Cryptoeconomics and Tokenomics as Economics: A Survey with Opinions

***Abstract*—This paper surveys products and studies on *cryptoeconomics* and *tokenomics* from an economic perspective, as these terms are still (i) ill-defined and (ii) disconnected from economic disciplines. We first suggest that they can be novel when integrated; we then conduct a literature review and case study following *consensus-building for decentralization* and *token value for autonomy*. Integration requires simultaneous consideration of strategic behavior, spamming, Sybil attacks, free-riding, marginal cost, marginal utility and stabilizers. This survey is the first systematization of knowledge on cryptoeconomics and tokenomics, aiming to bridge the contexts of economics and blockchain.**

***Index Terms*—blockchain, economics, bitcoin, survey**

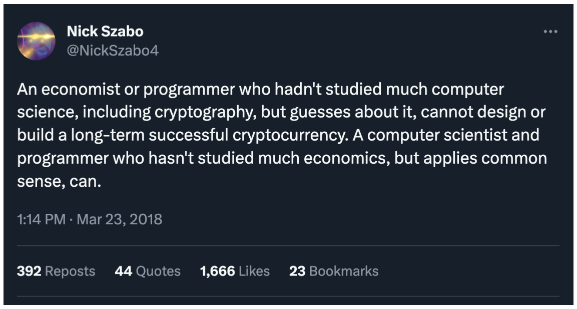
I. Introduction

Bitcoin [1] is the first practical protocol to employ an economic incentive design to implement a peer-to-peer electronic cash system.[1] Specifically, it has enabled consensus-building on transaction records among an unspecified number of strategic peers—a long-standing problem for peer-to-peer electronic cash—with cryptography and subject to the following main rules:

Main Rules of the Bitcoin Protocol

- Transaction records are sequentially stored in blocks, and peers share an identical chain of blocks due to consensus-building (*blockchain*).
- Peers can create a new block and connect it to any existing block in the chain; however, this task succeeds only with a probability proportional to the relative amount of computing resources the peer has expended (*proof-of-work* [6], [7]).
- If the chain forks to multiple paths, the longest chain is considered the consensus (*Nakamoto consensus*).
- Peers who create a block in the longest chain will be rewarded with newly minted Bitcoins (*coinbase as contribution rewards*).

In other words, the Bitcoin protocol makes undesirable actions unprofitable, not impossible. The Bitcoin protocol's novelty lies in utilizing economic incentives for decentralized autonomous consensus-building.



Nick Szabo
@NickSzabo4

An economist or programmer who hadn't studied much computer science, including cryptography, but guesses about it, cannot design or build a long-term successful cryptocurrency. A computer scientist and programmer who hasn't studied much economics, but applies common sense, can.

1:14 PM · Mar 23, 2018

392 Reposts 44 Quotes 1,666 Likes 23 Bookmarks

Fig. 1: Disconnect between Economics and Blockchain

Source: X.com (https://x.com/NickSzabo4/status/977035747713675264, accessed September 4, 2023).

This novelty has transferred to subsequent blockchain-related products, such as *Ethereum* [8], [9] (a protocol that generalized consensus-building to cover from transaction records to state transitions to implement *decentralized applications* [DApps] [10]), *The DAO* [11] (one of the first DApps on Ethereum that aimed to create a decentralized autonomous investment-fund [of Ether]),[2] and *Lightning Network* [19] (another layer on the Bitcoin protocol to increase transaction processing speed [i.e., scalability]).

Cryptoeconomics and *tokenomics* emerged from the above contexts (c. 2014-2016). Namely, if taken in purpose rather than definition, these terms extend the coverage of Bitcoin's novelty—utilizing economic incentives for decentralized autonomous consensus-building—from on-chain transaction records to more generalized information, including on-chain state transitions (Ethereum), off-chain peer beliefs regarding appropriate investments (The DAO), and off-chain transaction records (Lightning Network).

Despite their importance, cryptoeconomics and tokenomics face two challenges at the time of this writing. First, they are ill-defined. Section II shows that these terms are often used without clear definitions or distinctions because

[1] Peer-to-peer electronic cash systems prior to the Bitcoin protocol include, for example, *b-money* [2] and *Bit gold* [3]. The extant literature provides a comprehensive pre-Bitcoin history [4], [5].

[2] The term *Decentralized Autonomous Organization* (DAO) first appeared in the Ethereum Whitepaper as "a virtual entity that has a certain set of members or shareholders which, perhaps with a 67% majority, have the right to spend the entity's funds and modify its code [12]." Buterin also referred to a concept very close to what is now called a DAO in 2013 as follows: "But what if, with the power of modern information technology, we can encode the mission statement into code; that is, create an inviolable contract that generates revenue, pays people to perform some function, and finds hardware for itself to run on, all without any need for top-down human direction? [13]." Note that The DAO was hacked in 2016 and and is currently inaccessible [14], [15]. The extant literature provides the characteristics and types of current DAOs [16]–[18].

of their emerging and interdisciplinary aspects [20]. This ambiguity makes productive discussions difficult. Second, even with the name "economics," they are disconnected from economic disciplines. As cryptographer Nick Szabo's post (Figure 1) implies, these terms have not adequately referenced prior economics studies or attempts to integrate economics with computer science (see Sections III and IV for more details). Conversely, economists appear to show limited interest in cryptoeconomics and tokenomics despite the synergy between economics and blockchain-related products. This disconnect, a factor in reinventing the wheel, further makes productive discussions difficult.

This paper surveys products and studies behind cryptoeconomics and tokenomics from an economic perspective to address the two challenges. We address the former challenge by presenting a new definition through a historical review of the two terms; the latter challenge is examined via a literature review and case studies, following *consensus-building for decentralization* and *token value for autonomy*. To the author's best knowledge, this survey is the first systematization of knowledge (SoK) on cryptoeconomics and tokenomics that aims to bridge the respective contexts of economics and blockchain.[3]

This paper comprises six sections, including this introduction. Section II covers history and opinions for terminology, Section III reviews prior studies on designing consensus-building for decentralization, and Section IV reviews prior studies on designing token value for autonomy, Section V provides case studies for each protocol and DApp, and Section VI presents the conclusion and future research directions.

II. History and Opinions for Terminology

Cryptoeconomics and tokenomics have a clear purpose, but their definition and distinction remain unclear. For a productive discussion, this section will first review the history of the two terms chronologically and then present the author's opinion on how they should be defined.

A. Cryptoeconomics

Cryptoeconomics is a term that originally came from the Ethereum community. It was first used publicly in a 2015 presentation by Vlad Zamfir, one of the core members of the *Ethereum Foundation* [22]. In his presentation, he referred to cryptoeconomics as "a formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols" [23].

Around the same time in 2015, Vitalik Buterin, one of the two founders of Ethereum, described the concept *cryptoeconomic* as follows: "it's decentralized, it uses public key cryptography for authentication, and it uses economic incentives to ensure that it keeps going and doesn't go back in time or incur any other glitch" [24]. His description becomes more specific in a later 2017 presentation. Buterin stated that cryptoeconomics concerns "Building systems that have certain desired properties. Use cryptography to prove property about messages that happened in the past. Use economic incentives defined inside the system to encourage desired properties to hold into the future" [25]. Buterin provided this definition while introducing several examples (e.g., *SchellingCoin* [26], blockchain-fork) that leverage cryptography and game-theoretic coordination for consensus-building.

Davidson, et al. (2016) [27] was probably the first publication to explicitly mention the above trend in academia. They positioned cryptoeconomics as "a branch of mechanism design, which is a branch of microeconomics [27]," based on the definition by Vlad. Similarly, Obasi (2017) [28] interpreted cryptoeconomics as follows: "It has more in common with mechanism design—an area of mathematics and economic theory, sometimes referred to as reverse game theory [28]." Furthermore, Voshmgir and Zargham (2019) [20] referred to cryptoeconomics as "an emerging field of economic coordination games in cryptographically secured peer-to-peer networks [20]," noting its relevance with several other disciplines, including system theory, political science and network science. See Figure 2 below for the relationship between microeconomics, game theory, and mechanism design that the series of discussions implicitly assume.

