parts (i.e. many stakeholders). Decentralizing largely involves equalizing the relative importance of stakeholders (or actors) and re-aligning incentive to a maximal end, reaching a market equilibrium of sort. The problem at hand is that centralized financial systems (like stock exchanges) tend towards "whales" for their ability to hedge risk and create market stability. For instance in the process of IPO to Exchange, there involve a few key stakeholders who have traditionally centralized/hedged risk: underwriters (Investment Bankers), investors (angels, vc's, funds), startup companies, and the exchange itself.

3.1 How the Current IPO Pipeline Works

To understand how these stakeholders inter-play we need to understand how they interact in the traditional IPO market. Currently, companies raise multiple private rounds of capital for equity (presumably at lower and lower prices). While the lower price per round trend doesn't always hold, it is generally the intent of founders to acquire strategic capital and not take on debt or sell more than desired. Eventually, the company reaches some scale and decides to sell its equity to the public market. Stakeholders like VC's, equity holders, and the founding team utilize risk underwriters (like investment bankers) to hedge the risk away from the issuance of stock and the new capital to be raised from the public markets. Once these underwriters have sold equity to large buyers to raise capital, the new buyers have the opportunity to dump the equity on the public markets. These underwriters and institutional buyers provide the centralized risk hedging notable to large financial systems like securities exchanges. Once the equity is listed and traded on-exchange, broker fees and co-location fees malign the incentives of exchanges. Exchanges sell the right to change a security's price/access and the right to snipe orders with latency faster than most retail traders have access to. The need for these institutions arises from a failure of the financial industry to have adequately adapted from its former

paper-based ways. In the modern crypto-financial system, a software based service can be built at low cost to enclose all these stakeholders in one end-to-end system.

3.2 How Astro Works

Crypto-assets to be listed on our exchange will, at least initially, be backed by equity and ICO'd on-exchange around Series A-C of the company's lifecycle. This stage is often referred to as the 'growth stage'. Since 2014 the number of VC rounds in early technology companies halved from 19k to 10k, early stage investments are risky for VCs and as such most have focused on inter-round arbitrage. By law 'seed stage' non-revenue earning companies cannot be sold as securities to public (unaccredited/retail) investors. Many obstacles hinder companies in this stage from going public: including lack of institutional early-stage investors and the cost of IPO'ing (due to underwriters and other fees). To solve the dearth of early-stage investments, the 'accredited investor' (i.e. vc's, angels, etc) miner ecosystem can use mining rewards to make more seed investments and bring more companies to market (positive investment feedback loop). In order to make this feedback loop work in practice the exchange must implement the decentralized infrastructure necessary to provide mining rewards (rent/dividends) to early seed-stage investors who have taken on the largest risk by investing in the earliest stage. Equity of these companies will be IPO'd similar to a direct listing, i.e. without the use of Investment Bank underwriters and many of the million dollar expenses that make IPOs cost ineffective for startups. Thus, making the IPO process more cost-effective for startup companies.

3.3 Decentralizing the Exchange and Stakeholders

In encouraging seed stage VC investment through mining rewards, we setup a decentralized model for an exchange to re-align and govern all stakeholers including: Underwriters, VCs, Equity Owners, and the Astro Exchange itself.

3.3.1 Underwriters

In the crypto market, most investors have small-medium amounts of capital (though the value of most sitting crypto has drastically risen) and are looking for high risk/return investments. Given the risk appetite of the investors, centralized risk hedging practices become less necessary, and as such the fees these whales eat away can be done away with.

Underwriters in the crypto market have largely been replaced by sound ICO practice and finality guaranteed by smart contracts. Existing ICO preocesses and listing procedures remain a good starting point for a crypto-asset listing. In the case of Astro we propose a direct listing (similar to spotify IPO) with a 30

day-sale (similar to Vitalik's Interactive ICO). The 30 day sale will halt withdrawals on the 20th day, while all bids will remain publicly accessible through the chain during the process. Each 10-day period may contain a bonus, like an early-bird special. At the end of 30-day period all orders are processed and a final price is determined. Each of these phases will be governed by smart contracts ran on-chain, as such it will remain infallible.

3.3.2 VCs, Founding Shareholders, & Investors

The current investment market has a dearth of early stage investors. These investors have dwindling incentive to go 'early' and instead play later stage inter-round arbitrage. Giving early investors a 'dividend' on their seed stage investment can incentivize a further increase in early stage investment. Providing these investors (miners) ongoing rent (mining rewards) on their investment by means of a decentralized multi-crypto exchange involves decentralizing the exchange order book. Decentralized order books face two critical design challenges: latency & transaction ordering.

