# How to invest in Cryptocurrencies - A model of value capture in decentralized application ecosystem

Nikhil Malik
Carnegie Mellon University, Pittsburgh, Pennsylvania 15213
nmalik1@andrew.cmu.edu

The scale of investments raised by Initial Coin Offerings (ICO) has generate a debate on how to value Crypto coins and what ICO's to invest in. We first present a contrast against traditional monopoly platform to highlight the potentially revolutionary benefits of decentralized Proof of Work (PoW) crypto platforms. A monopoly investor profits from collection of transaction fee revenue (*Operational Value*) in every period while a PoW investor extracts a one time *Turnover Value* by sale of tokens. Unlike a monopoly, PoW's *Turnover Value* driven revenue mechanism does not incentivize investment in platform quality. PoW's potential to expand user surplus by banishing monopoly control over transaction fee is diluted by a low investment in platform quality. Proof of Stake (PoS) which promises to eliminate PoW's wasteful puzzle solving turns out to instead raise the fees for users. From an investors point of view PoS allows monetization of both *Operational Value* and *Turnover Value*, thus a preferable alternative in most cases. PoS platforms, as a middle ground between PoW and monopolies, are best bet to disrupt existing monopoly intermediaries.

We further assess partition of value between decentralized protocols (Bitcoin, Ethereum, EoS) and applications (Augur, CryptoKitties, uPort) on top of them. Our model supports the *Fat Protocol* hypothesis i.e. larger value capture in protocols. We independently show three contributing factors - first mover advantage in setting platform design by protocol investor, *Store of Value* characteristic of protocol tokens and direct network effects. We also present empirical evidence in the form of two prevalent phenomenon - *Ecosystem Funds* and *Protocol Forking*. Investors looking for the Amazon's and Google's of the decentralized era must look to high quality Proof of Stake protocols with a vision to either create or subsidize creations of applications.

## 1. Introduction

### ICO Tokenomics

Initial Coin Offerings (ICO) have become a significant mode of raising capital for entrepreneurs globally. In 2017 alone more than $5 Bn dollars were raised through ICO's,

a trend which is not showing any signs of slowing down in 2018. Traditional entrepreneurs raise funding via Venture Capital wherein the investors (VCs) become equity holders. A stake in equity gives the investors power over the companies management as well as a share in future profits. ICO's that raise investment to build decentralized platforms do not necessarily promise any decision making rights over future of the platform or profit payouts. Instead the investors are rewarded upfront with native digital (crypto) tokens. Ecosystem of economic activity on these platforms is partially walled off from outside world by enforcing usage of native tokens - instead of fiat currency- for using the platform. User demand for native tokens to transact on these platform creates a liquid token/fiat exchange markets. The investors that see early value in the enterprise sell these native tokens when a significant user demand for transacting on the platform raises the token prices. The developer teams typically *promise* to hold significant chunk of their earnings in tokens. A shared risk of future token prices somewhat allays investor uncertainty on future direction of the platform.

The sudden rise in this form of investment capital begs the question - what makes these decentralized platforms unique? These platforms offer connectivity among its user to buy and sell goods & services, however unlike traditional online marketplaces or banks they offer decentralized transaction processing. In case of a financial transaction, activities such as checking for double spending, maintaining ledger of activity and account balances are performed by consensus among individual *miners* instead of a trusted intermediary. A traditional platform often derives revenues from charging a fees (above the unit cost) for this transaction processing. The trust posited by users on the traditional intermediary allows it to generate profits for investors (equity holders). Decentralized platforms instead

open up these activities to be performed by any individual, thus encouraging lower fees by competition among *miners*. Low fees from near perfect competition among willing *miners* coupled with algorithmic trust has the potential to transfer a significant surplus to the users. We build a model to show this transfer of surplus when comparing a traditional monopoly with a decentralized platform.

This lack of control over revenues from transaction fees mean that traditional VC investors can not derive regular profits. A critical element of our model is to capture the alternative mechanism for ICO investors to make profits. ICO investors that receive a fixed supply of (initially worthless) native tokens upfront re-sell these tokens when prices are driven up by demand. Note that a traditional VC investor in a startup (say Facebook) may profit from passing on its equity stake to other private VCs or open market via IPOs as valuation of the company rises. A ICO's (equity-like) native token is not just passed on from investor to investor, instead its eventually passed onto users. For example a platform with a supply of 100 tokens that attracts user turnover worth $ 1 Mn (all denominated in native token) results in a token value of $ 10,000. A portion of the fixed token supply may remain in hands of investors who continue to expect perpetual growth in user demand. Users of traditional platforms (Facebook, Amazon) do not hold equity in the companies, users of decentralized platforms must hold native tokens. Going forward our model refer to traditional revenues from transaction fees as *Operational Value* and returns from resale of native tokens to platform users as *Turnover Value*.

