Difuon Fog–Dual Tokenomics: *Redemptive Benefit Token*

Samuel M. Smith Ph.D.[1]

Original 2018/10/25, Version 1.3, 2018/11/29

Abstract— . A novel dual utility tokenomics model is described consisting of both a medium-of-exchange (MoE) token and a store-of-value (SoV) token that together provide true separation of concerns between the need to support stable pricing, low friction, and high throughput transactions and the need for appreciative value to reward virtuous participation on the platform including investment. This approach avoids the inherent conflict between the two concerns that is the root cause of the failure of the single utility token model. A key insight is that optional utility is still utility. Once separated from the constraints of stability, low friction, and high throughput, the SoV token mechanism design can be fine-tuned to improving participation and value growth in the associated platform. A new complex SoV token is introduced called a redemptive benefit token that employs several complementary features that limit downward volatility and drive virtuous behavior and value during different growth stages of the platform. We call these *HoDling* powers. This approach is general and can be beneficially adapted to many utility token applications.

Index Terms— *Tokenomics, Dual Token, Utility Token, Mechanism Design, Stable, Investible, Separation of Concerns,*

1. Utility Tokenomics

Many Blockchain-based business models are of some form of two-sided marketplace or network. This is more formally called a *platform* business model [13; 32; 33; 44]. One the reasons for using a distributed ledger is to provide a trusted way for multiple parties to exchange value over a network by tracking the associated transactions in the ledger. Moreover, the trust in the system may be enhanced if the governance and control of the distributed ledger is decentralized or diffused across many parties. Obviously, a good way to facilitate and track the value exchanged in the transactions is to use a currency as the unit of account and the medium of exchange. A good medium of exchange has the following features: low friction, widespread access, high throughput, low latency, high velocity, low average settlement cost, and stability. Low friction means that the use of the medium of exchange is highly convenient for the participants. Widespread access means that likely participants have the potential to obtain the medium of exchange in order to participate. High throughput, low latency, and high velocity mean that turnover in units of the medium of exchange is rapid so that transactions are not impeded by the mechanism for settlement of the transactions. Low average settlement cost means that the fees or overhead costs on average of using the medium of exchange for a given transaction are very low relative to the value of that transaction. Finally, stability means that the change in price of products and services in the medium of exchange due to volatility, appreciation, or depreciation is insignificant relative to the product life cycle. Fiat currencies like USD exhibit most of these characteristics, especially cash. The problem is that for a network the transactions must be electronic (digital) such that cash is not practical. This then requires some electronic payment channel which may introduce some latency to the transactions, and whose provider may charge relatively large settlement fees especially for micro- or nano-transactions. The requirement for an electronic payment channel may often limit access by some participants, especially the unbanked. But all else being equal the low friction, high velocity, and stability of fiat make it the primary candidate for an electronic medium of exchange.

The fact that the distributed ledgers can be used to support a cryptocurrency or a cryptographic token has created the option where the medium of exchange is a crypto token instead of a fiat currency. The main attraction of a cypto-token as a medium of exchange is the potential to have lower latency and lower settlement costs relative to conventional electronic fiat payment channels. Another attraction has been the potential to have pseudonymous transactions like cash but electronic. A popular type of crypto token is a *utility* or *usage* or *network-medium-of-exchange* token [8; 41; 52; 68; 72]. The term utility is used because the token derives value from its utility in the functioning of the associated network or platform. Typically, the primary function of the utility token is as a medium of exchange and unit of account for transactions on the network. Another function of utility tokens is to incentivize the participation in the network to support the distributed ledger and other related functionality. This is done by awarding tokens to participants who perform these functions.

2. Single Utility Tokenomics

But what has really accelerated the adoption of utility tokens is as an alternative means for raising non-equity-dilutive capital in order to fund the creation of the associated online marketplace [11; 14; 41]. This is done through a series of token generating events, where tokens are sold to investors that are then traded on exchanges. This type of raise is typically called an ICO (Initial Coin Offering). So far in combined 2017 and 2018 almost 2000 startups have raised over 13 Billion dollars using ICOs [30]. In

1. Senior Member IEEE, CTO Co-Founder Difuon.

order for a utility token to be attractive to investors it must have an appreciative quality, meaning that the investors must be able to buy low and sell high. The hypothesis is that a large appreciative driver of price for the token can be created by limiting the supply and making network function highly dependent on the use of the token [20; 41; 72]. As the value of transactions on the network grows demand for transactions will drive demand for tokens which given the limited supply and functional dependency will drive the price upwards. The token then acts as a store of value that is appreciating over time[7; 9]. The simple approach to forcing functional dependency is to have a single utility token for all functions of the network. This also simplifies the software needed to support the network function relative to the token. This is the approach that the majority of the early and existing token generating events have taken. A source of problem is the thought that one should add as many sources of value to the token as possible in order to enhance the market value of the token [72].

There are two serious flaws in this hypothesis. The first is that merely limiting the supply and functional dependency are not sufficient to drive the price upwards, the velocity of turnover of the token must also be kept low [4; 12; 15; 68]. That is, relative to the latency of transactions, the availability of token reuse for subsequent transactions must be kept low. This is in direct conflict with the desirability of using a cypto-token as a low friction, low latency medium of exchange. The second flaw is that appreciative price of the token is in conflict with its use as a stable medium of exchange. As the token appreciates in price, the price of products and services on the network also increase making the network as a whole less attractive to alternative markets that provide competitive products and services[12; 15; 40]. This becomes a disincentive for participants to use the network to exchange products and services. Only products whose demand is highly elastic relative to the price will be attractive on a platform where the pricing is going up fast relative to the product lifecycle and opportunity cost elsewhere. Together the low availability of tokens and the appreciative pricing are strong counter drivers to product demand. These means that the network value never grows or grows so slowly that the intrinsic demand for the token as a medium of exchange never grows or grows slowly thus nullifying the appreciative driver that was the motivation for using a utility token in the first place as a means of raising capital. In other words, it is not practical to use a single crypto token as both a *store-of-value* (investable, appreciative) and as a *medium-of-exchange* (low friction, stable). Another way of looking at this is with Gresham's law, that states, "bad money drives out good" [10]. What this means is that if two tokens are in circulation with the same face value, the more valuable one will disappear from circulation, i.e. it will stop being used as a medium-of-exchange. A good medium-of-exchange must be just a little bit bad so no one prefers holding onto it over exchanging it.

The result is that the most of single utility tokens have failed already or are predicted to fail in the marketplace [23; 36; 38; 70]. The usual lifecycle of a single utility token follows: The initial sale price to investors is usually discounted from what the expected price will be once the network is functioning and is approaching its market potential for transaction volume and value. Prior to network going online, the tokens are traded on an exchange and the price is purely speculative. Hype and promotion of the potential value of the network (*pump*) incentivizes secondary buyers to acquire the token at a higher price, thus allowing the initial investors to liquidate their tokens at a profit. In most cases, the liquidation floods the market with more tokens than the demand can absorb and the price drops, thus incentivizing investors to liquidate even faster (*dump*), thus driving the price to a relative zero [19; 31]. This is classic example of the *greater fool theory* in action [25; 26]. The price charts for the vast majority of single utility token raises have followed this pattern [47]. Two examples are shown below [17].

Fig. 1. EOS Price chart

Fig. 2. Tezos price drops as soon as listed on exchange.

A small percentage of networks funded this way have gone online and are selling products and services. In many of these cases, however, either the velocity of the token is high enough that the network is functional without the token price appreciating back to anywhere near its pre-launch levels or the network pricing has appreciated making the products and services uncompetitive. In a notable case, QuantStamp, the network added a fiat payment channel in order to restore price competitiveness [6]. This addition removed most of the value of the token (the network is no longer functionally dependent on it in a non-trivial way). Prior to this change the Quantstamp token had been generally appreciating. Afterwards the price declined never to recover.

Fig. 3. QuantStamp (QSP) Price Chart

The failed actual performance of dozens of networks over the last few month due to these characteristics is a strong refutation

of the single utility token hypothesis [35].

3. Multi-Utility Tokenomics

A more complex nuanced approach is to use two or more tokens for the function of a given network. Given the failure of single utility tokenomics, a motivation for a dual or multi-token approach is to support the separation of concerns between the use of a token as a medium-of-exchange (MoE) (non-appreciative, stable) and a store-of-value (SoV) (appreciative, investible). Somewhat confusing is the fact that some networks like Ethereum (Ether and Gas) and VeChain (Vet and Thor) use dual utility tokens to separate other concerns such as a floating price relative to Ether in Gas for the spot pricing of computation on the network independent of the pricing of products and services provided by the network [51; 62; 67]. Such is an example of dual utility tokens for two different network functions. Also confusing are dual tokens of different types. The first token is a utility token, which is used as a medium-of-exchange on the platform. The other token could be of a different type such as a security token or an asset backed token [1; 27]. A security token has rights to equity or share of profits and is not part of network function but appreciates based on the value of the equity and/or profits generated by the network [65; 66]. The problem with security tokens is the lack of viable security token exchanges [5]. An asset backed token derives its value from an associated asset that has intrinsic appreciative value based on property (real or intellectual) or a scarce commodity [3]. Of note is the distinction between a utility token that is sold as a security and a security token. Under US securities law the Howie test determines whether something is a security or not. Simply if a token is sold that does not have true consumptive value or the buyer does not have reasonable consumptive intent then that token could be a security. Before a network or platform launches a medium-of-exchange token has no consumptive value and is therefore its sale is likely to be considered that same as the issuance of a security [34; 42; 71]. Once the network launches then sale of the token might not longer be considered a security issuance.

