.

MADTOKEN ECONOMIC SPECIFICATION

MICHAEL ZARGHAM, N.D. JEBESSA, AND TOM BOLLICH

Abstract. The MAD Network is a suite of decentralized applications serving the advertising technology ecosystem. The application of blockchain and smart contract technologies holds great promise in terms transparency and efficiencies, yet adapting new technologies to transform existing ecosystems does not come without challenges. When innovating, iterative research bridging from theory to simulation to implementation is required to ensure success. This technical whitepaper focuses on formal definitions, providing context and justification for the MAD token and defines a preliminary path to launching and maintaining a healthy economic system. This material represents ongoing work and is therefore subject to evolve as we learn from our research.

M. Zargham, CEO BlockScience; N.D Jebessa, Researcher Madhive and T. Bollich, CTO Madhive.

1. Introduction

1.1. **Motivation.** The MAD Network is comprised of three distinct blockchain layers: MADnet Books, MADnet Core and MADnet Data. The MADtoken is an ERC-20 equivalent token, available on public markets but whose primary function is as a software license, providing access to the MAD Network applications. Specifically, MAD Token will be escrowed to activate a payment channel for the accounting, fulfillment and instant reconciliation of ad delivery. Advertisers and publishers will have the option to exchange on credit or settle in real time with currency of their choice; in early phases of adoption, it is expected that Advertisers will fulfill their commitments in fiat. Ultimately publishers have the final say in how they would like to be paid and the MAD Network will streamline that exchange of value. The focus of this document is the relationship between the publicly traded MAD Token and the private payment rail service MADnet Books. The MADnet Books is a private chain maintained by the AdLedger Consortium, designed to track high-frequency network transactions, expose price manipulation and facilitate accurate reconciliation, [1].

1.2. **Tools and Technology.** This solutions proposed are based on the principles of Nakamoto Consensus first defined in [2] for a general ledger and later refined for use to maintain the state of a virtual machine in [3, 4]. While a large number of options are available for blockchain frameworks this document remains agnostic to this choice, though as is standard in the blockchain field, consistency is assumed to take precedence over availability as it pertains to partition tolerance as defined in Brewer's CAP Theorem, [5, 6].

Broadly speaking this document focuses on the economic system that sits atop a suitably designed protocol layer; the mechanisms discussed are influenced by the study of game theory, [7]; both cooperative [8, 9, 10] and non-cooperative [11, 12] are considered with a focus on stability around desirable economic equilibria [13, 14] using mathematical tools from control systems engineering, [15, 16].

2. Definitions and Notation

2.1. **Overview.** This section provides definitions of terms and variables as well as an event centric overview of MAD and the additional book-keeping tokens which exist within the closed MADnet Books system. Per the MAD Network white paper, [1], the use case under consideration is an Advertiser or their broker agent escrows MAD Token enabling a commitment to spend fiat on advertising within the MAD Network. The MAD Network software executes that ad spend, precisely tracking the distribution of the Insertion Order specific funds using the non-fungible MAD Cred token. Publishers, miners, and data or service providers coming into possession of MAD Cred, redeem that credit for fiat with the Advertiser that issued the Insertion order; the time frame for this claim is dictated by the net terms of the insertion order contract. Good actors who fulfill their commitments are rewarded with MAD Bonus.

2.2. **Advertising Definitions.** In this subsection, precise definitions of terms and notation for the associated terms is outlined. While ad-tech term definitions may very, the

MAD Network uses this set of definitions as core building blocks for the purpose of formal economic systems engineering.

Definition 1. *An **Advertiser** is a business entity making a financial commitment in order to have advertisements served which verifiably meet a set of campaign specifications.*

In this document the set of all advertisers operating in the MAD Network ecosystem is denoted $\mathcal{S}_A$ and a particular advertiser will be denoted $A \in \mathcal{S}_A$. Initially, the financial commitment is expected to be denominated in fiat but the MAD Network is architected to support payments denominated in any currency, including crypto-currency, which is explicitly identified in the financial commitment portion of the insertion order.

Definition 2. *An **Insertion Order** also referred to as an **IO** is a commitment by an Advertiser to make to pay for advertisements served meeting a set of specifications that characterize a particular advertising campaign. The IO is comprised of the fiat denominated value of the commitment, the net terms of that commitment, and a reference to the campaign specifications.*

The set of all insertion orders is denoted $\mathcal{S}_o$ and any particular insertion order has a unique identifier $o \in \mathcal{S}_o$. Every Insertion order can be uniquely mapped back to the Advertiser making the commitment, denote A_o and the financial commitment associated with that Insertion order f_o, unless otherwise indicated, f_o is denominated in fiat. Furthermore, each IO refers to a unique campaign. The net terms of the Insertion order are denoted ΔT_o and refer to the time window reserved by the advertiser over which to make good on payment associated with commitments made under an Insertion Order.

Further note that the Insertion Order refers to a legally binding contract in the real world and while there will be a smart contact associated with that legal contract, discussion of smart contracts is reserved for the following section.

Definition 3. *A **Campaign** is defined by its campaign specification, a set of rules provided by an advertiser which determines whether a particular Ad Opportunity is acceptable and would merit payment per the Insertion Order commitment.*

Note that while the campaign is uniquely defined by a particular Insertion Order, the *Campaign Specification* may vary in time if the advertiser who made the Insertion Order commitment chooses to do so. The rules provided by an Advertiser are stored in the campaign management application; some limitations to changes allowed under the insertion order legal contract may apply. For example, the Advertiser may not retroactively change the rules such that a formerly valid ad served is deemed out of spec after the fact.

Definition 4. *An **Ad Opportunity** is a specific instance of inventory provided by a publisher which may or may not be an acceptable match for any particular campaign per the campaign specification.*

Since this ruleset is used to determine a truth value it is defined as a function:

$$h_o : \mathcal{S}_a \to \{0, 1\} \tag{1}$$

where $\mathcal{S}_a$ is the set of all Ad Opportunities and any particular Ad Opportunity can be denoted $a \in \mathcal{S}_a$ and the subscript o refers to any campaign $a \in \mathcal{S}_a$. The set $\{0, 1\}$ represents a Boolean value where $0 = False$ and $1 = True$. An Ad opportunity, a is a candidate match for a particular campaign, denoted by its Insertion Order $o \in \mathcal{S}_o$, if and only if $h_o(a) = 1$.

This ruleset denotes any and all criteria used to determine acceptability of an ad opportunity including but not limited to CPMs, flights, dayparts, audience targeting criteria, frequency caps and pacing rules.

Definition 5. *A **Publisher** is a business entity wishing to be paid to serve advertisements which verifiably meet a set of inventory specifications where those specifications are defined on a per ad request basis.*

In this document the set of all publishers operating in the MAD Network ecosystem is denoted $\mathcal{S}_P$ and a particular advertiser will be denoted $P \in \mathcal{S}_P$. Any particular ad opportunity available to an advertiser is an ad request coming from a publisher; thus ad requests are also denoted $a \in \mathcal{S}_a$. Any particular ad request a has an associated publisher a_P which is precisely the entity making the Ad Request and will claim payment for delivering the ad in accordance with the net terms.