Bitcoin the first and most popular platforms for decentralized financial transactions best represents this mechanism of rewards for investors. The original creator and other early

contributors of Bitcoin acted both as developers and investors. They created Bitcoin's open source code base and deployed hardware for transaction processing in return for native tokens. In its early days with non existent user demand these native token rewards were worthless. Further Bitcoin by design openly allowed new miners (with transaction processing hardware) to enter thus giving no control over possibility of future profit from transaction revenues. However these early investors held on to their native tokens long enough to benefit from growing user demand. By some estimates Bitcoin creator Satoshi Nakamoto is estimated to have been worth $19.4 Bn. Unlike Bitcoin, most platforms today are built by developer teams that diversify some of the financial risk by raising a portion of initial investment through private and public ICOs. In this paper going forward we use the term *investor* to mean both the developers and investors.

The low transaction fees for users and novel investor reward mechanism appears revolutionary at first glance. Our model illustrates two significant limitations - (1) Low platform quality and (2) High fixed cost of trust-less consensus. A traditional intermediary chooses a transaction fee level to maximize its *Operational Value* i.e. a very low fees leaves very little revenues after paying for processing costs while a very high fees curtails the demand. In order to raise fees while keeping the demand, the intermediary invests in platform quality upfront. An ICO investor does not have the same incentives from raising fees by investing in higher quality. The *Turnover Value* is maximized by attracting the largest possible demand by keeping fees as low as possible. The result is a cheap but low quality platform. The seemingly large user surplus is therefore largely wiped out when our model accounts for the optimal choice of investment. We characterize the market parameters where the decentralize ICO platform still dominates a traditional monopoly platform.

The second limitation arises because the platform relies on consensus among anonymous miners. Every individual miner (performing transaction processing) needs to exhibit a *commitment* in the platforms success. Proof of Work is one such mechanism where miners reveal a large stake of computing resources in return for ability to process transactions and collect fees. The computing resource stake is credibly signaled by quickly solving crypto graphic puzzles. A single dishonest miner would need to stake a prohibitively large amount of computing power to over power the remaining mining community. Somewhat counter productively, the lower transaction costs achieved by allowing zero barrier entry to miners is reversed when we account for this cost of mining. If a PoW platform design does not enforce a sufficient level of mining cost, it risks relatively cheap attacks from dishonest adversaries. The investor must balance the two objectives - maximizing *Turnover Value* by dropping the fees and keeping the overall fee collection high enough to admit a minimum level of mining cost expenditure.

The Proof of Work (PoW) mechanism has been widely criticized for generating exorbitant amounts of energy usage during wasteful puzzle solving. In PoS miners must have stake in native tokens instead of computing hardware in order exhibit commitment in platform success. Similar to PoW, a dishonest miner needs to acquire a very large stake of native tokens in order to attain monopoly power over transaction processing. Any perceived tampering would result in loss of user demand and thus an exorbitant cost to the dishonest miners holding large volumes of the same token. Proof of Stake was suggested as an alternative mechanism which largely eliminates wasteful energy consumption. Consequently, one expects PoS to return this conserved *surplus* back to the users.

Our model shows that surprisingly, PoS can be worse off for the users. PoS creates additional demand for holding the native tokens by the miners. If miners are able to charge high fees, new miners enter the transaction processing raising the demand. As a result the token value increases until the cost of holding a stake of tokens matches the transaction fee revenue. The investor is now able to monetize both the *Turnover Value* driven by user demand and *Operational Value* driven by miner stakes. It leaves relatively smaller surplus for the users and gives back extra source of revenue to the investor compared to PoW. Since the investor is at least partially rewarded for improving utility (by raising miners ability to collect higher fees) they invest more upfront into the platform quality. PoW is an extreme mechanism that result in low fee, low quality and large user base compared to a traditional monopoly. While PoS typically turns out to be middle ground between PoW and traditional monopoly subject to market and platform design parameters.

While our model assumes constant market size, both PoS and PoW expose users to volatility in transaction fee with evolving demand. While volatility may be normal in some markets (e.g. housing), it would be anomalous in other situations (e.g. file storage). A dual token PoS is yet another token model where the transaction fees is fixed in terms of a token pegged with fiat currency while a second token floats with fixed supply floats in value driven by demand. Our model shows a similar outcome for the dual token PoS as described for single token PoS. Specifically in constant market size setting these two models turn out to be equivalent. Beside these three models, numerous other mechanisms - proof of burn, triple token, pegged token, access based token, buyback etc have been proposed in recent times. We currently skip individual treatment of all of these models for now.

### Protocols and DApps

Market for ICO driven platforms has somewhat fragmented into Protocols and Applications. A Protocol platform offers a base layer that can be used by multiple applications. Application on the other hand focus on specific markets such as - Sports betting (Augur), Voting (uPort), Blogging (Leeroy), Social Networking (Steem). Early platforms - such as Bitcoin, Litecoin - offered a combined protocol and application layer for financial transactions. More recent protocol platforms - such as Ethereum, NEO, EoS - do have some native application but they offer easy development of other applications on their ecosystem through *Smart Contracts*. While protocol layer delivers core functionality such as correctness of transaction history, elimination of double spending etc, the application layer perform more application specific tasks such as reporting outcome of a sport event (Augur) or rating online content (Steem). This fragmentation has some parallels with the evolution of TCP/IP, HTTP protocols and Google, Facebook, Amazon as applications on the internet. The internet revolution witnessed significant revenues for application making them some of the biggest firms on the planet while the protocol layer was unable to monetize its wide usage. Investor community has been forced to answer the same question in the Blockchain revolution, what will capture the value - protocols or applications.