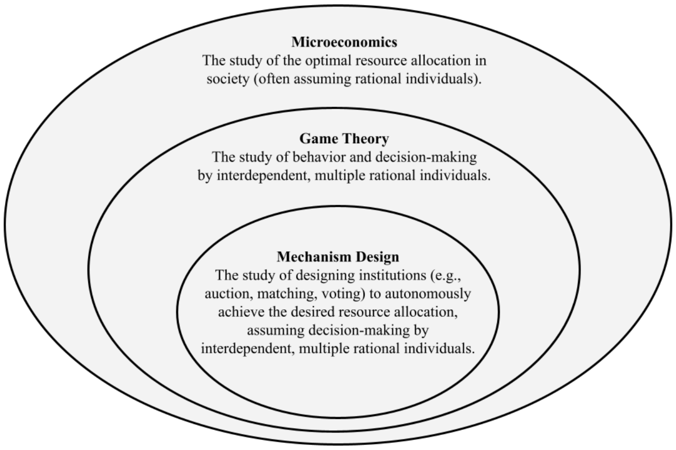

Microeconomics
The study of the optimal resource allocation in society (often assuming rational individuals).
Game Theory
The study of behavior and decision-making by interdependent, multiple rational individuals.
Mechanism Design
The study of designing institutions (e.g., auction, matching, voting) to autonomously achieve the desired resource allocation, assuming decision-making by interdependent, multiple rational individuals.

Fig. 2: Relationship between Microeconomics, Game Theory, and Mechanism Design

Finally, as a hybrid of the above discussions, Brekke and Alsindi (2021) [29] provided the following general definition: "Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies [29]."

Thus, cryptoeconomics focuses on economic incentives as a means of consensus-building and, although interdisci-

[3] Strictly speaking, this survey is an extended version of the report by Ito (2018) [21] (in Japanese).

plinary, it would be placed in the context of mechanism design.[4]

B. Tokenomics

Tokenomics has existed since at least 2012 [30]; to the author's knowledge, it was first used in blockchain discussions by Mougayar (2017) [31]. Unlike many other studies, he interpreted cryptoeconomics as "a term that has come to describe the mechanics and specifics of token distribution, according to a given sale and ownership structure [31]," and started to use the term tokenomics as a contrast to emphasize the importance of "the utility role of the token [31]" to "deliver a viable business model for the long term [31]." In other words, tokenomics was originally used to promote attention to tokens' demand side (i.e., utility) rather than their supply side.

In contrast, Ennis, et al. (2018) [32] mentioned three aspects of tokenomics: "(1) a means of self-funding within the crypto economy, (2) the deployment of a token within the ecosystem of an ICO project and (3) the set of all economic activity generated through the creation of tokens [32]." Here, tokenomics was extended to cover both the demand and supply sides.[5]

Furthermore, Au and Power (2018) [30] defined tokenomics more broadly, even overlapping with cryptoeconomics. They interpreted tokenomics as "the concept of the study, design, and implementation of an economic system to incentivize specific behavior in a community, using tokens to create a self-sustaining ad hoc mini-economy. It includes game-theory, mechanism design and monetary economics [30]."

Finally, Kampakis (2022) [34] provided the broadest definition: "the study of how crypto tokens are used within the blockchain ecosystem [34]," covering "1) The number of tokens issued and the way they are issued (vesting schedule, airdrops, etc.). 2) The economics of a consensus algorithm; largely referred to as crypto-economics. 3) The general structure of the system: game theoretic and economic incentives [34]."

As shown tokenomics began with a discussion of token value and gradually came to encompass cryptoeconomics as a subcategory.

C. Opinion: They Are Individually Not So Novel

Such trends lead to two opinions. First, cryptoeconomics and tokenomics have similar precedents in economics.

For cryptoeconomics, game theory was applied to cryptography at least as early as 1993 [35], and the two has been studied together ever since [36]. Nisan et al. (1999) [37] and subsequent studies [38], [39] have developed an *algorithmic mechanism design* (AMD) that applies mechanism design to computational issues (e.g., routing and load balancing), considering additional constraints like computational resources. Furthermore, as a branch of AMD, Feigenbaum et al. (2000) [40] even proposed the concept of *distributed algorithmic mechanism design* (DAMD), which primarily focuses on peer-to-peer systems where agents, computational resources, and networks are all distributed. A survey paper [41] in 2004 outlined several open problems in DAMD, including the following:

> "Open Problem 10. Can digital signatures (or, more generally, cryptographic protocol-design techniques) always be used to convert a distributed algorithmic mechanism in which some of the parties must be assumed to be obedient into one with a more realistic strategic model?"

> "Open Problem 18. Can one design monetary P2P systems that provide better performance than purely barter P2P systems? Can one characterize, in simple models, the possible outcomes achievable with both kinds of P2P economies?"

Although raised a decade before the implementation of Ethereum, these open problems are very close to those in cryptoeconomics.

For tokenomics, value and price were theorized in 19th-century (neoclassical) economics [42], which states that a good's market price is determined as the intersection of supply-side value (depends on marginal cost) and demand-side value (depends on marginal utility).[6] Based on this theory, economic studies have analyzed more specific goods, such as money [43], securities, and stocks [44], and developed dynamic models that consider individual expectations. These studies share similarities with tokenomics [45] and have been extended to the design of (rule-based) monetary policies [46] and digital currencies [47]. These precedents are very close to tokenomics because they are trying to design financial rules and products based on theories of value and price.

D. Opinion: They Can Be Novel When Integrated

Second, cryptoeconomics and tokenomics can be novel when integrated. Despite similar precedents for each, to the author's knowledge, no academic efforts have addressed (cryptoeconomic) consensus-building and (tokenomics) token value together; however, such integration is essential because the two aspects are interrelated in practice. Consensus-building cannot be autonomous if the token as a reward

[4] Brekke and Alsindi (2021) [29] argues the interdisciplinary nature of cryptoeconomics as follows: "Cryptoeconomics is an embryonic field at present and can be taken to include several areas of focus: information security engineering, mechanism design, token engineering and market design [29]."

[5] Blemus and Guégan (2020) [33] interpret this definition as "a self-funding mechanism for projects within the crypto economy [33]" and add the following two to this primary definition: "would apprehend the notion of token, beyond this strictest definition, along the lines of its function [33]," "tokenomics which focuses on the economic activity and value generated through the token creation [33]."

[6] Marshall (1890) [42] likened the debate over whether the source of value lies in cost or utility to a futile debate over whether the top or bottom blade of scissors does the cutting. This perspective is relevant in discussing the Bitcoin's value, where the marginal cost corresponds to the computational resource of proof-of-work, and the marginal utility corresponds to its utility as an electronic peer-to-peer cash system and transaction fee. The market price of Bitcoin is at their intersection (see Section IV for more details). Despite the theory's simplicity, whether Bitcoin's value lies in proof-of-work is still often debated, and to the author's knowledge, no economists has pointed out the futility of the debate. This situation reflects the disconnect between blockchain and economics.

does not have value, and token value does not contribute to decentralization if the product lacks consensus-building. Accordingly, cryptoeconomics and tokenomics should be integrated and renamed to reflect *the design of mechanism and reward*, or *token-based mechanism design*.

This section organized the history of cryptoeconomics and tokenomics chronologically, suggesting that they can be novel when integrated. The next two sections will present blockchain-related products and prior studies in more detail, following two categories for integration: *designing consensus-building for decentralization* (Section III) and *designing token value for autonomy* (Section IV).

III. Designing Consensus-Building for decentralization

In the context of blockchain, decentralization is strongly associated with consensus-building[7]; instead of delegating centralized authorities, we require some mechanism for eliciting and aggregating information from peers and making some output as a consensus (e.g., the aforementioned *main rules of the Bitcoin protocol*). This section presents what obstacles blockchain-related products and prior studies have faced and addressed in designing such consensus-building for decentralization.

A. How to Address Strategic Behavior

First, consensus-building must prevent the strategic behavior of peers, which intuitively denotes the action of deliberately misreporting accurate information.[8] For example, peers in the Bitcoin protocol might create a block containing conflicting transactions (e.g., double-spending); peers in The DAO might misreport their beliefs about appropriate investments to gather more Ether to their proposals. Such behavior would be more likely to occur given the possibility of collusion among multiple peers.