Definition 6. *An **Ad Request** being a specific instance of inventory, is further characterized by an inventory specification. The inventory specification is a ruleset which defines whether a particular campaign, denoted by its insertion order, is acceptable to the Publisher making the Ad Request.*

The rule set for the Ad Request is denoted by a function:

$$g_a : \mathcal{S}_o \to \{0, 1\} \tag{2}$$

where $\mathcal{S}_o$ is the set of all Insertion Orders and any particular campaign can be referenced by its Insertion Order $o \in \mathcal{S}_o$ and the subscript a refers to any Ad Request $a \in \mathcal{S}_a$. The set $\{0, 1\}$ represents a Boolean value where $0 = False$ and $1 = True$. A campaign referenced by o is a candidate match for a particular Ad Request $a \in \mathcal{S}_a$, if and only if $g_a(o) = 1$.

Definition 7. *A **Match** is an instance of inventory that for a given Campaign, defined by its Insertion Order and a given Ad Request, the advertisement matches both the campaign specification and the inventory specification.*

The notion of a match must be formally defined as it in the fact the very purpose of the advertising ecosystem to identify and execute matches. The formal characterization of a match is a pairing (a, o) where $a \in \mathcal{S}_a$ and $o \in \mathcal{S}_o$ such that

$$(h_o(a) = 1) \wedge (g_a(o) = 1) \tag{3}$$

guaranteeing that the Ad opportunity a is a candidate match for the campaign associated with Insertion Order o *and* conversely the campaign referenced by o is a candidate match for Ad Request a. Again, note that Ad Opportunities and Ad Requests refer to the same events but the naming convention is used to clarify perspective. A Publisher makes an Ad Request and that request from the perspective of an Advertiser is an opportunity.

Definition 8. *A **Data Provider** is a business entity wishing to be paid to provide data used to identify or verify a valid match.*

The set of all Data Providers in the MAD network ecosystem is $\mathcal{S}_D$ and a particular data provider is denoted $D \in \mathcal{S}_D$; a data provider must materially contribute to the identification or verification of some subset of either the rules within campaign specification $h_o(a)$ or the rules within the inventory specification $g_a(o)$. In the event that such a contribution occurs, the Data provider will be entitled to a share of the fee for serving that ad in accordance with a data provider agreement. For now it suffices to reserve a share γ of ad spend for data providers, defined networkwide.

2.3. **Crypto-Economic Definitions.** In this subsection, precise definitions of crypto-economic terms and notation for the associated terms is outlined. These definitions make reference to the Advertising ecosystem definitions provided in the previous subsection.

Definition 9. *An **IO Smart Contract** is a program running on a public blockchain network through which an Advertiser, or a Broker acting on behalf of an Advertiser, may escrow a quantity of MAD token and use the MAD Network software to service a specific Insertion Order contract.*

The IO Smart Contract is a digital representation of a real world legally binding contract $o \in \mathcal{S}_o$, which asserts that an Advertiser commits to pay a total ad spend f_o for the delivery of a campaign with campaign specification $h_o(\cdot)$, and net terms ΔT_o.

Definition 10. ***MAD Token** also referred to as simply **MAD** is an access token serving the role of a software license associated with the MAD Network suite of ad-tech software services.*

MAD token is an ERC-20 equivalent token made available on a public blockchain for use as a license to access the MAD Network Software. In order to activate the IO Smart Contract for an insertion order $o \in \mathcal{S}_o$, associated with a financial commitment f, the Advertiser or a Broker acting on the Advertiser's behalf escrows a quantity m of MAD token in accordance with the license function:

$$m = L(f, b, F, M, X) \tag{4}$$

where b denotes a quantity of MAD Bonus, a reward token to be defined further below; M denotes all MAD Token escrowed in all active IO Smart Contracts networkwide

$$M = \sum_{o \in \mathcal{O}} m_o \tag{5}$$

where the set $\mathcal{O} \subseteq \mathcal{S}_o$ is the subset of Insertion Orders that is currently active; an Insertion Order is no longer active once payment is completed. The quantity F denotes all fiat commitments in active insertion orders networkwide

$$F = \sum_{o \in \mathcal{O}} f_o \tag{6}$$

and X is a placeholder variable for any other facts that may be chosen as inputs to the license function.

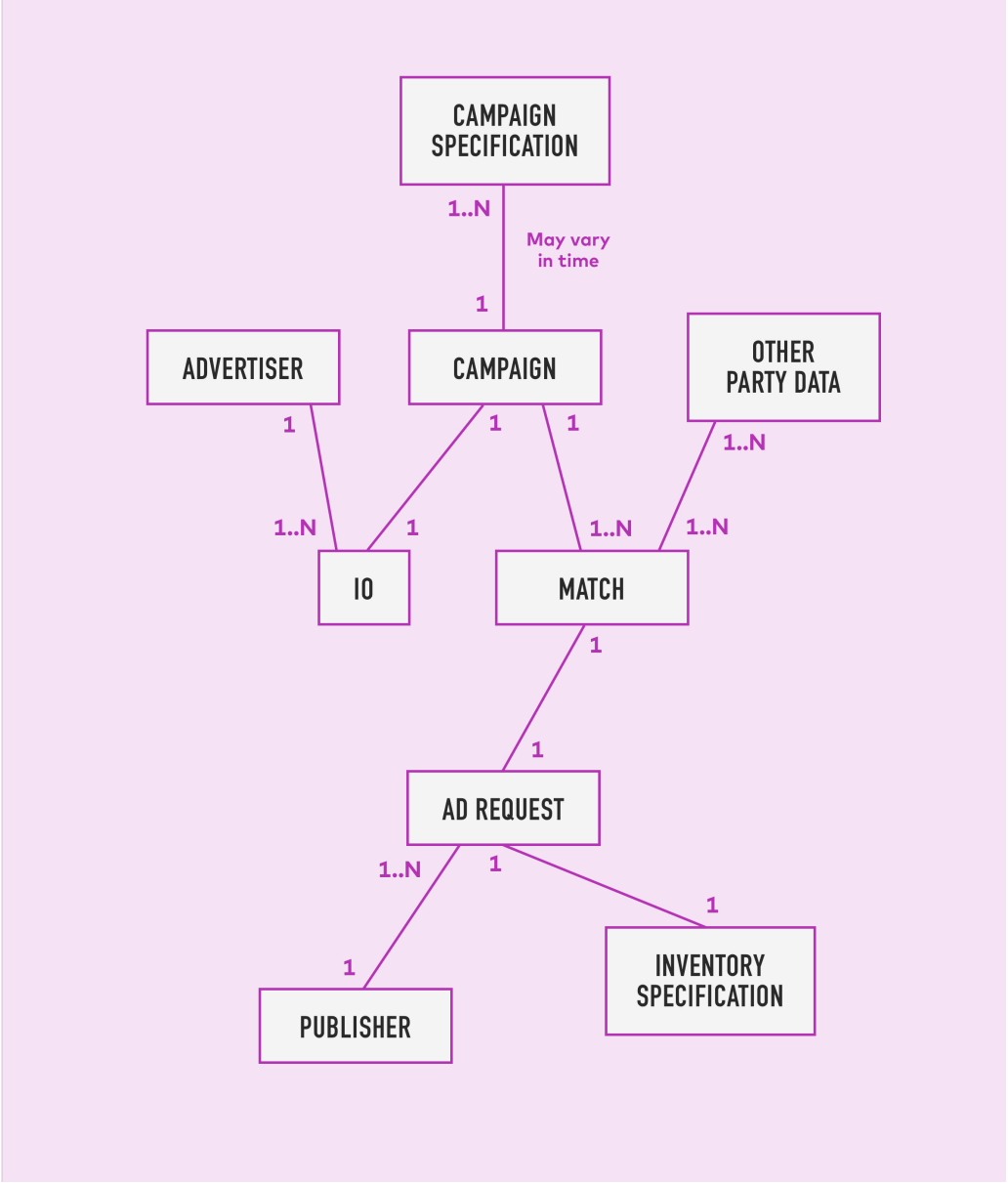

FIGURE 1. A map of the relationships between the advertising concepts defined throughout Section 2.2. The notation 1 and N on the links denotes relationships: one to one as $1-to-1$, many to one as $1-to-N$ and many to many as $N-to-N$.