We model a multi stage game where the protocol and application investors sequentially make investment and other platform design choices in the first period. Users and miners who fully observe the platform qualities create demand to buy native tokens from the creators in the second period. We assume that all participants hold rational homogeneous beliefs of market size and the market size remains constant in the second period and beyond. Given a constant market size and therefore token demand, investors have no

incentives to hold back any tokens from sale to users and miners in the second period. The token value realized in second period therefore remains perpetually constant. We use a discounting factor to incorporate any opportunity cost of investing in interest bearing fiat assets or a risk of decentralized platform collapse faces by users holding the tokens. While our results do not change drastically, we model a Proof of Stake (PoS) mechanism for both the protocol and application.

We show that the *Operational Value* is shared between the protocol and application investors with the protocol capturing a larger chunk by its first mover advantage. The *Turnover Value* goes to application layer alone. We first model a setting where a single application is built over the platform and users do not directly interact with the protocol at all. Interestingly, even under such extreme setting the protocol layer is a more profitable investment. The turnover value - demand by users to hold application tokens - captured by application does not prove enough of a compensation. This gap between the value of protocol and application widens when we consider multiple applications on a single protocol. Firstly, by a simple network effects argument i.e. applications capture value proportional to $n_a^2$ (number of users on application a) while protocols with many applications (a1,a2, a3) monetize quadratically larger networks effects $(n_{a1} + n_{a2} + n_{a3})^2$.

If we restrict to markets where users do not derive utility from direct network effects i.e. utility from a transaction remains the same irrespective of network size. A larger number of applications still result in widening gap between protocol and applications values. Increasing number of applications encourage users to hold protocol tokens and exchange for application tokens only for the duration of application usage. The protocol token resembles

a *store of value* while the application token becomes a *means of payment*. As a result the token velocity on application increases relative to the velocity on the protocol. For example an application with a fixed supply of 100 tokens and a periodic turnover of $1 Mn but with a token velocity of 10 (same token used in multiple sequential transactions) results in a token value of $1,000 instead of $10,000. In contrast *Store of Value* tokens exhibit a relatively low velocity as users hold a large enough pool of tokens in case of unexpected upswing in their need to use multiple applications.

We find support of our theoretical findings in the prevalent *Fat Protocol* hypothesis among Venture Capitalists and other practitioners. This hypothesis predicts that - unlike the internet era - most of the investor value will be stored in the protocols instead of applications. As of June 2018, the market capitalization of Bitcoin and Ethereum stand at $112 Bn and $46 Bn respectively. In comparison some of the most popular DApps CryptoKitties, IDEX (currency exchange), Etheroll (gambling) have a market capitalization of $12 Mn, $17 Mn and $8Mn USD respectively. CryptoKitties application at its peak accounted for 5-10% of transactions on Ethereum protocol but the value posited in its native coin remained (1/10000)th of Ethereum. Protocol *forking* is a widely observed phenomenon where application developers (when not using an ecosystem fund) fork (copy) an existing protocol. They prefer to make their application available on a copy of the existing protocol (with zero initial adoption) instead of using the existing protocol (with sizable adoption). This is a complementary evidence toward the greater value posited in protocols. Ownership of protocol has stronger promise of future value capture than ownership of application on an already adopted protocol.

On the basis of the result described above naturally application investors under invest in the quality of the platform in the absence of expectations of future revenue. This hurts the protocol investors potential for profits. We expand our model to allow an artificial (credible) mechanism for transfer of investment by the protocol investors into application layer quality. Consequently, the protocol investor is willing to subsidize application developer with positive transfer of investment. This prognosis from our model once again finds evidence in the recent emergence of *Ecosystem Funds*. These Venture Capital backed funds are promised by protocol investors as investment to a sizable number early high quality applications. Note that such empirical support - market valuations and investor choices - for our theoretical model come with serious caveats. Beside a few broadly accepted breakouts - Bitcoin, Ethereum, Ripple etc - a large number of tokenized applications and protocols have turned out to be shams. The market valuations for vast majority of these platforms may turn out to be bubbles. At the very least the current state of decentralized platforms as well as beliefs of investors and users show little stability

Finally an interesting argument for low valuation of decentralized platforms relates to the open source nature of these technologies. In theory, any room to make positive profits by investors is lost if their technology can be readily copied over. A new investor could simply copy over the technology and offer the native tokens at a discounted value. In practice we have observed significant stickiness exhibited by users once they trust the quality and development teams behind a platform. While we model a single stage of platform development, in reality users expect ongoing technology updates and therefore they are reluctant to jump over to a technology copy without committed technologists. Our model side steps this interesting phenomenon for now by assuming un-forkable application technology. We discuss qualitatively some implications of open source technology to our primary results.