The Bitcoin protocol addresses strategic behavior by adopting the aforementioned main rules. Particularly, the combination of proof-of-work and Nakamoto consensus turns consensus-building (on transaction records) into a form of majority voting, where voting power is proportional to each peer's computational resources. Furthermore, many subsequent blockchain-related products have adopted variations of the following *token-staking* rules for consensus-building.

> *Token Staking (a simple example of binary choice)*
>
> - Peers can stake any amount of their tokens to either *accept* or *reject* a proposal,
> - Consensus is the choice of which collects more tokens after a certain period,
> - All staked tokens are redistributed among peers who staked them on the consensus side.

Namely, token-staking is assumed to prevent strategic behavior by i) majority voting with tokens (mostly at some cost to obtain) and ii) the penalty of losing staked tokens. The above is a simple example, and various forms of token-staking exist for consensus-building. The DAO adopted the token-staking with multiple choices. *Nouns DAO* [51], another DAO detailed in IV-B and V-C, adopts token-voting, where staked-tokens are neither redistributed nor burned (i.e., trying to prevent strategic behavior without penalty). Ethereum adopts *proof-of-stake* [52] and *Gasper* [53], where staked tokens are not redistributed but are burned when a peer misreports (i.e., staked tokens are like a deposit for consensus-building).[9]

Prior studies in economics, especially in game theory, have formalized strategic behavior and its solution concepts. For example, *strategy-proofness* (*truthfulness*) is a solution concept where players in a *mechanism* [55] cannot gain more utility by deviating from truth-telling.[10] Strategy-proofness has been applied to systems including voting, and the mechanism satisfying it was later generalized as the *VCG mechanism* [58]–[60].[11] It would be natural to apply the game-theoretic approach to blockchain-related products. In particular, a number of studies have modeled the Bitcoin protocol as a game and analyzed peers' activities using solution concepts like strategy-proofness [61]–[63]. Token-staking has also been modeled in game theory [64]. These studies, especially the axiomatic ones [65], [66], tend to evaluate the combination of proof-of-work and Nakamoto consensus compared to others based on token-staking.

The *Keynesian beauty contest* [67], [68] is perhaps one of the most essential game-theoretic concepts for blockchain, representing the case where players vote based on the prediction of other players' beliefs rather than their own.[12] The Keynesian beauty contest could occur in the Bitcoin protocol and the token-staking (not voting) rule. Peers who want to

[7] Here, the usage of the term decentralization follows Hoffman et al. (2020) [48] and Zhang et al. (2022) [49].

[8] In computer science, strategic behavior encompasses a broader concept known as the *Byzantine Generals Problem* [50], which includes considerations of unintentional malfunctions of peers, such as communication failures. The Bitcoin protocol offers a quasi-solution to this problem, given that Nakamoto consensus lacks finality (III-D).

[9] Previously, Ethereum utilized proof-of-work and Nakamoto consensus; however, this changed with a major update in September 2022. See Pavloff et al. (2023) [54] for the detail of new consensus-building on Ethereum.

[10] Note that strategy-proofness ensures truthtelling is a weakly dominant strategy, meaning that it allows for cases where truth-telling and other strategy yield the same amount of utility. More practical solution concept, such as *strongly truthfulness* [56], also exist. See Tardos and Vazirani (2007) [57] for example about the detail and differences of other solution concepts.

[11] Mechanism design is often referred to as inverse game-theory because it derives institutions from solution concepts, not solution concepts from institutions.

[12] Recently, the concept of Keynesian beauty contest has been generalized as the *p-Beauty contest game* [69], [70]. This is a number-guessing game where players predict mean value of submitted numbers, multiplied by $p \in (0, 1]$. If the game involves guessing the mean value (i.e., $p = 1$), there exists as many Nash equilibria as the number of choices.

maximize their expected rewards might decide on the block to connect [71] or the choice to stake their tokens [72]–[74] based on the prediction of other peers' beliefs rather than their own. This case presents a challenge in eliciting true beliefs from each peer. Nevertheless, the Bitcoin protocol and the token-staking rule remain popular for two reasons. First, experimental studies [75] and behavioral game theory [76] have shown the existence of unique Nash equilibria (*Schelling points*) even in the Keynesian beauty contest, suggesting that it is critical in theory but less so in practice. Second, as shown in III-B and III-C, these consensus-building approaches help address other obstacles, such as spamming, Sybil attacks, and free-riding.

B. How to Address Spamming and Sybil Attack

Moreover, consensus-building needs to address *spamming* [77], [78] and *Sybil attacks* [79], where the former means "the act of spreading unsolicited and unrelated content," and the latter means "the forging of multiple identities." For example, peers in The DAO might create numerous meaningless proposals to disrupt consensus-building (spamming) or pretend to be different individuals even though they are controlled by one entity (Sybil attack). A decentralized system must address these problems without relying on the management of some centralized entity.

Blockchain-related products have levaraged the traditional solution for spamming, assigning a small cost for each transaction. This method, initially proposed as *Hashcash* [80], adds a minor computational cost to sending email. The cost accumulates as the number of transaction increases, making spamming unprofitable. Protocols like Bitcoin and Ethereum require *transaction fees* in Bitcoin or Ether, which is paid by the transaction sender to the miner (validator) who includes the transaction in a valid block.[13] DApps usually impose additional fees in tokens whenever peers create a proposal that requires consensus-building [51], [81].

For Sybil attacks, blockchain-related products ususally address this problem by making voting power independent of individuals. In the Bitcoin protocol, the probability of creating a new block is proportional to computational resources (proof-of-work), i.e., one CPU = one vote. The token-staking has similar objective; voting power is (in most cases) proportional to the token amount, i.e., one token = one vote. This approach would be natural in an environment where individuals can make any number of peers. Alternatively, some platforms, like *Gitcoin* [82] (see also V-B) and *Worldcoin* [83], use more direct methods like requiring social media accounts or employing biometric authentication using the iris. While these models are not as decentralized as the one CPU = one vote or the one token = one vote models, they offer more direct ways of establishing individual identities, enhancing the efficiency of consensus-building.[14]

Prior studies in economics (in addition to axiomatic ones [65], [66]) have also addressed spamming and Sybil attacks. Spamming has been modeled as a game between a spammer and a detector [86], including models that impose a small cost on each transaction, similar to blockchain solutions [87].[15] Sybil attacks have also been examined from a game-theoretic perspective, with studies [89]–[91] proposing various mechanisms involving rewards, penalties, and costs for mitigation. Such game-theoretic approaches to Sybil mitigation have recently been applied to blockchain-related products, especially to the protocol alternative to proof-of-work and proof-of-stake [92], [93].[16]

C. How to Address Free-riding Problem

Even if we can prevent strategic behavior, spamming and Sybil attack, how can we facilitate consensus-building participation? Given the time and effort for assessment, peers may not commit to consensus-building in the first place or provide uninformative reports independent of true beliefs (e.g., automatically sending the same report). Such behavior, described as "an individual user who uses the system resources without contributing anything to the system" [95] is typical in peer-to-peer systems as a *free-riding problem*.[17]

Blockchain-related products have addressed this free-riding problem simply by rewarding participants. The Bitcoin protocol provides newly issued Bitcoin to the peer who creates a block in the longest chain (i.e., coinbase). Token-staking usually involves redistributing staked tokens (e.g., The DAO) or issuing new tokens to peers participating in consensus-building (e.g., Ethereum); however, these free-riding measures through rewards induce strategic behaviors such as the Keynesian beauty contest.[18]

Few prior studies in economics cover free-riding because game theory or mechanism design implicitly assumes that players participate in consensus-building without any rewards (e.g., auction, voting)[19]; however, this topic has been studied in DAMD, especially in fields applying game theory to elicit true beliefs from peers (agents) in systems such as crowdsourcing, rating systems, and federated learning [101], [102].[20] These studies generally assume that peers i) first report the content of stochastic *signals* emitted from the assigned *tasks* ii) and then obtain *rewards* whose amount is computed from collected reports (Figure 3). The goal is

[13] Note that Hashcash is also the origin of proof-of-work. The Bitcoin protocol has applied the solution for spamming to the solution for strategic behavior in consensus-building as well.