> *To that end, a better line of inquiry is: "Can a digital asset that was originally offered in a securities offering ever be later sold in a manner that does not constitute an offering of a security?" In cases where the digital asset represents a set of rights that gives the holder a financial interest in an enterprise, the answer is likely "no." In these cases, calling the transaction an initial coin offering, or "ICO," or a sale of a "token," will not take it out of the purview of the U.S. securities laws. But what about cases where there is no longer any central enterprise being invested in or where the digital asset is sold only to be used to purchase a good or service available through the network on which it was created? I believe in these cases the answer is a qualified "yes."*[71]

Herein we focus on multi-utility tokenomics for the purpose of separating the two concerns of medium-of-exchange and store-of-value. The core thesis is that an appropriately designed *dual utility token model* allows one of the tokens to be a store-of-value utility token which provides liquidity to investors when traded on available exchanges (unlike security tokens) and may appreciate as a function of the value of the associated network while the other token acts as a low friction high velocity medium-of-exchange thus avoiding the drawbacks of a single utility token model. The key insight is that optional utility is still utility. The network can function as a successful competitive business consummating transactions merely with a medium-of-exchange utility token without requiring a store-of-value utility token. However, the store-of-value token, although optional, can provide additional value to the participants in the network and to the function of the network that may be appreciative in nature [58]. Indeed, the flawed hypothesis that *required utility* is essential forces the inherent conflict between appreciation, pricing elasticity, and velocity that has resulted in the almost universal failure of single utility token models for anything other than as pump-and-dump speculative vehicles.

The medium-of-exchange token could be fiat. Indeed, given the low friction, relatively high stability, high availability and low latency of fiat, it is difficult to argue that the medium-of-exchange should be anything other than fiat. Currently most non-fiat tokens have super high friction to on-boarding participants and converting their fiat to non-fiat utility tokens. This friction has become even higher in the USA, because the IRS classifies non-fiat crypto token exchanges as asset transactions subject to capital gains taxes. The biggest motivation for using a non-fiat token would be lower latency and lower settlement costs than existing electronic fiat payment channels. But in either case, because the world runs on fiat, having a transparent fiat payment channel to access a non-fiat medium-of-exchange token is essential to universal adoption of the network. One way to achieve both stability and lower settlement costs is to peg the utility token to fiat for stability, but batch the conversion to and from fiat to reduce settlement costs. The simplest peg is an ephemeral two-way one-to-one peg with a liquidity pool in fiat. Ephemeral means the token is minted and burned on demand. A fiat-pegged stable ephemeral utility token is not appreciating or depreciating by design so it is not investable or tradable, but may only be used to acquired products and services on a platform. These are good features from a regulatory perspective. This type of ephemeral peg is in contradistinction to non-ephemeral but stable crypto-currencies that are meant to be traded [18].

An example of a utility token medium-of-exchange with a fiat payment channel is the Stellar network, wherein fiat anchors provide credit from fiat accounts for end-to-end fiat-to-fiat transactions that use the utility token (Lumen) as an ephemeral medium-of-exchange [56]. The fiat anchors provide fiat liquidity pools to back the credit they extend for the duration of the transaction settlement time (< 5s). The result is that Stellar acts as a transparent, low friction, low latency, fiat payment channel with low average settlement costs. The Stronghold network on top of Stellar is providing a USD pegged anchor [10]. Utility tokens used as a medium-of-exchange would want to exhibit similar features.

There are other more complex ways to implement a stable utility token such as using an algorithm for fine tuning dynamic supply that may make the token even more stable than fiat. However, for many two-sided network business models, fiat is sufficiently stable such that a simple peg is all that is needed if not fiat itself.

Given that a low friction, high velocity, stable medium-of-exchange token (which may be fiat) is used to consummate transactions and pay participants for supporting the network, an optional companion store-of-value utility token can be added without conflict with the function of the medium-of-exchange token. Primarily the optional utility comes from using the store-of-value token to promote and reward virtuous participation in the network. Such a token may provide value as a marketing tool to incentivize adoption, shape behavior, and reward participant-sourced improvements to the network. These are all good drivers of the positive two-sided network effects that enhance value of the network. These drive the network dynamics with positive feedback loops. The goal is that the platform via its mechanism design and associated algorithms may automatically result in appreciation of the SoV token as the network grows.

3.1. Redemptive Benefit Token

We have designed a new kind of optional store-of-value utility token as a companion to a medium-of-exchange in a dual token model. We call this new store-of-value token a *Redemptive Benefit Token* (RBT). Mechanism design is a term used to describe the process of coming up with the functions of a token in a system that drive it to attain certain behavioral characteristics. The redemptive benefit token is based on a mechanism design with mutually reinforcing feedback loops that incentivize desirable behavior and de-incentivize undesirable behavior in the tokenomics. Its primary goal is to incentivize growth and good behavior of participants in the network while limiting downward volatility and allowing for upward appreciation in the price of the token. The token benefits both its holders and the network. In homage to the internet meme resulting from the drunken misspelling of *hold* as "*hodl*" to describe the practice of holding onto store-of-value tokens, which serendipitously is also an acronym for "*Hold On for Deal Life*" *(HODL),* we have titled these mechanisms the "*HODLing powers*" of the redemptive benefit token [24; 28; 61].

3.1.1. Hodling Powers of the Redemptive Benefit Token

The redemptive benefit token (RBT) approach to providing a store-of-value (SoV) token that works with a companion medium-of-exchange (MoE) token combines the beneficial properties of gift card, loyalty, rewards, and staking programs to incentivize acquisition and holding of the SoV token in the following ways:

(1) **Redemption:** Like a gift card SoV tokens can be redeemed at the rate specified by the MoE tokens for items on the platform's products and services menu. The menu is two-sided with one side priced in the SoV token and the other side in a MoV token which is pegged to fiat. This provides a composite floor value of the SoV in fiat that is equal to the consumptive weighted average of the fiat value of the items in the menu. This is designed to minimize downward volatility and help ensure purchaser's of SoV tokens who purchase at a discount realize positive returns and also virtuously ensures that later purchasers of SoV tokens are protected from downward volatility. The redemptive value is effectively a worst-case value for the SoV token once the network is live.

(2) **Promotion:** Like the points in a loyalty program, SoV tokens may be redeemed for MoE Tokens for products and services at promotional prices provided only to members of the program. This allows conversion at better than retail rates and allows for anti-Moore's Law appreciation as service classes through the Menu are upgraded over time in response to technological advancements. This drives early adoption by users of the Project and enables repeated adoption acceleration as new products and services are introduced to the network through the menu at promotional pricing.

(3) **Rewards:** Like a rewards membership, holders of the SoV may earn MoE tokens as of function of both their holdings of SoV and their spending in MoE on the platform. These earned MoE Tokens may then be redeemed in exchange for Fiat at the rate specified in the Menu or used to purchase additional products or services on the platform. The earning rate of MoE per expenditure of MoE is an inverse nonlinear function of the number of SoV they hold. For example, a holder of 10,000 SoV would earn MoV at a higher rate (but less than 10x) for the same expenditure of MoE than a holder of 1,000 SoV. The exact nonlinear function and parameters is tuned to the market dynamics. An example of a nonlinear function is given in section 4.2 below. This incentivizes large users of the platform to hold increasingly large numbers of SoV in order to obtain larger rewards in MoE. The amount of SoV held increases as a function of the market cap of the network in services provided. Holding of the SoV token can be further incentivized by increasing the discount as a function of the time the SoV token is held

(4) **Membership:** Like membership in a club, participation in several activities within the network require the staking (holding) of SoV. These include, either directly or as a delegate, the hosting of support nodes, the voting on the use of community tokens for bounties, or the voting on features and upgrades to the network protocol. This staking rewards good participant behavior by providing the opportunity to share in the revenue generated from fees associated with supporting the network and dis-incentivizes bad behavior as participants would lose their stake as a result. The participation strength is an inverse nonlinear function of the amount staked. This also greatly incentivizes the holding of large numbers of SoV that increases as a function of the size of the network infrastructure.

Given that the supply of SoV is limited, then the holding drivers above would increase demand for SoV as the transactional value of products and services exchanged on the network increases, thereby providing an appreciative driver to its price.

The Redemption HODLing Power above is designed to limit downward price pressure when the network is small whereas HODLing Powers 2, 3 and 4 above are designed to provide upward price pressure for SoV tokens well above their redemption value as technology improves, usage expands, and participation in the platform increases. The intent of this design is to produce a price curve with beneficial characteristics. The Membership HODLing power uses staking of SoV to ensure good behavior. It

can be thought of a potentially refundable license fee or deposit that enables an entity to host a platform node and receive transaction fees for that hosting. Should the entity misbehave then they lose both their membership and their staked SoV fee/deposit. A notional example of the pricing behavior due to the combined effect of the four HODLing powers over time is shown in the following diagram.