Definition 11. *An **IO Shadow Contract** is a program running on a consortium blockchain which becomes activated as a result of escrowing the appropriate quantity of MAD token in an IO Smart Contract on the public blockchain; the IO Shadow Contract is a smart contract containing the private functionality of an Insertion Order in the MAD Network software.*

From a users prospective the IO Smart Contract and the IO Shadow Contract are not distinguishable; collectively they encode the Insertion Order contract and allow it to be executed. The differentiation is presented here as it directly relates to the implementation. The IO Smart Contract and the IO Shadow Contract create a bridge between the public functionality of the public ERC-20 equivalent MAD token and the MAD Network software remains private to the consortium. In order to participate in the MAD Network software ecosystem it is necessary to be a verified member of the AdLedger Consortium. This community is self governing and determines rights and responsibilities of its membership.

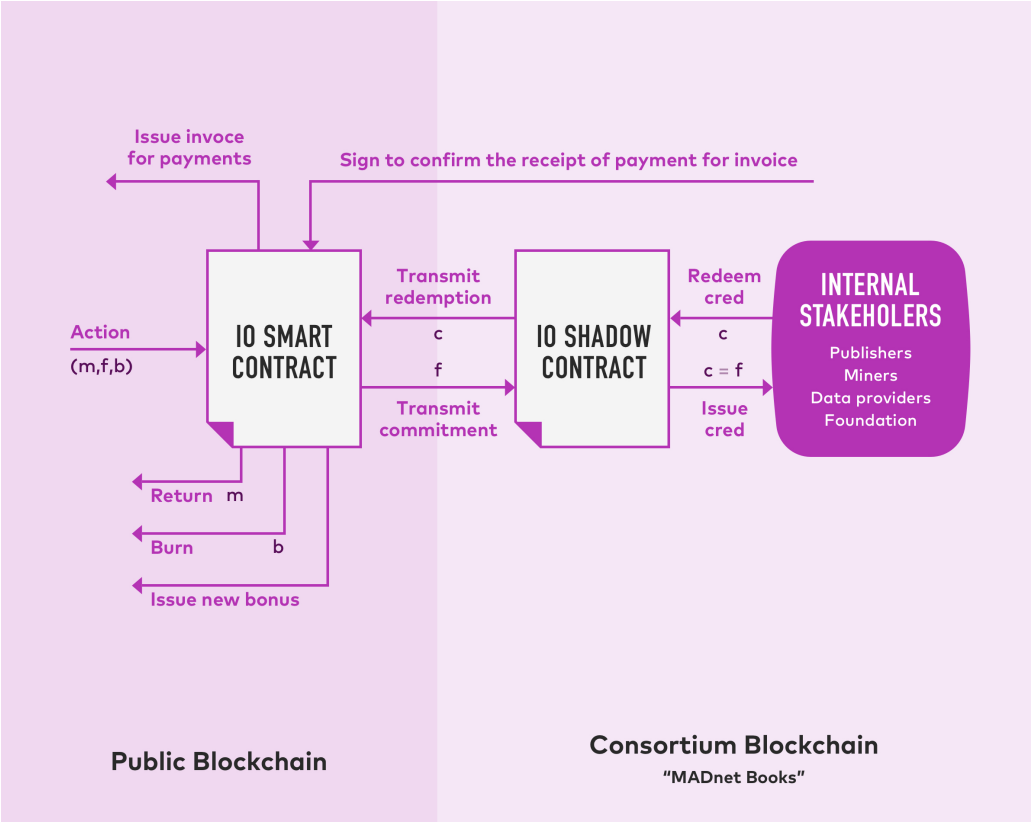

FIGURE 2. Map of the bridge between the IO Smart Contract on the public blockchain and the IO Shadow Contract on the consortium blockchain as described in Section 2.3.

Definition 12. ***MAD Cred*** *also referred to as simply* ***Cred*** *is a non-fungible fiat denominated token internal to the MAD Network eco-system which is issued and tracked inside of a consortium blockchain as a result of an IO Smart Contract being activated with MAD token.*

The MAD Cred is an ERC-721 equivalent non-fungible token with an explicit reference to the Insertion Order contract that it tracks. The total amount of Cred issued is precisely f_o for Insertion Order $o \in \mathcal{S}_o$. A share γ is reserved for payment to data providers

$$c_o^{(data)} = \gamma \cdot f_o, \tag{7}$$

a share ρ is reserved as payment for the miners in the consortium network

$$c_o^{(miners)}) = \rho \cdot f_o, \tag{8}$$

and a share θ is reserved for the foundation maintaining the MAD network software

$$c_o^{(foundation}) = \theta \cdot f_o. \tag{9}$$

It immediately holds by linearity that the total revenues for Data Providers, Miners and the governing Foundation are directly proportional to the total ad spend locked over the lifetime of MAD Network:

$$C^{(data)} = \gamma \cdot \sum_{o \in \mathcal{S}_o} f_o \tag{10}$$

$$C^{(miners)} = \rho \cdot \sum_{o \in \mathcal{S}_o} f_o \tag{11}$$

$$C^{(foundation)} = \theta \cdot \sum_{o \in \mathcal{S}_o} f_o \tag{12}$$

respectively indicating the networkwide revenues generated.

Property 1. *The MAD Network Efficiency ϕ is given by*

$$\phi = \frac{C^{(publishers)}}{C^{(total)}} \tag{13}$$

$$= \frac{C^{(total)} - \left(C^{(data)} + C^{(miners)} + C^{(foundation)}\right)}{\sum_{o \in \mathcal{S}_o} f_o} \tag{14}$$

$$= 1 - (\gamma + \rho + \theta) \tag{15}$$

where we define, without loss of generality, the total MAD Cred issued to date at any time:

$$C^{(total)} = \sum_{o \in \mathcal{S}_o} f_o \tag{16}$$

equal to the total the ad spend by all Advertisers and $C^{(publishers)}$ is the amount of MAD Cred that is paid to Publishers.

The efficiency parameter is critical for understanding the value proposition of the MAD Network and given that the MAD token is an access token serving as a software license for the MAD Network the value of the MAD Token itself will depend on ϕ. The role of the MAD Network efficiency will be further discussed in the following section.