[14] See also *Decentralized Identifiers* (DIDs) [84], [85] as a similar concept.

[15] See Rao and Reiley (2012) [88] for other economic analysis on spamming.

[16] See Levine et al. (2006) [94] for other ways to mitigate Sybil attacks.

[17] Note that in economics, the term 'free-riding' is specifically used for non-excludable goods and carries a slightly different meaning than it might in the blockchain context [96].

[18] According to Appendix A of Ito (2021) [97], the simple rule of redistributing staked tokens in token-staking rules does not seem to increase the expected amount of rewards. Therefore, issuing new tokens is necessary to effectively address the free-riding."

[19] To the author's knowledge, Thum (2018) [98] and Soria (2020) [99] have analyzed whether it is reasonable for peers to participate in the consensus-building of the Bitcoin protocol, using the framework of *Tullock contests* [100].

[20] This topic is also known as *Information Elicitation without Verification* (IEWV).

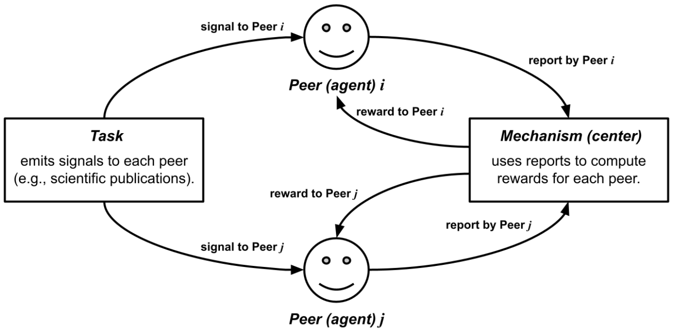


Fig. 3: Mechanisms for Information Elicitation

to design a mechanism that provides maximum expected rewards when peers report accurate signals. This field has proposed various mechanisms such as *Bayesian truth serum* (BTS) [103], *peer-prediction* [104], and *correlated agreement* (CA) [56]. For example, the following is an overview of a simple CA mechanism designed by Dasgupta and Ghosh (2013) [56] (DG13):

CA Mechanism by Dasgupta and Ghosh (DG13)

DG13 considers the following situation:

- Two peers, i and j, each review multiple tasks.
- They report binary signals, e.g., {accept, reject}.
- Each time i and j review the same task, they receive a reward x calculated as follows:

$$x = \delta(r_i, r_j) - \delta(r'_i, r'_j),$$

where r_i and r_j are the reports of i and j for the same task; r'_i and r'_j are other reports of i and j, selected randomly from their previous ones. δ is the Kronecker delta denoting the following function:

$$\delta(a, b) \;=\; \begin{cases} 0 & \text{if} \;\; a \neq b, \\ 1 & \text{if} \;\; a = b. \end{cases}$$

DG13 has two assumptions:

- Tasks emit binary signals, e.g., {accept, reject}, positively correlated among tasks.
- Peers take a mixed strategy for received signals.[a]

[a] Namely, peers decide $p_1 \in [0, 1]$ and $p_2 \in [0, 1]$, where they report *accept* with probability p_1 and *reject* with probability $(1 - p_1)$ if an *accept* signal is received. Peers report *accept* with probability p_2 and *reject* with probability $(1 - p_2)$ if a *reject* signal is received.

Despite its simplicity, this mechanism achieves the solution concept of *strongly truthfulness* [56] where peers maximize their expected rewards by constantly reporting accurate signals or constantly reporting wrong signals.[21]

TABLE I: Transaction per Second (TPS) as of October 2023

Protocols	approx. TPS
Bitcoin [1]	5 - 7
Ethereum [8], [9]	12 - 15
VISA	$1,700$

Sources: Blockchain.com (https://www.blockchain.com/explorer/charts/transactions-per-second, accessed September 4, 2023), Dune.com (https://dune.com/k06a/TPS, accessed September 4, 2023), HackerNoon.com (https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44, accessed September 4, 2023)

For task allocation and reward computation, these mechanisms on information elicitation usually assume centralized authorities (Figure 3); however, several studies [97], [106]–[109] try to apply these mechanisms to decentralized blockchain-related products, including an attempt to integrate information elicitation and information aggregation (i.e., how to make a consensus from elicited information) [110].

D. How to Address Other Norms

If we consider the obstacle to designing consensus-building, we must also consider the norms of what constitutes "good" design. Consensus-building can improve by addressing strategic behavior, spamming, Sybil attacks, and free-riding. Furthermore, the blockchain context has fostered a variety of other norms, especially in the process of improving the Bitcoin protocol.

One of the most critical norms is *scalability* [111]. Decentralized consensus-building can become congested due to an increasing number of transactions and peers, independent of spamming and Sybil attacks. Decentralized protocols currently have a lower *transaction per second* (TPS) compared to existing centralized systems (Table I),[22] which is a significant challenge for their practical use in peer-to-peer electronic cash systems or DApps platforms. Blockchain-related products have addressed this issue mainly via the *Layer 2* approach, i.e., building another layer on the protocol to aggregate and process transactions, such as the Lightning Network [19] and *ZeroSync* [114] for the Bitcoin protocol and *Arbitrum* [115], [116] and *ZK-SNARKS* [117][23] for Ethereum. Here, incentive design and cryptography are crucial in maintaining decentralized aspects on Layer 2.[24] The extant literature provides details of blockchain scalability [124], [125].

[21] Shnayder et al. (2016) [105] has extended DG13 from binary to multiple signals.

[22] According to official statements [112], [113], VISA's TPS has a capacity exceeding 65,000. The figure of 1,700 TPS mentioned in the table is an estimated based on its current usage.

[23] ZK-SNARKS employs a cryptographic method known as *zero-knowledge proof* (ZKP) [118]. In the blockchain context, ZKP was initially used for privacy-focused initiatives, such as anonymous money transfers [119]. Its applications to scalability issues were later promoted by Buterin [120], [121].

[24] Some argue that blockchain faces a *trilemma* [122], suggesting that it can achieve only two out of the three goals: scalability, decentralization, and security. This concept was recently formulated by Nakai et al. (2023) [123].

Other notable norms for consensus-building are *finality* [126] and *energy efficiency* [127]. Nakamoto consensus cannot reach the final (the state that will not be reverted) as the longest chain is stochastic in the Bitcoin protocol, not deterministic; proof-of-work requires a large amount of energy for consensus-building.[25] Consensus-building using token-staking is preferable from these perspectives as it is deterministic and more energy-efficient. For energy efficiency, blockchain-related products have explored using proof-of-work computational resources for other purposes, like finding prime numbers [131] and solving optimization problems [132].

Moreover, several products have introduced new norms for the voting power of peers. Decentralized storage networks [133], [134] (e.g., *Filecoin* [135], *Arweave* [136], and *Sia* [137]) have designed protocols where the voting power depends on the amount of storage provided by peers. *NEM* [138] proposed *proof-of-importance*, a hybrid of proof-of-work, proof-of-stake, and the network structure of token transactions. Gitcoin [82] adopts *quadratic voting* (QV) [139]–[142], a derivative of token-voting, where a peer's voting power for an option is the square root of the number of tokens they have staked there.[26] The extant literature provides the details of blockchain consensus-building [143]–[146].[27]

This section surveyed how blockchain-related products and prior studies have addressed the obstacles of designing consensus-building for decentralization, where obstacles include strategic behavior, spamming, Sybil attacks, and free-riding. A practical design should address these obstacles simultaneously.

IV. Designing Token Value for Autonomy

The previous discussion implicitly assumes that peers act to maximize the amount of their expected rewards; however, if rewards are tokens, we need to make the token valuable and sufficient to use as an incentive (peers would behave differently if the reward tokens were redeemable for 0.1 US dollars (USD) versus 1,000 USD). This section surveys how blockchain-related products and prior studies have addressed the design of token value for autonomy using the framework of microeconomics.

A. How to Ensure Market Price (Supply Side)

First, valuable tokens must ensure their market price. As mentioned in II-C, the intersection of the supply-side value on the marginal cost and the demand-side value on the marginal utility determines the market price of goods [42].