Decentralized Order Book

High latency is common to public permissionless ledgers where state changes are bounded by block time (completion of a consensus round). Similarly total transaction ordering (agreement on same set of messages in same order or 'atomic broadcast') on public chains requires the assumption of synchronosity, which public permisssionless chains do not have. The tradeoff to synchronosity in public chains is increased latency.

In order to solve the challenges of decentralized order books, the properties of private permissioned BFT (Byzantine Fault Tolerant) chains become useful. Permissioned private chains such as (in our case) those built on top of Linux Foundations Hyperledger Infrastructure run BFT consensus (lower latency, lower fault tolerance) unlike traditional PoW or PoS consensus run by public permissionless chains like Bitcoin & Ethereum. Moreover a BFT consensus ordering service built on top of a secure private chain, such as the BFT SMaRT protocol, could gurantee low latency and total ordering of transactions of the ledger. The BFT ordering service built on a synchronous 2 stage (endorse, verify) SMaRTstate machine replication protocol achieves a throughpout of 10,000 txns/sec.

BFT consensus algorithms demonstrate the agreement (global truth), correctness (local truth), and liveness (fault tolerance) properties of most public and private chains. This class of consensus algorithms operate with a fault tolerance of 33%, i.e. tolerance against 3f+1 faulty (f) nodes in any given round of consensus. Existing protocols such Ripple's RPCA and Stellar's Consensus Protocol use different variations on BFT consensus for its light weight and low

latency benefits. The low latency consequences to decentralized securities exchanges could allow for near real-time performance of order books and create a mining economy for decentralized assets.

Miner Ecosystem

Aside from the low cost, low latency, and total ordering advantages of private chain order books, these order books still remain consistent with crypto axioms, live (on-chain txn data), borderless (24/7 order book access), and whale preventing (VC Miners). What we refer to as VC Miners are no more than peers hosting a decentralized BFT consensus guaranteed transaction ledger.

Often, miners earn some rewards in exchange for the validity and finality they bring to the current state of the ledger (in our case, order book). On Astro, mining rewards are earned by a flat fee (approx 0.1%) applied to every cleared and processed order book transaction. Mining fees will be awarded to miners proportional to their global percentage of processed orders for a given order book. Since our system differs from traditional consensus systems, miners will not earn a transaction fee directly from the orders they process but rather earn a percentage of the global transaction fee for any given consensus round on equity's order book.

Mining Fees

Transaction fees applied to matched orders will be split evenly by buyer and seller. Half the reward will be denominated in crytpocurrency and the other half in crypto-equity. Over time such a fee would have a deflationary effect (similar to many token models like Bitcoin & Filecoin) on the order books float. Once a certain amount of market float has been captured in fees, an order books 'seller fee' will be dropped leaving only a buyer fee for matched orders (reducing friction in selling). Moreover, these fees will remain decreasing over time (bounded by a positive number for miners rewards) for all order books, based on some function of cumulative volume traded and time since listing.

Mining Rewards

Rewards from the transaction fees are distributed between the miners and the exchange to better align the incentive of early-investors and securities exchanges. Miners receive a fractional share rewards from a global fee pool based on the percentage of their processed (matched) orders. Miners (early accredited investors) benefit in two specific ways from these dividends: it provides them rent for high risk start up investment, and provides additional capital to invest in more rent-earning start up companies. While high capital owning investors may earn low mining rent on these high risky assets, retail investors with small-medium sized amounts of money can use the volatility of the asset to diversify

their own holdings. This works against the tradition of institutional 'whales' accumulating equity in multiple private capital rounds of financing before dumping it on the public markets.

3.3.3 Astro Exchange & Traders

The final stakeholder is the exchange and the traders that use it. As mentioned decentralized order books face structural problems (latency, ordering), but existing stock exchanges face issues of bad incentive. Existing stock exchanges have failed to adequately transition from paper-based ways to digitized stakeholders. As such many exchanges rely on layers of fees from brokers, colocating servers, and listing fees. Exchanges effectively sell the right to restrict access/price and buy better prices. In decentralized order books, colocation is theoretically infeasible due to the distributed nature of miners but in the worst case it can be disincentivized through mining rewards (and other more centralized tools accessible to private chains). Moreover, an end-to-end system of digitized stakeholders can effectively can supplant the need for brokers offering identical products. In order for the exchange to remain a neutral entity among all stakeholders, it will take on the role of an asset manager. Equity denominated fees earned from all equity order books on the exchange will position Astro as an asset manager of start up equity (high growth assets) that is inherently dependent on the volume of global unbiased orders (a positive feedback loop).