Definition 13. ***MAD Cred Redemption*** *also referred to as simply* ***Redemption*** *is an event whereby a stakeholder returns MAD Cred associated with a specific Insertion Order to its IO Shadow Contract in order to claim payment for the services rendered. The IO Shadow Contract writes a transaction to the associated IO Smart Contract indicating the claim.*

The Redemption event is the first part of the process by which a Publisher, Data Provider, Miner or other stakeholder claims fiat in payment for their contribution to the eco-system. This step is part of the MADnet books and ensures the traceability of funds back to stakeholders who had an explicit role in serving of advertisements within the campaign associated with a particular Insertion Order. At this stage the Advertiser has ΔT_o in accordance with the net terms to provide payment to the redeemer.

When the MAD Cred is returned to the Shadow Contract it is burned, the record of the redemption event includes both the quantity of MAD Cred returned and the account that returned it. The quantity of Cred returned is denoted $c_o^{(redeemed)}$ where *redeemed* is a reference to the redemption transaction and thus to the account of the stakeholder who returned the Cred; the *redeemer* may be any member of the AdLedger consortium, regardless of role or roles.

Definition 14. ***Payment Confirmation*** *also referred to as simply* ***Confirmation*** *is an event whereby a stakeholder signs a transaction to an IO Smart Contract as a confirmation of payment conferred dictated by the MAD Cred returned to the IO Shadow Contract during a Redemption event. When the entirety off the commitment has been confirmed as paid, the IO Smart Contract is considered complete and rendered inactive.*

In order to insure all parties are adequately incentivized the IO Smart Contract does not release escrowed MAD token or provide MAD bonus reward tokens until the Payment Confirmation transactions are signed. Consider an event where a *redeemer* returns $c_o^{(redeemed)}$ to the IO Shadow Contract $o \in \mathcal{O}$, the Advertiser o_A remits payment equal to $c_o^{(redeemed)}$ to the *redeemer*, who then signs the Confirmation transaction with the same account and the IO Smart contract returns a quantity

$$m_o^{(returned)} = m_o \cdot \frac{c_o^{(redeemed)}}{f_o} \tag{17}$$

to the account which originally activated the IO Smart Contract by escrowing m_o MAD token to support the financial commitment f_o. Observe that once all Cred is redeemed and payment is confirmed, all of the escrowed MAD has been released back to the account that originally escrowed it. The expected period over which the MAD token will remain escrowed is the period of the net terms ΔT_o.

Definition 15. ***MAD Bonus*** *also referred to as simply* ***Bonus*** *is a a non-fungible, non-transferable reward token on the public blockchain; MAD bonus*

As an additional incentive to continue to participate in the MAD-Network Ecosystem, the Payment confirmation event also results in the issuance of MAD Bonus. While the MAD Bonus resides on the public blockchain it is not an ERC-20 equivalent token; the MAD Bonus intentionally has extremely limited functionality when it comes to transfers. It is always issued to precisely the account which originally escrowed MAD token in order to activate an Insertion Order Smart Contract.

The MAD Bonus is for successfully completing all payments associated with an Insertion Order and is provided when the IO Smart Contract is considered complete and rendered inactive. This may occur in one of two cases, a) the entire commitment is confirmed as paid or the b) the Insertion Order contract is terminated and all unclaimed MAD Cred is Burned and all claimed Cred has been redeemed at payment is confirmed.

In the latter case the total commitment is updated to reflect the original commitment less the unclaimed Cred: $f_o \leftarrow f_o^+$ where $f_o^+ = f_o - c_o^{(unclaimed)}$. Accounting for completion of Insertion Orders, while it remains that $o \in \mathcal{S}_o$, completion indicates that $o \notin \mathcal{O}$, the set of active IOs.

The quantity $b_o^{(issued)}$ of MAD Bonus that is generated when the Insertion Order Smart Contract is completed is given by

$$b_o^{(issued)} = \eta \cdot f_o \tag{18}$$

where $\eta > 0$ is a networkwide parameter chosen by the foundation governing the MAD Network software and economic eco-system.

The only use for MAD Bonus is to apply it to a future Insertion Order Smart Contract initiated by the same account and its effect is determined by the function $L(f, b, F, M, X)$. Note that when the Insertion Order Smart Contract is completely repaid, rather than being returned, all MAD Bonus escrowed it burned. Although sent to the same account, the newly created MAD Bonus is distinct from the MAD Bonus that was burned because it is a non-fungible token with an explicit reference to the IO Smart Contract that was successfully completed to create it. In the event that the consortium needs to impose punishment on a bad actor within the system, one mode of reprisal would be to render a specific batch of MAD Bonus invalid by blacklisting all MAD Bonus with reference back to a specific Insertion Order Smart Contract; such an action would be at the sole discretion of the consortium community.

3. Mad Token Economics

MAD Network is an eco-system of software, community and economic incentives. The MAD token plays a critical role in that eco-system as software license and as such its value is fundamentally driven by the utility of that software. The best way to understand tokens which provide access to software services is to think of them as decentralizing the Software as a Service (SaaS) business model. It is a common misconception to conflate the role of a utility with the role of payment for services within a piece of software. Under that model,

the token would simply be domain specific money and it would hard to make claims about its utility other than by analogy to money.

In the case of MAD token the utility is defined by analogy to property and it is the MAD token license function that allows the design of the IO Smart Contract to behave like property. Before getting into the economic analysis of the MAD token, let us first review the goals of the economic system instantiated by the MAD token and its role as license to access the MAD Network software.

3.1. **Business Requirements.** The MAD Token is a continuously valued software license with level of service defined by the successful throughput of financial commitments made and paid; the value of the token which is dictated by the utility of the software service itself to the community served as defined by improving the efficiency of the ad serving stack. The efficiency of the ad serving stack is defined as the share of ad spend which makes it to the publishers, with the caveat that all payments to parties other than the publishers are tied to a service that explicitly adds value to the process, i.e. Data Providers contributing audience targeting attributes for an ad that was actually served. Further considerations for data markets are discussed in [17, 18]

Requirement 1. *Users of the MAD Network access that software by escrowing MAD, and the impact of volatility in the crypto markets on the ability of a user to access the software is minimal; speculation does not hinder use.*

Requirement 2. *Since MAD is returned as payment commitments are fulfilled, the license is perpetual and the amount of MAD token held determines the level of service, which is measured in total outstanding commitments that a user may have at one time.*

Requirement 3. *There exists a value estimate of the MAD token that can be inferred from the usage of the MAD Network software, and that inferred value is directly related to increasing usage of the MAD Network Software.*

Requirement 4. *Holders of MAD token improve their financial position by using their MAD token to access the software on their own behalf or by serving as brokers escrowing it on behalf of Advertisers using the MAD Network Applications*

Requirement 5. *Advertisers or their Brokers engaging with the IO Smart Contracts are incentivized to maintain a consistent identity both by requiring membership in the AdLedger and by rewarding accounts associated with completed Insertion Orders the MAD Bonus reward token which cannot be moved between accounts.*

Additionally, the effort to build an ad tech ecosystem introduces explicit evaluations of fairness. The formal notional of fairness is defined in [19] and [20]. Extensive discussions of fairness in the context of engineered systems can be found in [21, 22, 23].