On the supply side, the value depends on the marginal cost: the cost added by producing one additional unit of a product or service. Intuitively, we continue to produce goods as long as we can sell them at a price above their marginal cost.

Many blockchain-related products seem to incorporate this concept naturally. For example, the Bitcoin protocol provides a coinbase for the peer who succeeds in making a new valid block at the expense of proof-of-work, meaning creating one additional Bitcoin unit requires computational resources. Moreover, the following additional rules are worth noting for the marginal cost of Bitcoin:

Additional Rules of the Bitcoin Protocol

- The amount of coinbase halves for every 210,000 blocks. This halving will continue until all Bitcoins (21 million) are mined (*block-reward halving.*[a])
- The difficulty of proof-of-work changes for every 2,016 blocks to keep the block interval 10 minutes (*difficulty adjustment.*[b])

[a] https://www.bitcoinblockhalf.com/

[b] https://www.blockchain.com/explorer/charts/difficulty

The extant literature provides more details [1], [148], [149]. Notably, the former *block-reward halving* works to gradually increase the marginal cost.[28] For blockchain-related products, marginal cost is not limited to computational resources. Ethereum uses the opportunity cost of staking because its proof-of-stake requires token staking to participate in consensus-building. Decentralized storage networks (III-D) use storage space, while The DAO (and many other DApps) use human resources (in addition to the opportunity cost of staking) because its consensus-building deals with subjective issues.

The marginal cost (of a token) may depend on another token. For example, many DApps adopt *initial coin offering* (ICO) for the initial distribution of tokens [150], [151], where we can obtain tokens by exchanging them for other tokens (mostly Ether) at a given rate for a given period.[29] In this case, marginal cost is the value of another token (even at the time of initial distribution). Some DApps (such as *Edgeware* [153] and *Astar* [154]) adopt *lockdrops* for the initial distribution of tokens, where tokens can be obtained by depositing another token (mostly Ether) for a given period. Unlike ICOs, locked

[25] See the Hashrate chart [128] for information on the computational resources used by the Bitcoin protocol for consensus-building. Some studies criticize this level of resource consumption [129], while others defend it [130].

[26] Note that models, deviating from the one CPU = one vote or one token = one vote principles, may be more vulnerable to strategic behavior, spamming, Sybil attacks, and free-riding. In particular, QV is susceptible to collusion and Sybil attacks, as discussed in V-B.

[27] Prior studies in economics, particularly in social choice theory [147], have also fostered norms related to consensus-building. These norms serve as the foundation for game theory and mechanism design. Comparing norms with each other, or applying them to contrasting topics, could be another way to bridge the contexts of economics and blockchain.

[28] It is also worth noting that block-reward halving contributes to user acquisition in the early phase. This is because it offers a kind of first-mover advantage; specifically, peers who participate in consensus-building early can earn more Bitcoin as a reward.

[29] Ethereum itself also conducted an ICO (even though the term did not exist at the time), using Bitcoin [152]. To the author's knowledge, the first ICO that used Ether was conducted by The DAO (referred to as a crowdsale at that time). In both cases, these ICOs encouraged early participation by gradually increasing the exchange rate throughout the sale.

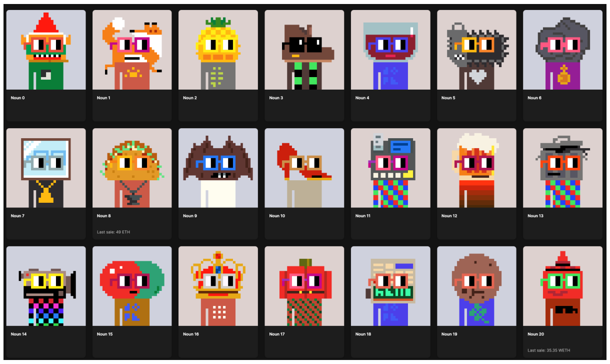


Fig. 4: NFTs of Nouns DAO

Source: OpenSea.io (https://opensea.io/collection/nouns?search[collections][0]=nouns&search[sortBy]=CREATED_DATE, accessed November 8, 2023).

tokens will be returned after the period (e.g., one year). In this case, marginal cost is the opportunity cost of another token.[30]

Prior economics research focused on token valuation [156] rather than design, potentially because economics has already concluded that we can design supply-side value by imposing some cost on new token issuance (and it is even better if that cost increases over time). Marginal cost has been a useful quantitative measure for valuation, especially for Bitcoin as computational resources are relatively easy to calculate. Hayes (2015, 2017, 2019) [157]–[159] developed a cost-of-production model for the valuation of Bitcoin,[31] which has extended to focus on halving[32] [161], [162] and analyze tokens other than Bitcoin [158]. For proof-of-stake, Fanti et al. (2019) [163] modeled the opportunity cost of staking as the expected rate of return on a risk-matched investment strategy in financial markets.

B. How to Ensure Market Price (Demand Side)

On the demand side, the value depends on the marginal utility, i.e., the benefit gained from consuming one additional unit of a product or service. Intuitively, we continue to consume goods as long as we can buy them at a price below their marginal utility.

Blockchain-related products have designed tokens with a variety of marginal utility. For example, the Bitcoin protocol ensures this aspect simply by its utility as an electronic peer-to-peer cash system, where the marginal utility may exponentially increase with the number of users (*Metcalfe's law* [164]). Bitcoin also has the utility of a transaction fee in the protocol. Ether has the utility of being able to use DApps on Ethereum; this is why Ether is often called as digital-oil while Bitcoin is called as digital-gold [165]–[167].

Subsequent DApps have diversified marginal utility (of a token). A straightforward approach is the analogy with stocks, i.e., token holders can participate in the governance and receive a share of the profits. This type of token is expected in the context of DAO and *decentralized exchange* (DEX) [168], [169], a DApp for exchanging tokens without a centralized entity (e.g., *Uniswap* [170], *Curve* [171]). DEXs usually create a *liquidity pool* for exchange, a vault of two (or more types of) tokens collected from peers (see IV-D for details). Here, peers who provided tokens to the pool can earn *liquidity provider (LP) tokens* that reward holders with a portion of the fees from DEX users. DEXs may also issue *governance tokens* (e.g., UNI in Uniswap, CRV in Curve) that allow holders to participate in voting on system updates (see V-E for details). Another notable approach is the analogy with art, i.e., token holders can enjoy the design and rarity of tokens. This type of token is referred to as a *non-fungible token* (NFT) [172], [173], i.e., a standard to make the token a unique, collectible item (e.g., *CryptoKitties* [174] and *CryptoPunks* [175]). NFTs have an advantage over existing art in that, once issued, their authenticity and provenance are guaranteed (as they are on-chain data). Note that these approaches can be combined. For example, Nouns DAO [51] issues NFTs every once a day as collectible items (Figure 4), which can be used as governance tokens as well (see V-C for details). The extant literature provides a detailed classification of token utility [176]–[178].

Prior economics studies have used various proxies to quantify marginal utility. For the Bitcoin protocol, the number of users has been used as a standard proxy [179], [180]. For more general tokens, Cong et al. (2021) [181] developed a dynamic valuation model where tokens' current and future utilities are derived from the number of users and transactions. Liu (2022) [156] proposed a model that estimates token utility with token velocity, staking ratio, and the dilution rate.[33] For tokens with regular income (e.g., LP tokens), traditional asset valuation models, such as the DCF method, can be applied [182]. NFT valuation focuses on the above proxies [183] and their unique and heterogeneous aspects, such as visual images [184] and descriptions [185].[34]

C. How to Stabilize Market Price

Given its role as an incentive, the token's market price should not fluctuate too volatilely. Market prices fluctuate

[30] Another method for initial token distribution is an *airdrop*, where peers can obtain tokens provided their accounts meet certain conditions (e.g., having used the DApp before). Although this appears to incur little marginal cost, the rationale behind airdrops has recently been explored by Allen et al. (2023) [155].

[31] He has developed this model as a counter to the Yermack (2015) [160]'s argument that Bitcoin has no intrinsic value.

[32] Pagnotta and Buraschi (2018) [161] argues that the block reward-halving may have both positive and negative effect on the Bitcoin price, as it reduces the increasing rate of total supply, not the total supply itself (i.e., disinflation, not deflation).