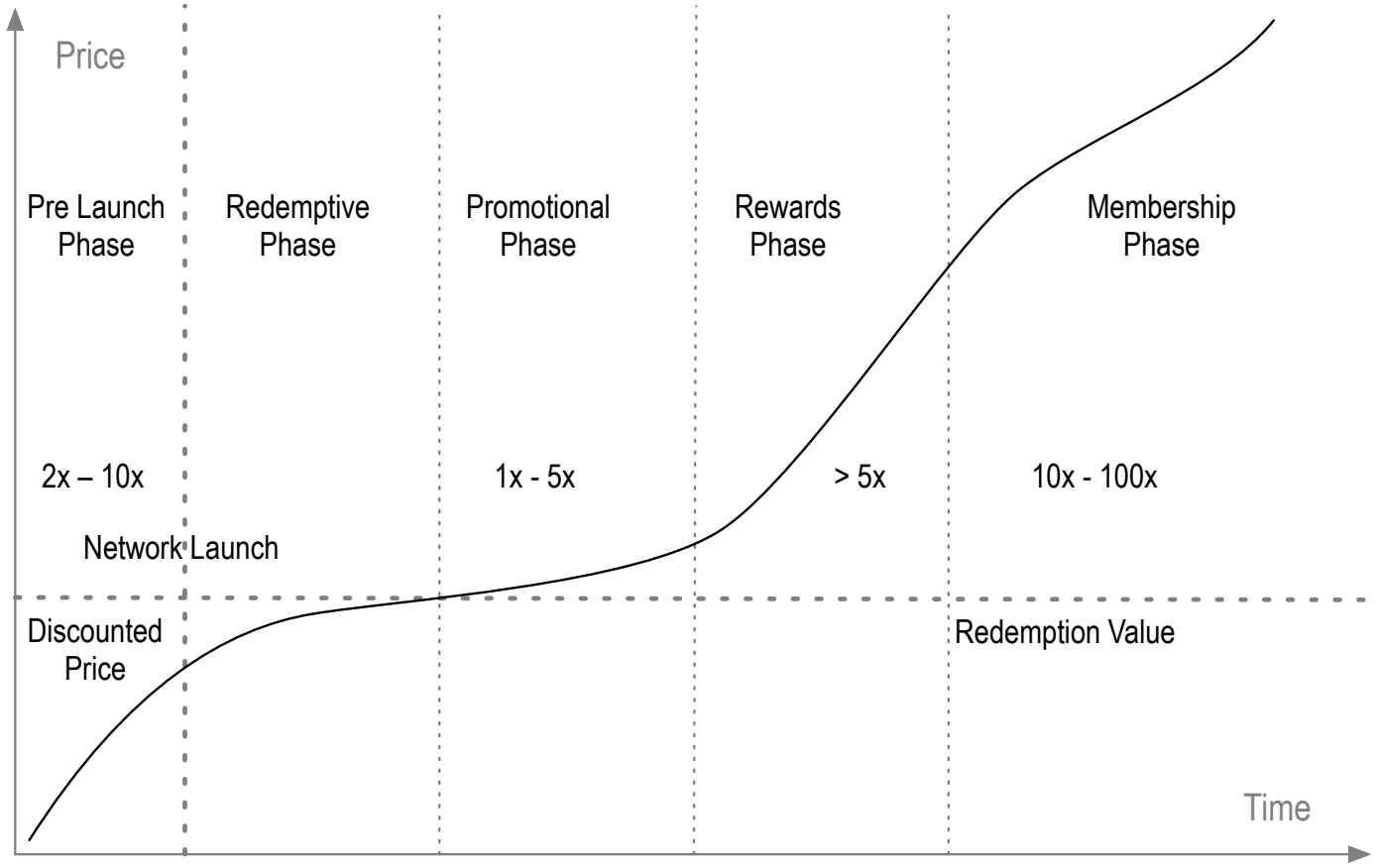

Fig. 4. Notional phased price versus time for SoV token with HoDling powers.

Discounted pricing of the SoV may be viewed as a type of warrant on future margins of the products and services. The number of discounted SoV tokens must therefore be limited and only be available prior to network launch during a pre-sale with a cap on money raised. To limit the rate of redemption of discounted SoV tokens and further incentivize holding, time locks and/or time variable redemption rates can be employed. A time lock can freezes or locks a token so that it cannot be redeemed until the lock expires. A time variable redemptive rate increases the discount as a function of time up to some maximum. This allows for immediate redemption but rewards the holder for waiting longer to redeem.

There are two main paths to obtaining MoE Tokens in order to purchase products and services off the menu. The first path is by purchasing SoV tokens and then redeeming them for MoE Tokens that may then be used to purchase products and services from the Menu. The second path is by purchasing MoE Tokens for fiat directly. The first path may reward investors and other platform participants. The second path may enable wider adoption through more conventional retail fiat purchasing. Products and services are priced in MoE Tokens and the MoE price is pegged to fiat. This stabilizes the price of the MoE token so that it is less susceptible to the pricing volatility which could hurt the competitiveness of the platform. Indeed, the MoE token could be fiat. A good peg is USD because of its ubiquity as a reserve currency but may be changed to one or more alternative fiat currencies on a geographic basis or to a basket of fiat currencies or some other pegging mechanism. The goal of this approach is a more stable price for products and services relative to fiat that is decoupled from the price dynamics of the SoV token.

Once the network is launched, the platform may offer additional retail SoV (at their redemption price or higher) in limited amounts to ensure liquidity, pay usage based earned rewards, and as bounties for team and community efforts to build and enhance the platform.

An alternative approach is to not enable paths through the two-sided menu from the SoV side to the MoE/fiat side. One reason to do this would be to remove the fiat liquidity pool requirements for issued SoV tokens for items on the menu. This means that producers any item on the menu would be willing to accept payment in SoV and not MoE/Fiat for that item. If not then the menu item is not accessible from the SoV side. Likewise a menu item could only be accessed from the MoE side and the producer would not accept SoV tokens. This could enable the platform time to build up liquidity. This would also simplify the demands on producers who wish to put their own items on the menu. The problem however is that it limits the accessibility of participants to products and services on the menu. In other words, some items can only be purchased and paid with MoE/fiat and some items can only be purchased and paid for with SoV.

In any event accounts are differentiated by the path through the menu for sake of refunds. The path out is always the reverse of the path in from the standpoint of refunds. This means that transactions maintain the path through the menu until final settlement. For example, if a purchaser has 60 days for a refund then the transaction path must be retained for 60 days to enable a refund to retrace the path in. If a refund does not retrace the path in then participants might try to arbitrage different effective SoV valuations for different items in the menu. This may defeat the promotional value of variable pricing in the menu. This is not a problem for MoE that was the result of a fiat only purchase but only MoE that came from an SoV redemption. SoV redemption can be thought of as creating an MoE voucher. The voucher persists until final settlement including any refund time periods. For example should someone redeem SoV in build but not consume all the services immediately then some balance will be outstanding. If at some time later (within the refund) window, the purchaser desires a refund then the refund amount is the amount given by the original redemption voucher path from SoV to MoE. This means that purchasers do not have an account with undifferentiated MoE. They have pools of MoE corresponding to the path into the purchases. These include a fiat pool (came in from fiat), and a separate pool for each menu item path they used to convert from SoV to MoE. Functionally SoV are very much like points in a loyalty program and menu items represent special certificates and vouchers that result from redeeming points for services. The points stay points until they are consumed with finality, that is, a final un-refundable purchase.

3.1.2. Use Cases

Consider for example a consumer that wishes to purchase products or compute services listed in the menu:

- The consumer is not interested in participating in the platform other than merely buying compute services at the prices offered in the menu. The sharing economy nature of the network should make some of those services competitively priced. Using the fiat purchase path the consumer can then buy those services using a similar payment channel to existing alternatives. The fiat payment channel transparently converts fiat to MoE tokens which are used as a medium of exchange and unit of account on the network. This payment channel seeks to minimize the friction to the consumer.
- Alternatively, the consumer may prefer to take advantage of the promotional pricing that may be available via an SoV purchase from the platform directory or the consumer may instead be able to buy an SoV token from someone else at a discount to its redemption value for products or services on the menu. The menu is two-sided with each item priced in both SoV and MoV tokens. Some items on the menu might be of more use to a given consumer based on the consumer's need and thereby might offer better value when purchased via the SoV channel rather than for fiat. A consumer, may be able to create better overall value for themselves. rather than by using fiat payment channel.

Consider another example where a consumer bought SoV at a discount or even at retail face value but held onto them until the network has grown and the reward or staking demand for the SoV has raised the price of the SoV token on an external exchange to above the redemption value of those SoV tokens via the Menu. Further, suppose the consumer now desires to purchase products or services from the platform. Given the SoV value on an external exchange is above the redemption value from the network for the SoV held by the consumer, the consumer may instead seek to obtains a greater number of products or services for those SoV than their face value by first selling some SoV on an exchange for fiat and then use the fiat payment channel to buy MoE tokens to obtain the products or services from the network.

Suppose instead that a large enterprise consumer of services from the platform wishes to obtain those services at a discount to their retail price. The SoV rewards program provides MoE tokens as a reward for the purchase of services as a function of the number of SoV tokens held at the time of such purchase. This effectively discounts the price of those services for such a consumer. The enterprise consumer would then buy and hold SoV tokens to enable the rewards of MoE tokens every-time the consumer purchased MoE tokens and hence services using the fiat payment channel. Notable is that the consumer does not redeem SoV tokens in this case but instead holds them in order to get rewards of more MoE tokens for the purchases of services through the Project.

Finally, suppose a participant on the network wishes to have a new feature added to the network and would like to vote for that feature. In this case the participant buys and holds SoV that it stakes SoV in order that the participant can vote on the new feature to be paid for with SoV tokens from the community allocation.

3.1.3. Simplified Examples

The redemption and promotion HODLing powers rely on a two-sided menu. A simplified example is shown in the following diagram. In the examples, the currency symbol for MoE/Fiat is $ and the currency symbol for SoV is #.

SoV Reserve Pool
0

SoV #	**Menu** *Products*	*MoE $*
1	P1	1
3	P2	3
4	P3	4
2	P4	2

MoE – Fiat Liquidity Pool
$ 0

Fig. 5. Two-sided Menu. Center column has product names; one per row. The left-hand column has the price in SoV. The right hand column has the price in

MoE/Fiat. Also shown is the reserve pool for redeemed SoV and the liquidity pool of fiat to back the MoE account balances.

In the following diagram is shown an example fiat transaction using the MoE side of the menu.