3.2. **Financial Commitments and Bonus.** This economic system is characterized by the design of the license function $L(f, b, F, M, X)$ first defined in equation (4). The MAD Network team understands that this is the critical function in defining the incentives around the MAD token. The material presented is a candidate design currently being researched;

this research begins with formal mathematical assertions, is followed by economic simulations, an agent based network emulation and eventually implementation. Below formal mathematical assertions are provided in accordance with the requirements listed above.

Suppose the License function is defined as

$$L(f, b, F, M, X) = (f - b) \cdot R(F, M, X) \tag{19}$$

recalling that f is the financial commitment, b is the MAD Bonus staked which is restricted to $b \leq \alpha f$; F and M are network state variables defined in equations (6) and (5), respectively. In this case, the role of variables F, M, and X are abstracted by the function $R(\cdot)$. Define the parameter α such that $0 \leq \alpha < 1$ to be controlled by the governors of the software in order to tune the behavior of the network.

Property 2. *The MAD Bonus is denominated in the same units as the financial commitment f and committing the maximum $b = \alpha f$, allows the user to execute an IO with fiat commitment f while only escrowing a smaller amount of MAD token that would be associated with*

$$\tilde{f} = (1 - \alpha) f \tag{20}$$

concluded by observing that

$$L(\tilde{f}, 0, F, M, X) = L(f, \alpha f, F, M, X) \tag{21}$$

for any function $R(F, M, X)$ and values of F, M, and X.

This property characterizes the effect of committing MAD Bonus when initiating an IO Smart Contract. The MAD Bonus serves to help ensure early adopters benefit from remaining users of the MAD Network software once they have made good on their commitments by allowing them introduce more ad spend even with the same amount of tokens under the same network conditions.

Note that this construction ensures that both MAD Cred and MAD Bonus are functionally pegged to the units of of the financial commitments in the IOs that created them. In some ways these tokens are akin to asset backed stable coins but differ from systems such as those found in [24, 25] in that these tokens are non-fungible and contain explicit references to the specific events that resulted in their issuance. In this regard the MAD network tokens simply account for the value promised in the IO and do not hold any promise outside the fulfillment of that financial commitment insulting it from the broader volatility in the open crypto-markets which poses fundamental challenges to stable value tokens that live outside of a consortium environment.

3.3. **Initial Implementation.** In the earliest implementation of the MAD Network software the market price, $p_t^{(MAD)}$ has been determined explicitly as $p_0^{(MAD)} = 0.25$ USD. Before the volatility of the open market takes hold, it suffices to define

$$L(f, b, F, M, X) = \frac{(f - b)}{p_0^{(MAD)}} \tag{22}$$

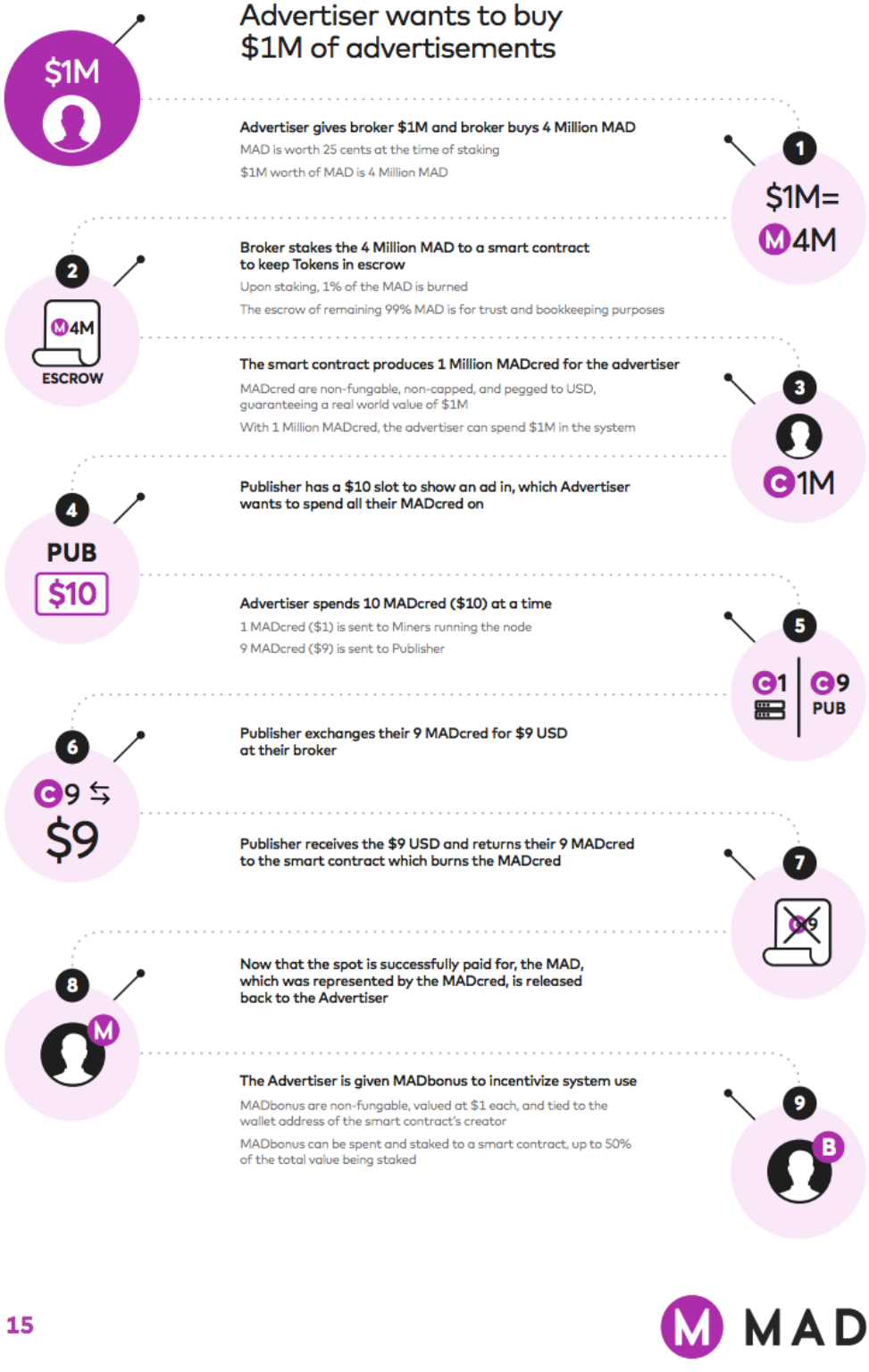

FIGURE 3. Walk through of the Mad Network Workflow from page 15 in the MAD Network whitepaper [1], demonstrating the most basic case of Insertion Order being executed.

corresponding to selecting $R(F, M, X) = 1/p_0^{(MAD)}$ and observing that this is a well defined choice, precisely because the function $R(\cdot)$, by its construction in equation (19), defines a conversion rate from USD to MAD.

The formulation in (22) is precisely the formulation described in the MAD Network whitepaper and other early media; due to the role of $R(\cdot)$ as a currency conversion it is by far the most intuitive formulation and it will be used as long as is suitable. In this case, $X = p_t^{(MAD)}$ is additional information which will need to be supplied via an oracle observing external data sources once the MAD token is being actively traded on exchanges. The simplicity helps guard against edge cases that may arise in the early days of the network under feedback based mechanisms. The walkthrough of the MAD network use case under this rule is provided in Figure 3. Alternatives are considered in order to ensure Requirement 1 is met in the medium and long term.