[33] Specifically, token velocity is "the percentage of tokens transacted over a specific period relative to the token supply" [156]; staking ratio is "the proportion of staked tokens to the total token supply" [156]; the dilution rate is "the annual growth rate of the token supply" [156].

[34] *Sentiment analysis*, which estimates demand using tools like Google Trends and posts from X (formerly Twitter), is worth mentioning in this context. While sentiment analysis can be applied regardless of the token type, previous studies have primarily focused on short-term price fluctuations [186], [187]. However, for example, Silberholz and Wu (2021) [188] attempts to decompose the results of sentiment analysis into speculative and utility-related elements.

due to speculative activities and unpredictable events, which may seem difficult to control by design. Nevertheless, protocols like Bitcoin and Ethereum include stabilizers that indirectly mitigate price fluctuations.

For example, the Bitcoin protocol includes the difficulty adjustment mentioned above that increases proof-of-work difficulty when the final 2,016 blocks are generated too quickly, and vice versa. Difficulty adjustment, even intended for constant block-interval, can contribute to the price stabilization in terms of making marginal cost predictable and less volatile, i.e., a sudden increase in computational resources may subside with the next difficulty increase.[35] An auction-based transaction fee is another stabilizer for the Bitcoin protocol, where senders add a voluntary fee to their transactions, and transactions are stored in blocks in order of the highest amount (i.e., first-price auction). In contrast, Ethereum recently switched to the combination of auction-based and posted-price fees [190], where the latter amount is set according to the size of the previous block. These fee mechanisms can stabilize prices to reduce network congestion by making marginal utility (concerning remittances) less volatile.

Prior studies in economics have analyzed and designed these stabilizers. Saito and Iwamura (2019) [191] and Iwamura et al. (2019) [192] present price-stabilization proposals for the Bitcoin protocol, which include performing the difficulty adjustment only when the block interval exceeds a certain threshold.[36] In contrast, studies [193] indicate the advantages of more frequent difficulty adjustments (e.g., *Bitcoin Cash* adjusts the difficulty of every block instead of 2016 blocks). Fee mechanisms are mainly studied by auction theory, and prior studies have recommended introducing a second-price auction [194] or monopolistic auction (collecting the same amount of fees from each transaction in a block) [195], [196] for the Bitcoin protocol. Ethereum's fee mechanism has also been analyzed [197], [198], and design proposals include using bids and the size of previous blocks to calculate posted-price fees [199] and combining second-price auction and burning mechanism [200].

D. How to Stabilize Market Price (Pegging)

A more direct stabilization approach would be to pre-define the exchange ratio between a token and another asset.

The most straightforward scheme is to peg the value of a token with another asset (e.g., one token = 1 USD); such tokens are called *stablecoins*. Stablecoins are generally issued by a centralized custodian that holds the underlying assets as collateral (e.g., *USDT* [201], *PAX Gold* [202]). In contrast, several stablecoins try to peg other assets while ensuring decentralized properties. For example, *DAI stablecoin* [203] is pegged to the USD but collateralized by Ether, where any peer can be a custodian.[37] *Basis* [204] and *TerraUSD* [205] are products classified as *algorithmic stablecoins*, which have no collateral and try to stabilize the price through some mechanism. Unfortunately, neither of the above products worked well (see V-D for the collapse of TerraUSD), and no practical algorithmic stablecoins currently exist. The extant literature provides more details of stablecoin [206], [207].

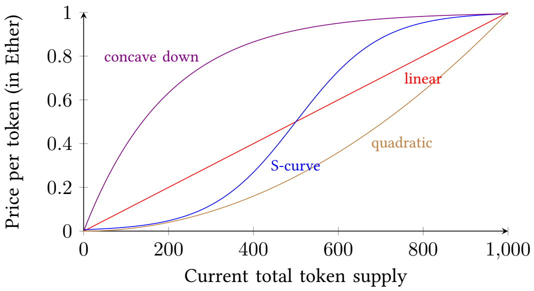


Fig. 5: Token Bonding Curve (TBC)

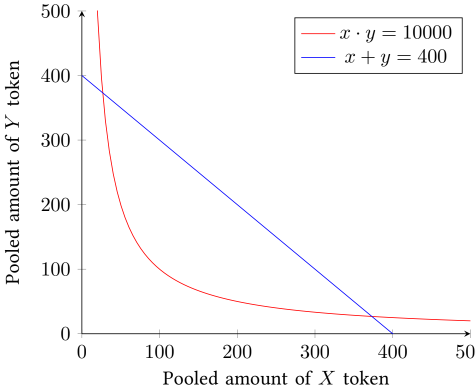


Fig. 6: Automated Market Maker (AMM)

Another scheme is to pre-define rules for exchange ratios. *Token Bonding Curve* (TBC), one of the first such rules for blockchain, was proposed [208]–[210] and implemented [211] in 2017. TBC is a program that mints new tokens by depositing Ether and returns Ether by depositing (burning) the minted tokens, where their exchange ratio (i.e., the price per token in Ether) is determined as a function of the current token supply. This function allows us to exchange tokens without counterparties; in the case of increasing functions (Figure 5), we can also earn Ether by first acquiring tokens and then burning them back to Ether once the supply has increased sufficiently.[38] Moreover, TBC can take another form of *automated market maker* (AMM) [212], which pre-defines the exchange ratio between two tokens as follows:

[35] Kjærland et al. (2018) [189] empirically observed that Bitcoin difficulty adjustment does not affect price fluctuation.

[36] Other proposals are i) making the amount of mining rewards variable, dependent on the results of difficulty adjustment (instead of block-reward halving) and ii) introducing a negative interest rate (depreciation) on all Bitcoins.

[37] This model requires overcollateralization to mitigate the risk of price fluctuations in the collateralized assets. For example, the DAI stablecoin currently requires 1.5 USD worth of Ether collateral to issue one unit of the stablecoin pegged at 1 USD.

[38] TBC essentially employs an increasing function for minting tokens, as decreasing functions offer no incentive to mint tokens initially.

Automated Market Maker (a simple example)

Create a liquidity pool:

- Peers can create a liquidity pool comprising two types of tokens, X and Y.
- A liquidity pool is established when it satisfies the following formula:

$$x \cdot y = k,$$

where x and y denote the pooled amounts of X and Y, respectively; k is a given, fixed value.

Exchange tokens in the liquidity pool:

- Peers can exchange X and Y through the established liquidity pool.
- The exchange ratio is determined so that it maintains the above formula; if a peer tries to exchange Δx of X for Y, they will receive Δy derived from $(x + \Delta x)(y - \Delta y) = k$.[a]

[a] Fees are omitted here for simplicity.

The red curve in Figure 6 depicts the $k = 10,000$ case, where the price of X (in Y) is 1 for $x = 100$, $y = 100$, and 5 for $x = 20$, $y = 500$. This mechanism allows us to exchange tokens without counterparties and provides arbitrage opportunities when a gap exists in the exchange ratio between the liquidity pool and other markets (i.e., AMM can autonomously reach the appropriate relative price). AMM is the core design of current DEXs and continues to be improved through various proposals, including other constraint formulas (e.g., $x+y = k$ depicted by the blue line in Figure 6) and flexible fees [213].[39] The extant literature provides more details [169].

TBC and AMM were developed to increase token liquidity, i.e., to facilitate exchange with other tokens[40]; however, they can also contribute to price stabilization by making the token price predictable.

Prior studies in economics have contributed to stablecoins, particularly dynamic analysis of incentives and expectations [215], [216]. For collateralized stablecoins, the behavior of users [217] and custodians [216], [218] has been studied, by using theoretical models of currency crises [219] and bank runs [220]; These studies generally emphasize the importance of the custodian's *commitment* [221]. For algorithmic stablecoins, their sustainability has been studied [222] while modeling them as a *Ponzi scheme*, reflecting the failure of preceding proposals [223]. Studies on TBC and AMM are mainly focused on formalization, e.g., TBC [224], [225] and AMM [226], [227], and the business side is ahead concerning their design [213], [228].[41] Nontheless, room remains for economics to contribute to their design, given that i) AMM is an application of an *indifference curve* and *marginal rate of substitution* in microeconomics, and ii) the scoring rules [230], [231] underlying BCT and AMM have been merged with game theory to produce various models for information elicitation (III-C).