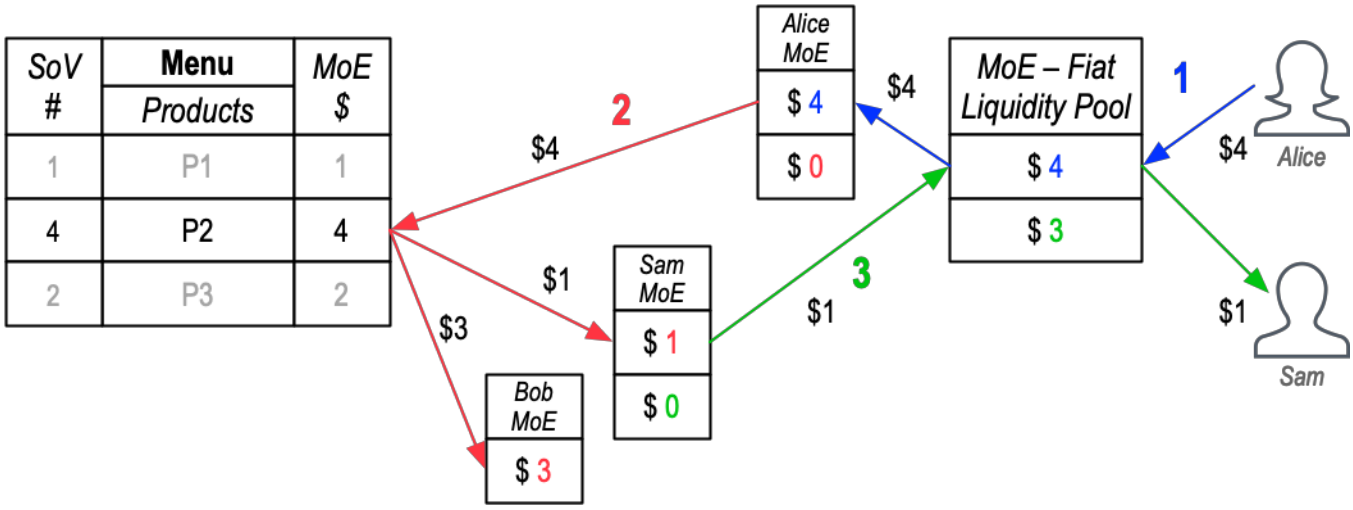

Fig. 6. Example MoE transaction. Color coded steps show account balances at the end of each step. Step 1: Alice (customer), chooses to buy product P2 from the menu using fiat (USD). She deposits $4 fiat into the liquidity pool and gets a $4 credit in MoE into her MoE account. The liquidity pool now has $4 and Alice has a $4 credit in her account. Step 2: Alice's $4 MoE credit is spent to purchase P2 and is deducted from her account. Bob (the platform) provides P2 to Alice. Bob pays $1 to Sam's (supplier) account for supporting the product leaving $3 in gross profit margin in Bobs account. Step 3: Sam cashes out by withdrawing $1 from his account and converting it to fiat through the liquidity pool. This leaves $0 in Sam's account and $3 in the liquidity pool.

In the following diagram is shown an example redemption transaction using the SoV side of the menu.

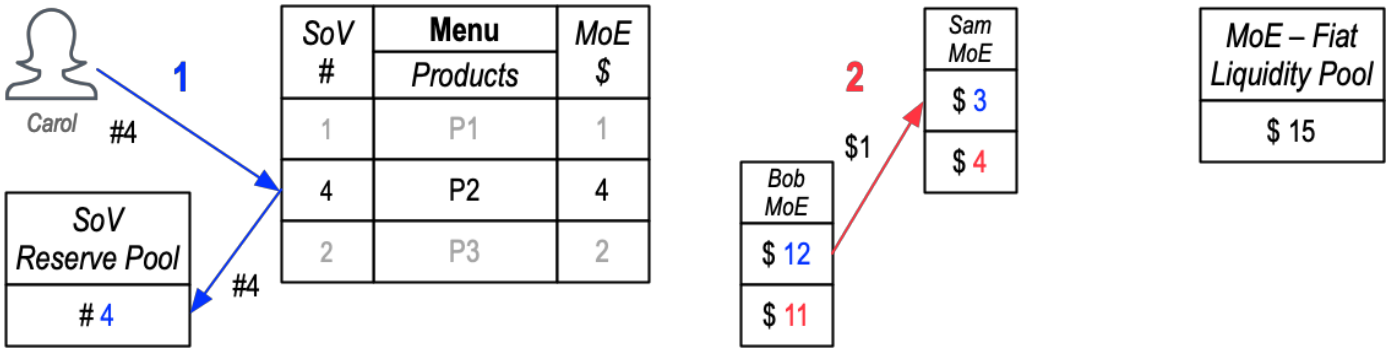

Fig. 7. Example SoV redemption transaction. Color coded steps show account balances at the end of each step. Starting balances: Sam = $1, Bob = $12, Carol = #4, Reserve Pool = #0 . Step 1: Carol redeems her #4 of SoV tokens for product P2 using the SoV side of the menu. The #4 SoV tokens are accepted by Bob (platform) and sent to the reserve pool. Bob gives product P2 to Carol. Bob does not get paid any MoE by this transaction. Step 2: Bob pays Sam $1 for supporting the product. This is deducted from the $12 in earned gross profits in Bob's account. When Bob originally sold the SoV tokens, (think gift card), Bob incurred a liability to provide products and services from the SoV side of the menu in return for the SoV in the gift card. Bob, when honoring the gift card for P2, must pay for his actual costs of providing the product. Bob's out of pocket costs to Sam are only $1. This cost is deducted from the accumulated gross profit on all of Bob's prior sales in Bob's MoE account and paid to Sam's MoE account. At the end of step two, the reserve pool has #4, Sam has $4 in his MoE account, Bob has $11 in his MoE account, and the liquidity pool still has $15.

In the following diagram is shown an example promotional redemption transaction using the SoV side of the menu.

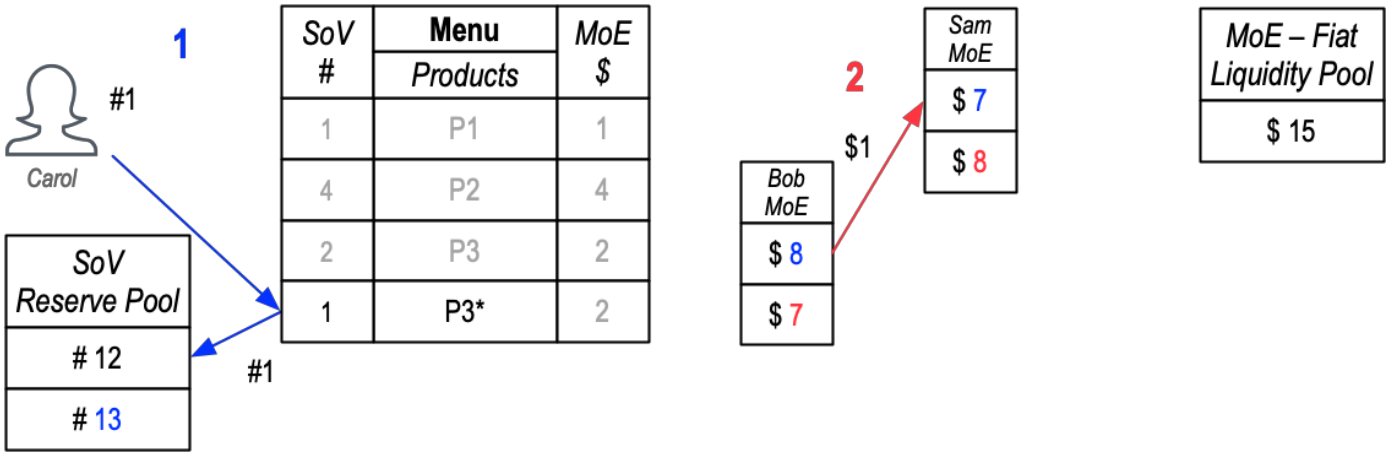

Fig. 8. Example SoV promotion redemption transaction. Color coded steps show account balances at the end of each step. Starting balances: Sam = $7, Bob = $8, Carol = #1, Reserve Pool = #12. Menu has new entry named P3* which is a promotional version of product P3. The promotional price is #1. Promotional P3* may include other special time or quantity provisions. During the promotion the value of an SoV token redeemed for P3 is now effectively doubled. Step 1: Carol chooses to redeem #1 of her SoV for P3*. The #1 SoV token is accepted by Bob (platform), and goes into the reserve pool. Bob gives product P3 to Carol. Step 2; Bob pays Sam $1 for supporting the product. This is deducted from the $8 in earned gross profits in Bob's account. Bob does not get paid any MoE by this transaction. Someone choosing to buy P3 with fiat must still pay $2. At the end of step two, the reserve pool has #13, Sam has $8 in his MoE account. Bob has $7 in his MoE account and the liquidity pool still has $15.

3.1.4. Summary

The goal of the dual token model is to provide more sophisticated tokenomics behavior that rewards and incentivizes participants as the network grows while also providing for competitive overall pricing.

To reiterate, the MoE tokens are pegged to fiat at a fixed stable exchange rate. Associated with the fiat payment channel will be a liquidity pool of fiat. When consumers of services originally buy MoE tokens using the fiat channel, some or all of the fiat used to purchase those MoE tokens will go into this liquidity pool. The associated MoE tokens are then used to buy services. The service providers receive MoE in exchange for providing services. From time to time the service providers may then choose to exchange their MoE back through the fiat payment channel and receive fiat from the liquidity pool. The motivation for using MoE tokens as a medium of exchange instead of fiat is that the settlement costs and latency of the fiat payment channel may be too high for the nano transactions needed to support services. The fiat-to-MoE conversions and the MoE-to-fiat conversions are batched to reduce costs and improve throughput. Over time, the liquidity pool may have an excess that is a result of the gross margin between what services cost in the menu and what service providers are paid. This excess can then be used for other purposes without negatively affecting MoE liquidity.