3.4. **Introducing Feedback.** Up to challenges around confirmation times, the blockchain is an incredibly powerful technology in a systems engineering sense because it provides direct observability of the entire network state. Furthermore, smart contracts can reference information on the blockchain when computing the code making up a smart contract. This renders the system controllable to a limit degree; controllability along with observability open the door to the use of tools from the systems engineering discipline. For further inquiry into this field, see [26, 27, 28, 29].

The application of feedback control to economic networks developed with blockchains and smart contracts is an area of ongoing research because complex computation still requires outsourcing to off-chain oracles even if off-chain data is not required to do the computation; in the event that off-chain data is required, an oracle is always required. In the event that the MAD Network software implementation relies on oracles for complex calculations, the team is considering the use of validation games per the research, [30].

Setting aside potential challenges, assume that it is possible to compute F and M, respectively defined in equations (6) and (5) and let us further define the networkwide total MAD Bonus locked in active IO Smart Contracts,

$$B = \sum_{o \in \mathcal{O}} b_o \tag{23}$$

where b_o is the amount of MAD Bonus locked in IO Smart Contract o. Define the the *Network License* version of the license function $L(\cdot)$ as

$$L(f, b, F, M, B) = (f - b) \cdot \frac{M}{F - B}, \tag{24}$$

using the same form as equations (19) and (22) but selecting $X = B$. Equation (24) is a special case of the *Discount Token* model presented in [31] where the level of service variable is $f - b$ and the user is always able and required to take a 100% discount, meaning that the software is always accessed by escrowing tokens. This special case will be referred to as an *Access Token*. In the discount token model, a parameter is used to ensure operational revenue is generate in this process; no such parameter is required in this construction

because the operational expenses are accounted for in the consortium network as defined in equation (12).

Property 3. *For a valid choice of f and $b \leq \alpha f$, given that a user possesses sufficient MAD Token to escrow*

$$m = (f - b) \cdot \frac{M}{F - B} \tag{25}$$

the users required commitment of MAD token to the MAD Network will be proportional to the share of use at the time the Insertion Order Smart Contract was initiated

$$\frac{m}{f - b} = \frac{M}{F - B}. \tag{26}$$

Furthermore, under the simplifying assumption that the most recent event of an Insertion Order Smart Contract initiated or completed is confirmed on the public blockchain before the next Insertion Order Smart Contract activation transaction is submitted, Property 3 is shown to be an invariant.

Suppose the current state of the network at block k is given by M_k, F_k and B_k and an Insertion Order Smart Contract with valid tuple (f, b, m) is confirmed, then the new state is given by

$$F_{k+1} = F_k + f \tag{27}$$

$$B_{k+1} = B_k + b \tag{28}$$

$$M_{k+1} = M_k + (f - b) \cdot \frac{M_k}{F_k - B_k} \tag{29}$$

and a simple coordinate transformation $g = f - b$, $G_k = F_k - B_k$ allows us to reduce to two dimensions

$$G_{k+1} = G_k + g \tag{30}$$

$$M_{k+1} = M_k + g \cdot \frac{M_k}{G_k}. \tag{31}$$

Observe that by factoring out M_k/G_k in equation (31), the expression can be algebraically manipulated

$$M_{k+1} = \frac{M_k}{G_k} (G_k + g) \tag{32}$$

$$\frac{M_{k+1}}{G_{k+1}} = \frac{M_k}{G_k} \tag{33}$$

$$\frac{M_{k+1}}{F_{k+1} - B_{k+1}} = \frac{M_k}{F_k - B_k} \tag{34}$$

ultimately recovering the desired invariant at block $k + 1$, provided it held at block k. Since our argument had no sign restrictions on the variables m, b and f, an identical argument holds ensuring the invariant when Insertion Order Smart Contracts are completed if mechanism for unlocking MAD token defined in equation (17) were modified to release

all MAD token from an IO Smart Contract only when it is completed. There are other reasons this alternative may be considered, the most notable is incentivizing Advertisers to agree to shorter net terms and complete payments promptly to unlock and reuse their MAD, which will generally increase the flow of money through the ecosystem.

3.5. **MAD Token Utility.** Per the requirements in Section 3.1, the MAD Token is best valued as property with similar financial accounting to the value of a taxi medallion. In order to substantiate this claim, it is necessary to derive a meaningful characterization of the tokens financial value accrued via use. To do so a comparison is made between the efficiency of the MAD Network defined as ϕ in equation (15) and the efficiency of the existing ad-tech stack defined as ϕ_0 which is known to be as low as 30 to 40% depending on which treatment of the *disappearing adtech dollar* concept one reads. Through the choices of γ, ρ and θ, the MAD Network is targeting $\phi = 0.65$ which amounts to an approximate 2x lift. For the sake of this analysis the variables ϕ and ϕ_0 will be used under the assumption that a lift

$$\beta = \frac{\phi}{\phi_0} > 1 \tag{35}$$

is achieved on average over an extended period of time. The following analysis characterizes the value of MAD token per unit of service defined by the financial commitment f. For the sake of this analysis, the quantity of MAD Bonus activated per unit of ad spend is assumed to be κ, thus set $b = \kappa \cdot f$ where it must be the case that $0 \leq \kappa \leq \alpha$.

The utility is derived from a comparative analysis of using MAD Network via MAD token or simply using the existing ad-tech stack. In case 1: the existing ad-tech stack the level of service is simply f and the total value extracted is $\phi_0 \cdot f$ worth of advertisements from publishers. In case 2: the MAD Network the m MAD token is locked up for a period ΔT and the value extracted is $\phi \cdot f$ worth of advertisements from publishers. The per net terms period value of the MAD token can then be estimated as

$$U(F, M) = \frac{\text{Case 2 Value Extracted} - \text{Case 1 Value Extracted}}{\text{Case 2 Token Cost} - \text{Case 1 Token Cost}} \tag{36}$$

$$= \frac{\phi f - \phi_0 f}{L(f, \kappa f, F, M, B) - 0}. \tag{37}$$

Applying equation (24) allows us to specify the above in a form that can be manipulated algebraically;

$$U(F, M) = \frac{f \cdot (\phi - \phi_0)}{(f - b) \cdot \frac{M}{F - B}} \tag{38}$$

$$= \frac{f \cdot (\phi - \phi_0)}{(f - \kappa f) \cdot \frac{M}{F - B}} \tag{39}$$

$$= \frac{\phi - \phi_0}{(1 - \kappa)} \cdot \frac{F - B}{M} \tag{40}$$

and it is observed that the variable f characterizing the level of service falls out. Using our assumption that κ is the Networkwide rate of bonus applied, let $B = \kappa F$ and the expression further simplifies to

$$U(F, M) = (\phi - \phi_0) \cdot \frac{F}{M}. \tag{41}$$

Property 4. *The per period ΔT utility of value of MAD token can be estimated as*

$$U(F, M) = (\phi - \phi_0) \cdot \frac{F}{M} \tag{42}$$

$$= \phi_0 \cdot (\beta - 1) \cdot \frac{F}{M} \tag{43}$$

where (F, M) collectively denote the MAD Network state and $\beta > 1$ is a unitless but measurable coefficient related to the use of the MAD Network software. Furthermore, the tokens to ad spend ratio F/M appears explicitly providing the appropriate units USD/MAD when the financial commitment F is measured in USD.