This section surveyed how blockchain-related products and prior studies have designed token value for autonomy. From an economic perspective, token value can be ensured by marginal cost and marginal utility, and stabilizers must adjust at least one (or pre-define the exchange ratio of tokens). Practical design requires imposing both marginal cost and marginal utility on the tokens.

V. Case Studies

Thus far, we have surveyed consensus-building for decentralization and token value for autonomy; however, as mentioned in Section II, integration is essential for practical design. This section evaluates the five products mentioned above from the integration viewpoint (i.e., whether they cover multiple requirements simultaneously). Table II presents the summary of results.

A. The Bitcoin Protocol

The Bitcoin protocol [1] is a peer-to-peer electronic cash system, the first practical protocol to employ an economic incentive design for consensus-building on transaction records. We have already confirmed its incentive design but briefly review it again here.

For consensus-building, combining proof-of-work and Nakamoto consensus prevents strategic behavior and free-riding. Spamming and Sybil attacks are addressed by transaction fees and proof-of-work, respectively. For token value, the combination of proof-of-work and coinbase stipulates its marginal cost, which increases over time by the block-reward halving and is stabilized (in line with current input computational resources) by the difficulty adjustment. Marginal utility is ensured through peer-to-peer electronic cash; transaction fees may also be included.

Here, a single function has multiple roles (e.g., proof-of-work contributes to preventing strategic behavior and Sybil attacks and ensuring marginal cost), which enables the integration of consensus-building and token value. Regarding integration, the Bitcoin protocol would be a benchmark for other blockchain-related products. Further consideration should be given to other norms, such as scalability, finality, energy efficiency, and voting power (III-D). Furthermore, *governance*—consensus-building on the protocol itself—is also an important issue for the Bitcoin protocol, which will be discussed at the end of this survey (VI-A).

[39] The $x \cdot y = k$ model is sometimes referred to as the *constant product automated market maker* (CPAMM) to distinguish it from other models. CPAMM has become the current standard due to its advantageous feature where neither X nor Y can be zero in the liquidity pool.

[40] Previous DEXs, such as *0x protocol* [214], required finding a counterparty (called a relayer) to exchange tokens. This requirement was a significant obstacle for practical use.

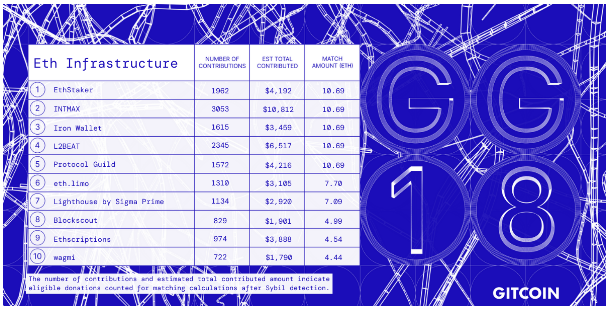
[41] To the author's knowledge, Krishnamachari et al. (2021) [229], which proposed dynamic constraint formula, is a study on the AMM design.

TABLE II: Evaluation of Five Blockchain-related Products

Products & Notes	Consensus-Building for Decentralization			Token Value for Autonomy		
	strategy-proofness	spam & Sybil-proofness	free-riding proofness	marginal cost	marginal utility	stabilizer
The Bitcoin Protocol [1] benchmark of integration	✓	✓	✓	✓	✓	✓
Gitcoin [82] QV at the expense of decentralization		✓ (centralized)	(not required)		✓	
Nouns DAO [51] room for NFT-specific extensions	✓	✓		✓	✓	
Terra [205] lack of marginal cost led to collapse	✓	✓	✓		✓	✓ (collapsed)
Uniswap [170] tokens with unclear raison d'etre	✓	✓		✓ (weak)	✓ (weak)	

B. Gitcoin

Gitcoin [82] is a DApp on Ethereum, where peers can pool any amount of Ether (or stablecoins) to donate the listed open source projects. Gitcoin is not entirely DAO (at the time of this writing), as a management team evaluates which proposals should be listed. Conversely, it adopts a decentralized consensus-building on redistributing pooled assets among listed projects.



Eth Infrastructure		NUMBER OF CONTRIBUTIONS	EST TOTAL CONTRIBUTED	MATCH AMOUNT (ETH)
1	EthStaker	1962	$4,192	10.69
2	INTMAX	3053	$10,812	10.69
3	Iron Wallet	1615	$3,459	10.69
4	L2BEAT	2345	$6,517	10.69
5	Protocol Guild	1572	$4,216	10.69
6	eth.limo	1310	$3,105	7.70
7	Lighthouse by Sigma Prime	1134	$2,920	7.09
8	Blockscout	829	$1,901	4.99
9	Ethscriptions	974	$3,888	4.54
10	wagmi	722	$1,790	4.44

The number of contributions and estimated total contributed amount indicate eligible donations counted for matching calculations after Sybil detection.

Fig. 7: Result of Gitcoin Grants Round 18

Source: Gitcoin Grants Round 18: Results and Recap (https://www.gitcoin.co/blog/gitcoin-grants-round-18-results-and-recap, accessed November 8, 2023).

For consensus-building, Gitcoin adopts QV (III-D) as a counter to the one CPU or one token = one vote norm[42]; however, QV is vulnerable to collusion (strategic behavior) and Sybil attacks [232] because the same token amount increases voting power with the number of holders. Aside from collusion, Sybil attacks are prevented by *Gitcoin Passport* [233] in which a management team requires each user to submit one or more social media accounts and pay a certain amount of tokens, guaranteeing as much one-to-one correspondence between addresses and individuals as possible. Figure 7 shows some of the results of the latest round of grant programs after QV and Sybil detection (by Gitcoin Passport). The management team prevents spamming, and the free-riding proof is not required here because Gitcoin is a platform for donations. To be DAO, Gitcoin issued Gitcoin Token (GCT) in 2021.[43] GCT appears to have no marginal cost for token value as it is a pre-mined token. Marginal utility relates to Gitcoin Passport and governance. Peers can increase the identity score of Gitcoin Passport by staking their GCT. The governance feature is under development, but a QV using GCT will likely be implemented to decide how to improve Gitcoin. The value of GCT has no stabilizer.

Overall, Gitcoin is a case of introducing a new QV norm at the expense of some decentralization. The risk of collusion remains even if we can ensure one-to-one correspondence between user addresses and individuals. Gitcoin tries to make quadratic voting and decentralized autonomous property compatible through the issuance of GCT; however, as it lacks a strategy-proof, marginal cost, and stabilizer design, GCT does not contribute much to the purpose (at least for now).

C. Nouns DAO

Nouns DAO [51] is another DApp on Ethereum that i) automatically generates a new NFT named *Noun* (Figure 4) every once a day. ii) Noun is automatically listed to the daily auction, which every peer can bid with Ether. iii) Noun holders can use pooled Ether to make Nouns more widespread (e.g., create T-shirts, pay to developers).[44] Since there is no centralized marketing manager, Nouns DAO needs a consensus-building among Noun holders on how to use the pooled Ether.

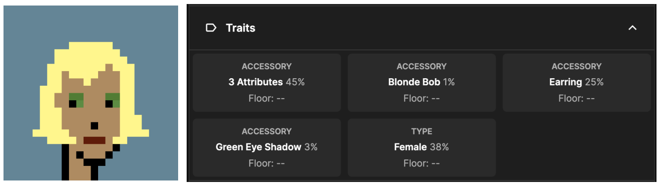
For consensus-building, Nouns DAO adopts the token-voting mentioned above (III-A). Peers can vote for three choices (*for*, *against*, *abstain*) of the proposal with Nouns, and this action carries no penalty or reward (Figure 9a). Strategic behavior, spamming and Sybil attacks are prevented by this token-voting (albeit the risk of Keynesian beauty contest), but free-riding remains due to the lack of rewards. Consensus-building is currently driven by the enthusiasm of Nouns

[42] To be precise, Gitcoin applies QV to fund allocation rather than voting, a method referred to as *quadratic funding* [142].