The tokenomics of SoV Tokens is wholly distinct. The platform will redeem SoV with MoE using the menu value of the associated services at the time of purchase (which can be valued at the corresponding pegged fiat value). This effective menu-based exchange rate may be significantly different from the floating exchange rate between SoV and fiat on a third party exchange. The associated MoE are then used to buy services. The service providers receive MoE in exchange for providing services. From time to time, the service providers may then choose to exchange their MoE back into fiat through the fiat payment channel and receive fiat from the liquidity pool. The liquidity pool will need enough excess to cover the eventual conversion of MoE back into fiat that were first sourced as SoV. This excess may come from funds raised on the sale of SoV or from the accumulated gross margin on the purchased services. There may be some liquidity risk should a large amount of SoV be sold at a discount greater than the equivalent gross margin of the associated services on the menu. The discounted SoV liquidity liability may be covered by the accumulated excess in the liquidity pool resulting from the gross margin on services bought by others at a less discounted price.

At some time in the future, once the platform is live and experiencing healthy revenue growth and profits and with appropriate regulatory approval, the platform may choose to also provide more convenient exchange paths for participants at the prevailing external exchange rate to directly exchange MoE for SoV, or SoV for fiat, or fiat for SoV. The reason for providing such exchange paths would be to reduce the friction experienced by participants in order to increase the rate of adoption and the size of positive network effect feedback. Initially, however, prior to network launch the only provided paths of exchange will be (1) SoV to MoE to fiat and (2) fiat to MoE to fiat. In each case, the fiat conversions will be through the fiat payment channel and liquidity pool. Direct conversion of MoE to SoV, SoV to fiat, and fiat to SoV, and will not be initially supported by the platform and must be performed on a third-party exchange, if at all.

4. Balancing Participants Interest and Influence

The main purpose of the SoV token is to incentivize beneficial participation on the platform. The token is used to positively reward good behavior and negatively reward bad behavior. We call the anticipated rewards or return of a participant their *interest* or *interests*. In a decentralized system multiple we call the control that some participants might have over some components of the network or the behavior of other participants, their *influence*. Its usually bad for the platform when the interests and influence

of some participants are such that they can use their influence to enhance their interest unfairly. Consequently one purpose of mechanism design is to build checks and balances on participant's interests and influence. For example, with the first two HODLing powers, *redemption* and *promotion*, SoV holders do not have much influence and their interests are simple. They merely may choose to make arms length exchanges of tokens for products or services. The exception is that when the platform is small, a holder of a large number of SoV tokens could pose a threat by redeeming to many tokens relative to the platform's capacity or liquidity. As previously mentioned, one way to balance this influence is to lock the tokens for some minimum time period or to have an increasing redemption rate that penalizes/rewards early/late redemption. The last two HODLing powers, *rewards* and *staking*, on the other hand have much higher potential for beneficial or detrimental effects on the platform.

4.1. Privacy and Consistent Pseudonymity

One complicating factor in online platforms is privacy. Because all transactions are performed electronically over a network it is easier for third parties to monitor and correlate transaction activity thereby reducing the privacy of the primary parties and putting them at risk of exploit by a third party. Exploits range from nuisances like spam more serious harms like slander and theft. To better describe the associated issues we first define some terms. We use a simple definition of *identity*, that is, an *identity* consists of one or more *identifiers* and associated *attributes* [53–55; 57; 60]. An *entity* may be any person, group, organization, computing device or software program. An *entity* may control or be associated with many *identities*. The set of all identities for an entity is its *identity graph*. Typically governments allow only one *legal identity* for an entity. Use of a *legal identity* puts the entity at risk to legal recourse for its associated transactions. Use of the legal identity also puts the entity at risk to exploits by malicious third parties. This is a two edged sword. In a transaction, knowledge of one party's legal identity by another imposes a check on the one party's behavior due to the risk of legal recourse for misbehavior. The use of the legal identity increases trust and facilitates the transaction. This is an incentive to use a legal identity. Indeed the POA network uses the risk of loss of reputation associated with verifiable legal identity as type of bond to ensure good behavior [45; 49]. Unfortunately, the risk of loss due to third party exploit may far outweigh the benefits of using a legal identity on a given online platform.

An alternative is to use a non-legal but consistent pseudonymous identity for online transactions. A consistent pseudonymous identity is based on a verifiable unique pseudonymous identifier. Typically this is a type of cryptonym based on a cryptographic public/private key pair. The emerging decentralized identifier (DID) standard is the best example of this type of identifier [21; 57]. Dozens of organizations are now either building portable identity systems or using such systems based on DIDs [2; 22; 37; 43; 59]. Consistency means the entity uses the same identifier for all transactions on the platform and all parties can verify the identifier is being used by the entity with the associated private key. Consistency allows a reputation to be associated with the identity which can build trust. Consistency also allows the platform to reward behavior of a given identity thereby also building trust. Pseudonymity preserves some privacy by making it more difficult for third parties to correlate to the entity's legal identity or other off-platform identities. Privacy may further be protected using zero-knowledge proofs (ZKPs) of credentials attesting to an entity's identity [49]. The Sovrin network is designed to better manage privacy loss using zero-knowledge proofs [60]. This comes at the cost of increased complexity and computation. The drawback of allowing pseudonymous identities on a platform is that entities may create multiple disposable or "*cheap*" identities that enable them to engage in bad behavior with little consequence to the entity. One form of bad behavior is a Sybil attack where the entity creates sufficient numbers of pseudonymous participants to unfairly distort the entity's influence or to overwhelm the network [64].

One approach to this problem is to force disclosure to a unique legal identity. This is the approach that banks must use in order to comply with legal regulations to impede criminal activity. This approach is called KYC/AML (Know Your Customer/Anti-Money Laundering) [16]. The problem is that legal entities may be organizations such as corporations that may be controlled by other entities. Setting up multiple legal organizations is more costly than creating pseudonymous identifiers but may still be relatively inexpensive. Because natural persons are unique, the ultimate nexus of interest and/or control will reside in a set of natural persons that are the ultimate beneficiaries of the organizational entities. Consequently KYC/AML requires disclosure of the natural persons that are the ultimate beneficial owners (UBOs) of organizational entities[29]. This may be a very high friction high cost way of preventing the use of multiple cheap pseudonymous identities for the same entity (even via private disclosure via zero-knowledge proofs). For many platform business models it may not be practical or economically feasible to use this approach, that is, proving traceability to the underlying unique legal identities. Instead a lower friction approach to mitigating the risks of multiple cheap pseudonymous identities may be to use economic incentives that reward the concentration of activity into consistent pseudonymous identities. For other platforms, especially where higher value participation occurs, it might be appropriate to use a mix of economic incentives and legal identity proving to mitigate the risks of both privacy loss and bad behavior. The next section describes how to build in economic incentives for concentrated activity.

4.2. Concentrated Interest Via Nonlinear Rewards

One way to penalize the use of multiple pseudonymous identities by the same entity on a platform is to reward the concentration of activity (interest) into one consistent identity. A consistent identity means that all the activity is attributed to a verifiable identifier or a set of linked verifiable identifiers. Attribution of activity to a consistent identity is a very basic form of reputation. Ultimately, what any party uses to decide whether or not to engage in an online transaction with another party is the reputation of the other party [53]. Suppose an entity is considering splitting its activity on a platform into two or more participant identities. If the the sum total interest of the split participants is less/greater than what it would be if the activity were concentrated into one participant identity then the entity has an disincentive/incentive to split. If on the other hand the the sum total interest of the split participants is the same as that of a single concentrated participant identity then splitting makes no difference in the reward.

Other factors, such as a desire to engage in untraceable bad behavior, would then govern the decision to split or not split. This latter case is true when a reward function satisfies the superposition property or principle [48; 63]. In other words, the sum total interest is the same for either split activity or non-split activity. When the reward function satisfies the superposition property, there is no penalty with respect to the reward function should an entity choose to enable its own bad behavior by splitting its activity across cheap pseudonymous identities. Consequently if some other factor provides an incentive to split then the reward system does nothing to counter that other incentive. The superposition property or principle provides a departure point for analyzing reward functions with regards to participant splitting. The definition of the superposition principle follows: Given a system reward function *R* with input *x* and output *y* at time *k*. Let

$$y_1(k) = R[x_1(k)] \tag{1}$$

$$y_2(k) = R[x_2(k)] \tag{2}$$

$$x_3(k) = a_1 x_1(k) + a_2 x_2(k), \tag{3}$$

where a_1 and a_2 are arbitrary scaling constants. Then we have,

$$y_3(k) = R[x_3(k)] = R[a_1 x_1(k) + a_2 x_2(k)]. \tag{4}$$

The reward function *R* satisfies the superposition principle if the output also satisfies,

$$y_3(k) = a_1 y_1(k) + a_2 y_2(k) = a_1 R[x_1(k)] + a_2 R[x_2(k)]. \tag{5}$$

This result leads to the following definition of a *linear system*. A reward system is linear if and only if,

$$R[a_1 x_1(k) + a_2 x_2(k)] = a_1 R[x_1(k)] + a_2 R[x_2(k)], \tag{6}$$

and,

$$R[0] = 0. \tag{7}$$

Using induction a system with this linearity property can be extended to any linear weighted combination of inputs where a_i are the weights. In general, a *linear* reward system satisfies the following,

$$R[\sum_{i=1}^{M-1} a_i x_i(k)] = \sum_{i=1}^{M-1} a_i y_i(k) = \sum_{i=1}^{M-1} a_i R[x_i(k)], \tag{8}$$

with,

$$R[0] = 0, \tag{9}$$

When equation Eq. (8) holds, that is, the reward system is linear, then splitting the activity between any number of participants provides the same total reward as combining all the activity into one participant. Thus only when the reward system is non-linear is there the potential to differentially reward or penalize concentration of activity. Suppose for example that the reward function of the form

$$y = bx. \tag{10}$$

where *b* is a constant. This is a common type of reward program where the participant receives a fixed percentage of their spending as "*cash back*". This is a linear system. Suppose that the entity wishes to split that activity among two participant identities under its control. The total reward is given by $\overline{y}(k)$ below.

$$\overline{y}(k) = \sum_{i=1}^{2} y_i(k) = \sum_{i=1}^{2} b x_i(k) = b \sum_{i=1}^{2} x_i(k) = b\big(x_1(k) + x_2(k)\big). \tag{11}$$

Suppose an entity's total activity is $10,000 and splits it with $8000 for one and $2000 for the other with *b* equal to 0.03. The individuals rewards are 0.03(8000) = 240 and 0.03(2000) = 60 and the total, 300 is the same as 0.03(10000) = 300. With this type of reward function there is no disincentive to splitting.