This property has a hand of interesting qualities. It is immediately clear that the lift β is critical; for $\beta \leq 1$ there would be no benefit in using the MAD Network and thus no utility value. For $\beta > 1$, the larger the lift the more value. Another quality is that the value grows proportionally to the total ad spend on the network, F but is declining in M. The latter may seem concerning but recall that the total supply of MAD token is strictly bounded and the Ad Spend could conceivably grow to include the entire market. Furthermore, the appearance of the ratio F/M is strictly consistent with the concept that the MAD token is a shared networkwide software license where each token can provide a share of the total locked ad spend, per the invariant in Property 3.

3.6. **Property Valuation of MAD Token.** When valuing a rent yielding property over time, it is conventional to use the net present value of annuity as the model. Since $U(F, M)$ is a per-license-period utility, it is appropriate to consider the time value of these savings derived assuming that the user chose to buy and use the MAD tokens as opposed to holding another crypto asset, such as Ethereum or Bitcoin, which is exhibiting ΔT rate of return r. Define the fair value of the token as $\bar{U}(F, M)$ according to the present value of a perpetual annuity, with the simplifying assumption that adoption and thus F/M has reached steady state making $U(F, M)$ constant,

$$\bar{U}(F, M) = \frac{1}{r} U(F, M) = (\beta - 1) \frac{\phi_0}{r} \cdot \frac{F}{M} \tag{44}$$

establishing the Requirement 3, that it is possible to make a meaningful estimate of the value of MAD token as a function of its use and furthermore, that value can be expected to grow with MAD Network traction. While the value $\bar{U}(F, M)$ is not expected to be a prediction of the market price its structure is telling; increases in utility drive incentives to buy and use creating buy side pressure on the MAD token market if the pressure begins to fall below the percived utility. A buyer intending to use the MAD token will respond to the low price by buying because $\bar{U}(F, M)$ does not depend on $p^{(mad)}$.

Property 5. *Whether the purchase was initially speculative or made intent to use, any holder MAD token is strictly better off using the token,* $V_T^{(user)} > V_T^{(investor)}$ *whether for themselves or on behalf of other users by serving the broker role in the MAD Network ecosystem :*

$$V_T^{(investor)} = m \cdot \left(p_T^{(mad)} - p_0^{(mad)} \right) \tag{45}$$

assuming the MAD token is sold at the end of period T*; under the same assumption,*

$$V_T^{(user)} = m \cdot \left(p_T^{(mad)} - p_0^{(mad)} \right) + m \sum_{k=0}^{T} \phi_0 \cdot (\beta - 1) \frac{F_k}{M_k} \tag{46}$$

represents the value claimed by the user over the same period.

Since all of the MAD token returns to the user at the end of the period, the value from investing and the value from using is strictly additive. An investor retains all the value of their speculative investment determined by the change in the market price over the time period but should they make the use of their tokens, extra value is extracted. It is precisely this property that makes MAD token function as a piece a property. In the real estate analogy, this would be akin to making a speculative investment on a condo in a rapidly gentrifying neighborhood; since the notion of flipping does not apply, the investor would always be better off renting the condo during the period of ownership rather than simply allowing it to remain empty while waiting for a good opportunity to sell. Visual description of this combined value is presented in Figure 4.

4. Ongoing Research

4.1. **Economic System Simulations.** The properties demonstrated in this economic specification are derived under a variety of assumptions. While these assumptions may be well justified in theory, the next step toward validating the analysis is to use simulations to demonstrate the intended properties and by further injecting noise, errors or other forms of synthetic uncertainty into the simulations it is possible to get a preliminary sense of the robustness of the analytical properties identified. It is important to recall that human agents are not simply rational actors, and often don't even exhibit consistency in their decision making processes, [32, 33, 34].

The numerical experiments under development are martingale simulations of the state update models accounting for new ad spend entering the ecosystem, MAD token and MAD bonus being escrowed in accordance with the license equation $L(\cdot)$ and the network states M, F and B are tracked. Since the simulations are driven by stochastic processes, the experiments are run repeatedly generating a cloud of possible trajectories and the data is collected into a table of experimental results. The results are analyzed with special attention to the invariant properties, the market price and the utility value of the MAD token. Upon completion of the initial experimental apparatus the simulation code will be open sourced.

4.2. **Technical Feasibility.** Designing economic models that are blockchain agnostic is a challenging problem. There are quite a few blockchain designs that could be used to realize the economic model specified in this paper. It is understood that there is inter-dependence between an economic model and the blockchain designs one had in mind while developing the model. It is acknowledged that the model presented in this paper makes references to, and draws inspiration from Ethereum's ERC-20 and ERC-721 standards. It will be interesting to see how the model will be influenced under different alternative blockchain designs, say Bitcoin or Stellar. A survey of blockchain protocols as of the time of this article is presented in [35].

The team is devising a novel research and development methodology for the MAD Network project, which will be presented in a forthcoming article. The general idea is for modeling and simulation-based research efforts to happen alongside blockchain protocol design, prototyping, and testing at scale. The authors acknowledge the basic tenet that all mathematical models are wrong and some are useful, [36]. As such, to quickly iterate over various economic models, the team is building an experimental testbed and employing a hybrid simulation/emulation approach; see, for example, the Shadow system [37].

References

[1] Mad-Network, "The evolution of ad tech." http://www.madnetwork.io/MAD-Whitepaper.pdf, November 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform." `https://github.com/ethereum/wiki/wiki/White-Paper`, 2014. Accessed: 2016-08-22.

[4] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger." `http://bitcoinaffiliatelist.com/wp-content/uploads/ethereum.pdf`, 2014. Accessed: 2016-08-22.

[5] S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," *SIGACT News*, vol. 33, pp. 51–59, June 2002.

[6] N. A. Lynch, *Distributed algorithms*. Morgan Kaufmann, 1996.

[7] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.

[8] A. Rapoport and A. M. Chammah, *Prisoner's dilemma: A study in conflict and cooperation*, vol. 165. University of Michigan press, 1965.

[9] D. Challet and Y. C. Zhang, "Emergence of cooperation and organization in an evolutionary game," *Physica A*, vol. 246, no. 3-4, p. 407, 1997.

[10] R. Axelrod and R. O. Keohane, "Achieving cooperation under anarchy: Strategies and institutions," *World politics*, vol. 38, no. 1, pp. 226–254, 1985.

[11] J. Nash, "Non-cooperative games," *Annals of mathematics*, pp. 286–295, 1951.

[12] T. Başar and G. J. Olsder, *Dynamic noncooperative game theory*. SIAM, 1998.

[13] E. Nier, J. Yang, T. Yorulmazer, and A. Alentorn, "Network models and financial stability," *Journal of Economic Dynamics and Control*, vol. 31, no. 6, pp. 2033–2060, 2007.

[14] D. Acemoglu, A. Ozdaglar, and A. Tahbaz-Salehi, "Systemic risk and stability in financial networks," *The american economic review*, vol. 105, no. 2, pp. 564–608, 2015.

[15] K. M. Passino, A. N. Michel, and P. J. Antsaklis, "Lyapunov stability of a class of discrete event systems," *IEEE transactions on automatic control*, vol. 39, no. 2, pp. 269–279, 1994.

[16] S.-H. Wang and E. Davison, "On the stabilization of decentralized control systems," *IEEE Transactions on Automatic Control*, vol. 18, no. 5, pp. 473–478, 1973.

[17] R. Nget, Y. Cao, and M. Yoshikawa, "How to balance privacy and money through pricing mechanism in personal data market," *CoRR*, vol. abs/1705.02982, 2017.
[18] G. Zyskind, O. Nathan, *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, 2015.
[19] P. C. Fishburn, "Arrow's impossibility theorem: concise proof and infinite voters," *Journal of Economic Theory*, vol. 2, no. 1, pp. 103–106, 1970.
[20] K. J. Arrow, A. Sen, and K. Suzumura, *Handbook of social choice and welfare*, vol. 2. Elsevier, 2010.
[21] D. Kahneman, J. L. Knetsch, and R. Thaler, "Fairness as a constraint on profit seeking: Entitlements in the market," *The American economic review*, pp. 728–741, 1986.
[22] M. Rabin, "Incorporating fairness into game theory and economics," *The American economic review*, pp. 1281–1302, 1993.
[23] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research society*, vol. 49, no. 3, pp. 237–252, 1998.
[24] MakerDao, "The dai stablecoin system." https://makerdao.com/whitepaper/DaiDec17WP.pdf, December 2017.
[25] M. Zargham, A. Bulkin, H. Huang, and J. S. Nelson, "Sweetbridge liquidity protocol: Mathematical specifications," *Sweetbridge Technical White Paper Series*, vol. 1, November 2017.
[26] K. J. Aström and R. M. Murray, *Feedback systems: an introduction for scientists and engineers*. Princeton university press, 2010.
[27] F. Bullo, J. Cortés, and S. Martínez, *Distributed Control of Robotic Networks*. Applied Mathematics Series, Princeton University Press, 2009. To appear. Electronically available at http://coordinationbook.info.
[28] M. Jackson, *Social and Economic Networks*. Princeton University Press, 2008.
[29] J. D. J. D. Sterman, *Business dynamics: systems thinking and modeling for a complex world*. No. HD30. 2 S7835 2000, 2000.
[30] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains." `https://truebit.io/`, March 2017. Accessed:2017-10-06.
[31] M. Zargham, A. Bulkin, and J. Nelson, "Raising social capital: Tokenizing a customer-driven business." https://sweetbridge.com/whitepaper, forthcoming 2017.
[32] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *Journal of Risk and uncertainty*, vol. 5, no. 4, pp. 297–323, 1992.
[33] E. G. Haug and N. N. Taleb, "Option traders use (very) sophisticated heuristics, never the black–scholes–merton formula," *Journal of Economic Behavior & Organization*, vol. 77, no. 2, pp. 97–106, 2011.
[34] A. Tversky and D. Kahneman, "The framing of decisions and the psychology of choice," *Science*, vol. 211, no. 4481, pp. 453–458, 1981.
[35] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*, pp. 1–5, IEEE, 2017.
[36] J. D. Sterman, "All models are wrong: reflections on becoming a systems scientist," *System Dynamics Review*, vol. 18, no. 4, pp. 501–531, 2002.
[37] Shadow, "an open-source network simulator/emulator hybrid." https://shadow.github.io.

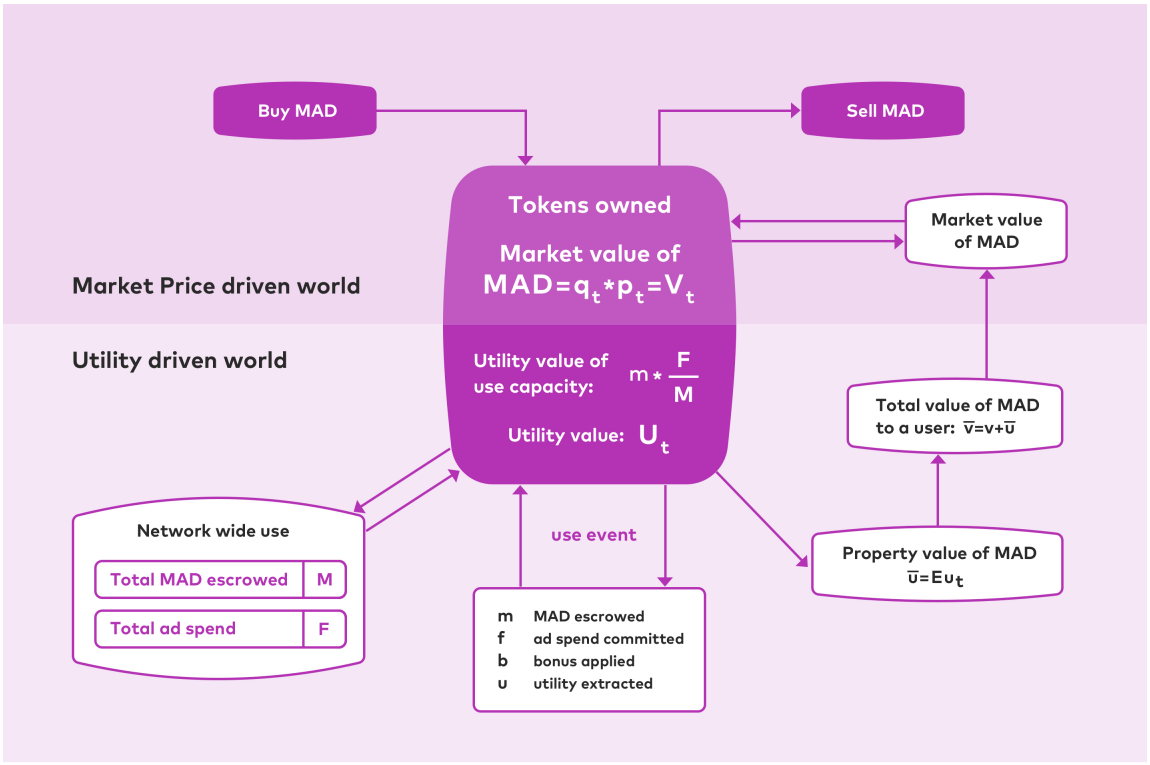

FIGURE 4. The use of the shared Network License in equation (24) unburdens the token from the role of currency and allows to function directly as a software license; the mechanics of the token revolve around use and thus drive rather than get driven by the market price, demonstrating adherence to Requirement 1. In the figure $\bar{V}$ denotes the value of MAD to a holder who is also a user and the notation for $\bar{U}$ presented in equation (44) is reduced to $\mathbf{E}U_t$ denoting the fact that $\bar{U}$ is an expected utility for use which may be estimate in the manner presented here or in accordance with other property-like assets as deemed appropriate. Yet, the value identified from the software utility bolsters rather than detracts from any speculative value perceived by the market. The critical message is that one can examine the value of MAD as a software license independently of its market price in the form of it's capacity to access the MAD Network software. This structure is given by the name *Access Token* and is a special case of the *Discount Token* presented in [31], whereby the user is always expected to escrow sufficient tokens to receive a 100% discount from recurring license fees that would be incurred in the absence of the token.