Suppose instead that the following nonlinear reward function is used:

$$y = \begin{cases} 0.2(x + (10000x)^{1/2}) & x < 10000 \\ 0.4x & x \geq 10000 \end{cases} \tag{12}$$

The function in Eq. (12) is graphed below. The reward function is nonlinear up to 10,000 in activity and then is linear above 10,000. Any split in activity below 10,000 results in less total reward to the entity. Once the entity's total activity reaches 20,000 it may split into two participants each with 10,000 in activity with no loss in total reward. This function incentivizes a minimum level of activity and hence reputation for a consistent identity before a split. This penalizes cheap participation and rewards concentrated behavior up to a point. Many other similar nonlinear reward functions may be customized to a particular application.

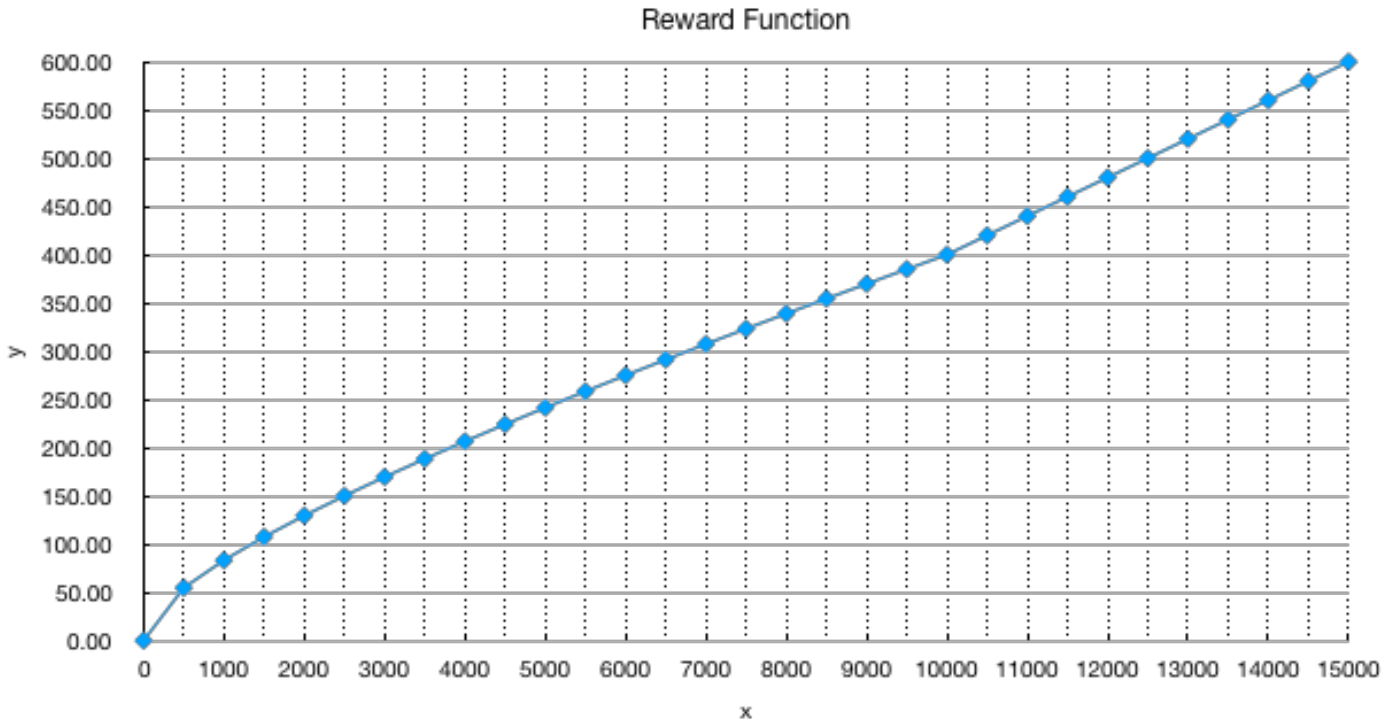

Fig. 9. Nonlinear Reward Function. Nonlinear below 10,000 in activity. Linear above 10,000 in activity.

The former example of a nonlinear reward function was dependent solely on participant activity in terms of purchasing products and services. This could be handled solely with the MoE token. An alternative would be to make the reward function also dependent on the number of SoV token held by a participant. The idea is to incentivize concentrated holding of SoV tokens by increasing the size of the reward in MoE tokens as a function of the number of SoV tokens held. This makes the reward function nonlinear with respect to participant activity in MoE as function of the SoV held. A simple example would be of the form,

$$y = bwx \tag{13}$$

where w is the amount of SoV tokens held, x is the activity in MoE tokens, b is a scaling constant, and y is the reward in MoE tokens. An entity may now split both their store of SoV and their activity across participants. Splitting their store of SoV, however, reduces the reward rate for a given amount of activity. This penalizes splitting.

An example reward system of this type is given below:

$$y = \begin{cases} \left(\frac{0.01}{1000}w\right)x & w < 4000 \\ 0.4x & w \geq 4000 \end{cases}, \tag{14}$$

where w is the amount of SoV tokens held, x is the activity in MoE tokens and y is the reward in MoE tokens. In this case the reward function is nonlinear up until the amount of held SoV reaches 4000 and is linear above that. This rewards concentration of behavior up to a point and penalizes cheap participation. It also drives demand for SoV tokens. The cost of purchasing SoV tokens can be amortized over the expected increase in reward for a given level of participant activity. This allows mechanism design of the total supply of SoV that will be in demand as a function of total activity on the platform. Indeed this is the essence of the third HODLing power. This HODLing power can be further enhanced by making the reward not just a function of the amount of the SoV held but also the length of time that amount of SoV is held. This makes the SoV "sticky".

A more sophisticated approach could combine Eq. (12) and Eq. (14) into one reward system as follows:

$$y = \begin{cases} \min\left(\left(\frac{0.01}{1000}w\right)x, 0.2(x + (10000x)^{1/2})\right) & w < 4000, x < 10000 \\ 0.4x & w \geq 4000, x \geq 10000 \end{cases} \tag{15}$$

Using the HOLDling power of a rewards program based on SoV tokens has the potential to both incentivize good behavior of participants and good pricing behavior of the SoV token.

4.3. Concentrated Influence via Nonlinear Staking and Rewards

The fourth HODLing power is via membership staking. By staking we mean that holders of the SoV token must put some of their SoV tokens at stake in order to join the platform and serve in specific support roles. A stake is like a refundable license fee that enables a participant to engage in a support role and get paid for that support. Like a deposit, the stake ensures good behavior because the participant risks losing its stake should it misbehave. The main difference between this fourth HODLing power and the third is that the types or participation are more involved than merely buying or selling products or services. Staking is used to modulate support and governance type participation on the platform. This includes delegation of stake to other participants as well as running network nodes. Staking is a means to manage participant influence on the platform. Instead of interest, we use the influence or the intensity of influence and the affiliated benefits as the return for putting SoV at stake. We can model this relationship as follows:

$$z(k) = I[w(k)] \tag{16}$$

where z is the intensity of influence on the platform, w is the size of stake, k is the time, and I is the influence system function. The same superposition principle based linear vs. nonlinear relationships apply here as above but to the splitting not of activity but the splitting of stake. Recently the concept of quadratic voting has gained attention as a way of allowing increased intensity of influence in voting as an inverse quadratic function of the size of the stake or cost of a vote [39; 46; 50; 69]. We can represent the quadratic voting function as an influence function as follows:

$$z(k) = I[w(k)] = \left(w(k)\right)^{1/2}, \tag{17}$$

where z is the intensity of influence on the platform, w is the size of stake, k is the time, and I is the influence system function. The idea behind quadratic voting is that entities can exercise greater influence but at a quadratically increasing cost. This changes form one-person-one-vote to one person can have more than one equivalent vote but at a higher and higher cost. The fundamental limiting assumption of quadratic voting, however, is that in general, entities are not allowed to split their participation across multiple pseudonymous identities. Typically the assumption is that an entity's participation is strongly tied to their legal identity. Indeed this typically means is it strongly tied to a natural person. In order to use such a system the platform must trace and enforce participation via strong legal identities. As previously discussed, use of an entity's legal identity, may be problematic from a privacy perspective for online platforms if not cost and complexity. When an entity is allowed to split their stake across multiple participants then quadratic voting has the opposite effect of its intent. Indeed, it strongly incentivizes splitting and has the counter effect of enabling greater influence by an entity for a given available cost or stake. Suppose an entity has some total amount of stake to split among M participants. The total influence of that entity as the sum of the influence of the split participants is as follows:

$$\bar{z}(k) = \sum_{i=1}^{M-1} y_i(k) = \sum_{i=1}^{M} I[w(k)] = \sum_{i=1}^{M-1} \left(w(k)\right)^{1/2}. \tag{18}$$

Consider the following example. Suppose an entity has 50 SoV tokens available to stake in order to influence some governance feature of the platform. If the entity splits their stake into two participants with 25 each their total influence is

$$(25)^{1/2} + (25)^{1/2} = 5 + 5 = 10. \tag{19}$$

If instead the entity does not split, its total influence is,

$$(50)^{1/2} = 7.071. \tag{20}$$

This demonstrates that a bare or naive inverse quadratic influence function actually rewards splitting. Indeed the entity may maximize its total influence by splitting its stake into as many participants as is practical. This means that in order for the platform must enforce a prohibition on splitting via unique legal identity proving to actually realize the intent of quadratic voting.This is a problem when we want to nonlinearly limit the influence of a single entity but foster privacy via consistent pseudonymous participant identities.

One solution would be to add a time component to the influence intensity function. The longer the stake is held by a given participant the higher the influence. Or even the longer any stake has been held by a given participant the higher the influence of all its stake. Thereby an entity is incentivized to add stake built up over time to its oldest participant identities and not split it with new ones.

Another solution is to use interest to balance influence in a staking based influence intensity system. In the case where an entity is engaged on the platform in purchasing products and services, the rewards program can be used to incentivize the concentration of stake into fewer participants. Consequently there would be a cost to an entity to increasing its total influence by splitting its available stake amongst multiple participants. In the case where an entity is not participating in the purchase of products or services, there is no balancing interest to penalize the splitting of its stake to maximize influence. Some other balancing interest(s) would then be required to penalize splitting. The particular type of participation might provide a way to create balancing interest(s). For example, some platforms use decentralized network nodes to provide distributed consensus or validation or observation of transactions. Node selection could be based on influence intensity as a inverse nonlinear function of a stake such as quadratic voting. If an entity wished to exercise influence over network nodes, that entity would have to participate in the staking program. If the number of nodes is restricted or has a minimum value then this forces concentration of stake to a limited number of selectable nodes or to better ensure selection. Should those nodes also receive rewards for their performance activity. Then the size of those rewards could also be a function of the actual stake. The higher the stake the higher the reward. This would incentivize an entity who wishes to exercise greater influence over the platform by hosting multiple

nodes to pay a price in lower total rewards and/or risk losing out in the selection process as a result of splitting its stake across multiple nodes. Thus concentration of stake is required both to be selected as a node and to receive a higher reward. This incentivizes the concentration of stake despite an inverse quadratic influence intensity function. These staking mechanisms provide balancing interests to the influence.

Yet another solution is to make the influence intensity a function of the activity of a participant on the platform. This would explicitly link influence to interest. It would also incentivize node controllers to also purchase products and services on the platform. A type of "eat your own dog food". This provides another positive feedback loop for growth of the platform. As previously described above, when an inverse quadratic function of a quantity such as stake is used to directly determine influence intensity it actually incentivizes splitting. In contradistinction, when an inverse quadratic or other nonlinear increasing function (where the rate of increase is decreasing) of some quantity such as stake is used to determine the rate of influence intensity when multiplied by yet some other quantity then it de-incentivizes splitting. Splitting reduces the rate which when multiplied by some other quantity will always total less across all the splits. So using activity as the other quantity de-incentivizes splitting while still incentivizing in a nonlinearly increasing way the holding of more stake to gain influence in order to control a node. This is subtle distinction and is why using an inverse quadratic function to determine the reward rate de-incentivizes splitting (see section 4.9) but using an inverse quadratic to directly determine a reward or influence does not.

These approaches of balancing influence and interest also work well with delegated stake or activity where a participant who does not have enough stake on its own to be selected as a node can receive delegated stake or delegated activity or both from others. The resultant combination can have higher total influence with higher total rewards but both the rewards and to some extent the influence are distributed across the delegate and delegators. The delegators have limited control over the node but in combination enable an otherwise weakly staked participant to garner enough influence to be selected as a node. The controlling entity must be responsive somewhat to the influence of its delegators lest they switch their votes to a different node. An entity attempting to control multiple nodes must compete with nodes that receive delegated stake. If it splits its stake across multiple nodes it may not have enough stake to win selection of even a single node. If on the other hand the entity splits its stake to join with delegates on multiple nodes it weakens its influence over any given node and depending on the reward distribution function may or may not reduce the total reward it receives.

For example, suppose that any selected node has a principal controlling entity. This entity is the delegate and its node receives the delegated stake for the purpose of selection. Suppose as well that the total reward increases at a nonlinearly decreasing rate as a function of total stake. Suppose further that the delegate only receives a nonlinear reward at the level of its own stake not as a share of the total reward due to the total stake of the delegate and delegators. Whereas the delegators receive a reward as a nonlinear weighted share of the remaining total reward due to the total stake. In this case the delegate risks getting less reward for a given stake even though total reward is higher due to the higher total delegated stake. The delegate is thereby incentivized to personally stake more and may chose to not accept any delegated stake if its own contribution is high enough to win selection. A delegate as principal entity has a lot of control over the node but must share the reward with its delegators. Whereas a delegator has little control over the node to which it delegates its stake but receives a higher reward relative to its delegated stake due to the a higher total delegated stake. If a delegator concentrates its stake on one node its reward may be higher but it may be less likely to pick a winner whereas distributing its stake across multiple nodes may have the opposite effect. This balanced approach incentivizes a high degree of concentrated participation and therefore reputable influence using only economic rewards without requiring the enforcement of legal identity proving. Of course a hybrid system that uses both might be more appropriate for higher value participation.

5. Conclusion

By separating the concerns of medium-of-exchange and store-of-value a dual utility tokenomics model has the potential to fix the broken single utility token model. The store-of-value token is now relatively unconstrained by the demands of stability, low friction and high throughput. This enables the store-of-value token to be designed with beneficial properties that incentivize virtuous participation on the platform that include a side effect of appreciative value. This approach is general and can be beneficially adapted to many utility token applications.

Samuel M. Smith Ph.D. Is the CTO and co-founder of Difuon, a startup that is building a decentralized fog computing platform. He is advisory architect for reputation and AI for ConsenSys. He serves on the technical governance board of Sovrin.org. Samuel received a Ph.D. in Electrical and Computer Engineering from Brigham Young University in 1991. He then spent 10 years at Florida Atlantic University, eventually reaching full professor status. His research specialties include automated reasoning, machine learning, and autonomous vehicle systems. He has over 100 refereed publications in these areas and was principal investigator on numerous federally funded research projects. Dr. Smith has been an active participant in open standards development for networking protocols and is a serial entrepreneur.

References

[1] “A Dual Token Structure Of Utility And Security Tokens-Leveraging The Best Of Both Token Worlds,” *Mint Health*, 2018/03/15 https://www.minthealth.io/a-dual-token-structure-of-utility-and-security-tokens-leveraging-the-best-of-both-token-worlds/

[2] “A Globally Interoperable Blockchain for Identity,” *veres.one*,
veres.one
[3] A. Robespierre, “Asset-Backed Tokens will lead to the first truly valuable Utility Tokens,” *Medium*, 2018/08/06
https://medium.com/@RobespierreBran/asset-backed-tokens-will-lead-to-the-first-truly-valuable-utility-tokens-65156b9defd3
[4] A. Evans, “On Value, Velocity and Monetary Theory,” *BlockChannel*, 2018/01/18
https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f
[5] A. Molé, “Token Up #2: Your Complete Guide to Security Token Exchanges,” *Medium*,
https://blog.neufund.org/token-up-2-your-complete-guide-to-security-token-exchanges-fab49baed8fc
[6] A. Milano, “Quantstamp Under Fire: Buyers Say Faith Shaken In $65 Million Token,” *CoinDesk*, 2018/06/13
https://www.coindesk.com/quantstamp-fire-buyers-say-faith-shaken-65-million-token/
[7] A. Lannquist, “Today’s Crypto Asset Valuation Frameworks,” *BlockChain*, 2018/03/6
https://blockchainatberkeley.blog/todays-crypto-asset-valuation-frameworks-573a38eda27e
[8] B. S. Srinivasan, “Thoughts on Tokens,” *Medium*, 2017/05/27
https://news.earn.com/thoughts-on-tokens-436109aabcbe
[9] B. Bernstein, “Cryptocurrencies are money, not equity,” *Token Economy*, 2018/07/22
https://tokeneconomy.co/cryptocurrencies-are-money-not-equity-30ff8d0491bb
[10] “Buy and Sell Digital Currencies,” *Stronghold*,
https://stronghold.co
[11] C. Long, “ICOs Were 45% Of IPOs In Q2 2018, As Cryptos Disrupt Investment Banks,” *Forbes*,
https://www.forbes.com/sites/caitlinlong/2018/07/22/icos-were-45-of-ipos-in-q2-2018-as-cryptos-disrupt-investment-banks/#64963a2e794c
[12] P. Cathy Barrera, “Tokens: Investment Vehicle or Medium of Exchange (Not Both),” *MIT Crypto Economics Lab*, 2018/07/3
[13] S. P. Choudary, G. G. P. Parker and M. Van Alystne, “Platform scale: How an emerging business model helps startups build large empires with minimum investment,” Platform Thinking Labs, 2015.
[14] C. Burniske, “Cryptoasset Valuations,” *Medium*, 2017/09/24
https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7
[15] C. Catalini and J. S. Gans, “Initial Coin Offerings and the Value of Crypto Tokens,” *SSRN*, vol. MIT Sloan Research Paper No. 5347-18, 2018/03/13
[16] C. Comben, “Have You Ever Wondered What Really Goes into KYC/AML?,” 2018/07/26
https://coincentral.com/kyc-aml/
[17] C. Masters, “EOS Leads in Transaction Volumes Ahead of Competitors,” *Cryptovest*, vol. 2018/08/02,
https://cryptovest.com/news/eos-blows-all-blockchains-out-of-the-water-with-extraordinary-transaction-load/
[18] C. Harper, “In Search of Stability: An Overview of the Budding Stablecoin Ecosystem,” *Bitcoin Magazine*,
https://bitcoinmagazine.com/articles/search-stability-overview-budding-stablecoin-ecosystem/
?utm_campaign=Weekly+Bits+October+9%2C+2018+%5BSponsored+by+BeMyApp%5D+%28PQ7LA2%29&utm_medium=email&_ke=eyJrbF9lbWFpbCI6ICJzYW1AcHJvc2FwaWVuLmNvbSIsICJrbF9jb21wYW55X2lkIjogImpTNDk3RyJ9&utm_source=Bitcoin+Magazine+Newsletter+2.0
[19] D. Floyd, “Tezos Investors Got a Chance to Sell This Week – And They Took It,” *CoinDesk*, 2018/07/18
https://www.coindesk.com/tezos-investors-got-a-chance-to-sell-this-week-and-they-took-it/
[20] D. Patrick, “On Tokenomics and ICO Valuations,” *Medium*, 2018/01/13
https://medium.com/@deanpatrick_63570/on-tokenomics-and-ico-valuations-5312e5bdc2bd
[21] “Decentralized Identifiers (DIDs),” *W3C Draft Community Group Report 23 August 2018*,
https://w3c-ccg.github.io/did-spec/
[22] “Decentralized Identifiers (DIDs),” *blockstack.org*, 2018/11/09
https://docs.blockstack.org/core/naming/did.html
[23] D. Rhodes, “Why are So Many ICOs Failing?,” *CoinCentral*, 2018/04/28
https://coincentral.com/why-are-so-many-icos-failing/
[24] GameKyuubi, “I AM HODLING,” *Bitcoin Forum*, 2013/12/18
https://bitcointalk.org/index.php?topic=375643.0
[25] “Greater fool theory,” *Wikipedia*,
https://en.wikipedia.org/wiki/Greater_fool_theory
[26] “Greater Fool Theory,” *Investopedia*,
https://www.investopedia.com/terms/g/greaterfooltheory.asp
[27] “Havven’s dual-token system solves the problem of volatility in the crypto economy,” *CryptoNinjas*, 2017/12/18
https://www.cryptoninjas.net/2017/12/18/havvens-dual-token-system-solves-problem-volatility-crypto-economy/
[28] “Hodl,” *Wikipedia*,
https://en.wikipedia.org/wiki/Hodl
[29] “How to Identify UBOs: Ultimate Beneficial Owners,” *Trulioo*, 2018/04/24
https://www.trulioo.com/blog/identify-ultimate-beneficial-owners/
[30] “ICO Data Funds Raised,” *ICO Data*,
https://www.icodata.io/stats/2018
[31] “It’s a dump or be dumped on world. How should regulators respond to the nature of the beast?,” *Finder*,
https://www.finder.com.au/boston-college-study-ico-pump-and-dumps-are-the-smart-option
[32] J. Currier, “The Network Effects Manual: 13 Different Network Effects (and counting),” *Medium*, 2018/01/09
https://medium.com/@nfx/the-network-effects-manual-13-different-network-effects-and-counting-a3e07b23017d
[33] J. Currier and N. F. X. Team, “The Networks Effects Bible,” *nfx.com*,
https://www.nfx.com/post/network-effects-bible
[34] J. Clayton, “Statement on Cryptocurrencies and Initial Coin Offerings,” *SEC.gov*,
https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
[35] J. Biggs, “Thousands of cryptocurrency projects are already dead,” *TechCrunch*,
https://techcrunch.com/2018/06/29/thousands-of-cryptocurrency-projects-are-already-dead/
[36] J. Pfeffer, “Doubts about the Long-Term Viability of Utility Cryptoassets,” *Medium*, 2018/04/18
https://medium.com/john-pfeffer/doubts-about-the-long-term-viability-of-utility-cryptoassets-db04350b1f55
[37] “Join us in building an open source decentralized identity ecosystem for people, organizations, apps, and devices.,” *Decentralized Identity Foundation (DIF)*,
http://identity.foundation
[38] K. Sedgwick, “46% of Last Year’s ICOs Have Failed Already,” *bitcoin.com*, 2018/02/23
https://news.bitcoin.com/46-last-years-icos-failed-already/
[39] S. P. Lalley and E. G. Weyl, “Quadratic voting: How mechanism design can radicalize democracy,” vol. AEA Papers and Proceedings 108, pp. 33-37, 2018
[40] Neufund, “If you invest in app tokens, you may be killing the project you fund (1),” *Medium*, 2017/11/07

https://blog.neufund.org/if-you-invest-in-app-tokens-you-may-be-killing-the-project-you-fund-1-6bd15b10f45e
[41] N. I. Tomano, “On Token Value,” *Medium*, 2017/08/06
https://thecontrol.co/on-token-value-e61b10b6175e
[42] N. Maleki, “Blockchain and the Broken Revenue Model: Complexities of Securities Laws and Blockchain,” *Medium*, 2018/06/11
[43] “Open Identity System for the Decentralized Web,” *uport.me*,
https://www.uport.me
[44] G. G. Parker, M. W. Van Alstyne and S. P. Choudary, “Platform Revolution: How Networked Markets Are Transforming the Economyand How to Make Them Work for You,” WW Norton & Company, 2016.
[45] “POA,” *poa.network*,
https://poa.network/governance
[46] E. A. Posner and E. G. Weyl, “Radical Markets: Uprooting Capitalism and Democracy for a Just Society,” Princeton University Press, 2018.
[47] “Price Graphs,”
https://coinmarketcap.com
[48] J. G. Proakis and D. G. Manolakis, “Introduction to Digital Signal Processing. 1988,” Macmillan Publishing Company, pp. 59-62.
[49] “Proof-of-authority,” *Wikipedia*,
https://en.wikipedia.org/wiki/Proof-of-authority
[50] “Quadratic voting,” *Wikipedia*,
https://en.wikipedia.org/wiki/Quadratic_voting
[51] R. R. O’Leary, “Ethereum’s Growing Gas Crisis (And What’s Being Done to Stop It),” *CoinDesk*, 2018/07/06
https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/
[52] R. Rottgen, “In Defense of Utility Tokens,” *HackerNoon*, 2018/02/04
https://hackernoon.com/in-defense-of-utility-tokens-97a35fbb618b
[53] S. M. Smith, “Open Reputation Framework,” vol. Version 1.2, 2015/05/13
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf
[54] S. M. Smith, “Decentralized Autonomic Data (DAD) and the three R’s of Key Management,” Spring 2018
https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/DecentralizedAutonomicData.pdf
[55] S. M. Smith and D. Khovratovich, “Identity System Essentials,” 2016/03/29
[56] “Send and Receive Money,” *Stellar*,
https://www.stellar.org/developers/guides/get-started/transactions.html
[57] S. Conway, A. H., M. Ma *et al.*, “A DID for Everything,” *RWOT Fall 2018*, 2018/09/26
https://github.com/WebOfTrustInfo/rwot7
[58] S. Cicero, “Blockchain Powered Platforms: Tokens,” *Medium*, 2017/10/12
https://stories.platformdesigntoolkit.com/blockchain-powered-platforms-tokens-8363755fdd83
[59] S. Foundation, “Sovrin: Identity For All,”
https://sovrin.org
[60] “Sovrin: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust,” *Sovrin.org*, 2018/01/01
https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf
[61] Stellabelle, “What’s The Backstory On The Word, HODL?,” *Medium*, 2017/04/30
https://medium.com/@stellabelle/whats-the-backstory-on-the-word-hodl-27756392b698
[62] S. Aggarwal, “Understanding Ether vs Gas,” *Medium*, 2017/06/27
https://medium.com/sunnya97/understanding-ether-vs-gas-82ce2f1dc560
[63] “Superposition principle,” *Wikipedia*,
https://en.wikipedia.org/wiki/Superposition_principle
[64] “Sybil attack,” *Wikipedia*,
https://en.wikipedia.org/wiki/Sybil_attack
[65] T. Koffman, “Your Official Guide to the Security Token Ecosystem,” *Medium*, 2018/04/18
https://medium.com/@tatianakoffman/your-official-guide-to-the-security-token-ecosystem-61a805673db7
[66] T. Pearson, “What is a Security Token? A Comprehensive Guide to How They Work and Their Impact,” *HackerNoon*, 2018/10/18
https://hackernoon.com/what-is-a-security-token-a-comprehensive-guide-to-how-they-work-and-their-impact-ef429a77a9c3
[67] “VeChain Mainnet Launches,” *CCN*, 2018/06/30
https://www.ccn.com/vechain-thor-blockchain-launches-token-swap-to-take-place-mid-july/
[68] V. Buterin, “On Medium-of-Exchange Token Valuations,” *Vitalik*, 2017/10/17
https://vitalik.ca/general/2017/10/17/moe.html
[69] V. Buterin and G. Weyl, “Liberation Through Radical Decentralization,” *Medium Cryptocurrency*, 2018/05/21
https://medium.com/@VitalikButerin/liberation-through-radical-decentralization-22fc4bedc2ac
[70] “Why Most ICO’s Will Fail: A Cold Hard Truth,” *BlockGeeks*,
https://blockgeeks.com/guides/why-most-icos-will-fail/
[71] W. Hinman, “Digital Asset Transactions: When Howey Met Gary (Plastic),” *SEC.gov*, 2018/06/14
https://www.sec.gov/news/speech/speech-hinman-061418
[72] W. Mougayar, “Tokenomics – A Business Guide to Token Usage, Utility and Value,” *StartupManagement*, 2017/06/10
http://startupmanagement.org/2017/06/10/tokenomics-a-business-guide-to-token-usage-utility-and-value/