[43] https://etherscan.io/address/0xde30da39c46104798bb5aa3fe8b9e0e1f348163f, [Accessed 20-11-2023]

[44] For the first five years, every tenth Noun auction is skipped, and the Nouns are automatically sent to the core developers. This mechanism serves as an incentive for the core developers, in lieu of pre-mined tokens.

holders.[45] For token value, marginal cost is equivalent to the winning bid (Ether) in the daily auction, which is determined by the market. As mentioned in IV-B, marginal utility exists as both an art and a governance token. There is no stabilizer for the value of Nouns.



ACCESSORY
3 Attributes 45%
Floor: --

ACCESSORY
Blonde Bob 1%
Floor: --

ACCESSORY
Earring 25%
Floor: --

ACCESSORY
Green Eye Shadow 3%
Floor: --

TYPE
Female 38%
Floor: --

Fig. 8: Stochastic Rarity of NFT collections (*CryproPunks*)

Source: OpenSea.io (https://opensea.io/assets/ethereum/0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb/0, accessed November 8, 2023).

Nouns DAO, especially the idea of leveraging NFTs and daily auctions, is well-designed but does not address free-riding and lacks a stabilizer. The author has two opinions on these issues. First, adjusting the Nouns' rarity could solve free-riding. Most NFT collections automatically generate groups of NFTs through programs that stochastically determine the traits of each part (Figure 8); NFTs with rare traits tend to have higher market prices [234]. Nouns are generated in the same way, but their stochastic elements are all uniformly distributed (i.e., there is no rarity in Nouns).[46] Here, the more a Noun is used in voting, the less likely its traits appear in the series of future Nouns. This function would encourage Noun holders to participate in consensus-building. Second, adjusting the auction frequency could be a stabilizer. Nouns are currently generated once a day, but adjusting this frequency according to the previous winning bid (i.e., more frequent with higher bids, less frequent with lower bids) would help stabilize the marginal cost of Nouns.[47] These NFT-specific extensions would make Nouns DAO more robust.[48]

D. Terra

Terra [205] is a protocol for algorithmic stablecoins, where peers can build consensus on pegging and transaction records. Terra consists of two tokens: TerraUSD (UST) and LUNA[49]; the former is a stablecoin, and the latter is a coinbase for consensus-building on UST's transaction records. LUNA works to stabilize UST prices by guaranteeing the exchange of one UST for one USD worth of LUNA. If the market price of one UST falls below 1 USD, arbitrageurs can obtain profit by exchanging one UST for LUNA, which stabilizes the UST price because Terra burns received UST and mints LUNA (and vice versa).[50] That is, the UST price is intended to be stable indirectly through the supply adjustment of LUNA.[51]

For consensus-building, Terra, as a protocol, adopts proof-of-stake (LUNA), Nakamoto consensus, and coinbase (LUNA). The combination of proof-of-stake and Nakamoto consensus addresses strategic behavior and free-riding. Spamming and Sybil attacks are prevented by the transaction fee (UST) and proof-of-stake. For token value, LUNA has no marginal cost because it is minted automatically through exchange with UST and proof-of-stake based consensus-building.[52] Marginal demand seems to be ensured by staking, i.e., peers can obtain LUNA (as coinbase) and UST (as transaction fee) due to consensus-building. In addition to the above-mentioned UST-LUNA exchange, Terra has several stabilizers to make UST an algorithmic stablecoin; these include adjusting the amount of coinbase, transaction fees, and the burn rate of UST after exchange.

Terra appears to be well-designed, referring to the Bitcoin protocol; however, this protocol collapsed in 2022 due to the inability to maintain the peg between UST and USD. Once the price of 1 UST fell below 1 USD, the demand for exchange into LUNA surged, and in response, new LUNA was minted, which lowered the price of LUNA, making it difficult to exchange for the equivalent of 1 USD, further lowering the price of UST, and so on in a death spiral. Several studies [236]–[238] empirically analyzed this incident, but from a design perspective, the fundamental problem is the lack of marginal costs in minting LUNA despite its use for price stabilization.

E. Uniswap

Uniswap [170] is also a DApp on Ethereum,[53] where peers can exchange tokens without a centralized entity (DEX). In 2020, Uniswap began minting and distributing UNI, a governance token, to several types of users including liquidity providers [81].[54] Apart from AMM (Figure 6), we review the governance of Uniswap using UNI tokens.

Uniswap adopts token-voting with UNI for consensus-building, similar to that of Nouns DAO (Figure 9b); thus,

[45] Nouns DAO employs a proxy voting system to mitigate low voter turnout; however, there are no rewards allocated for proxy voters.

[46] Nouns DAO generates pseudo-random numbers using the hash number of the previous block and the Nouns ID. More details can be found in the smart contract code at Etherscan. https://etherscan.io/address/0xCC8a0FB5ab3C7132c1b2A0109142Fb112c4Ce515#code

[47] This design is inspired by the difficulty adjustment. It would also be worth considering to reduce the auction frequency over time, similar to Bitcoin's block-reward halving, to increase the marginal cost.

[48] Recently, a fork occurred in Nouns DAO [235], which implies the difficulty of designing decentralized autonomous consensus-building.

[49] Terra issued stablecoins pegged to multiple currencies, although only USD is mentioned here for convenience.

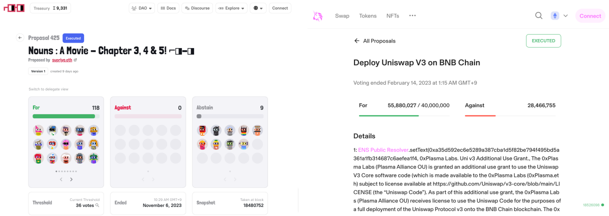
[50] In cases where LUNA is exchanged for UST, Terra only burns a portion of the received LUNA.

[51] It is presumed that these tokens are named after the celestial phenomenon of the moon orbiting the Earth, symbolizing a balance similar to that of gravitational forces.

[52] The marginal cost of a token minted with proof-of-stake is the opportunity cost incurred by rendering the staked token unusable. For example, staking Ether means losing the opportunity to use it for DApps. However, since LUNA's utility is the staking itself, there is no such opportunity cost, resulting in no marginal cost for the new mintage of LUNA.

[53] "Uniswap is now usable on several protocols, including Ethereum, *Polygon*, *Optimism*, *Arbitrum*, and *BNB Chain*.

[54] https://etherscan.io/address/0x1f9840a85d5af5bf1d1762f925bdaddc4201f984



Proposal 425

Nouns : A Movie – Chapter 3, 4 & 5! ⌐◨-◨

Proposed by supriyo.eth

For	Against	Abstain
118	0	9

Threshold: Current Threshold 36 votes

Ended: 10:29 AM GMT+9 November 6, 2023

Snapshot: Taken at block 18480752

(a) Nouns DAO

Deploy Uniswap V3 on BNB Chain

Voting ended February 14, 2023 at 1:15 AM GMT+9

For		Against	
	55,880,027 / 40,000,000		28,466,755

Details

1: ENS Public Resolver.setText(0xa35d592ec6e5289a387cba1d5f82be794f495bd5a361a1fb314687c6aefea1f4, 0xPlasma Labs. Uni v3 Additional Use Grant., The 0xPlasma Labs (Plasma Alliance OU) is granted an additional use grant to use the Uniswap V3 Core software code (which is made available to the 0xPlasma Labs (0xPlasma.eth) subject to license available at https://github.com/Uniswap/v3-core/blob/main/LICENSE (the "Uniswap Code"). As part of this additional use grant, the 0xPlasma Labs (Plasma Alliance OU) receives license to use the Uniswap Code for the purposes of a full deployment of the Uniswap Protocol v3 onto the BNB Chain blockchain. The 0x

(b) Uniswap

Fig. 9: Voting with Governance Token

Sources: (a) Nouns : A Movie - Chapter 3, 4 & 5! (https://nouns.wtf/vote/425, accessed November 8, 2023), (b) Deploy Uniswap V3 on BNB Chain (https://app.uniswap.org/vote/2/31, accessed November 8, 2023).

strategic behavior, spamming and Sybil attacks are prevented but the risk of free-riding still exists. Some studies [239], [240] indicate low voter turnout in the governance of Uniswap and other DEXs. For token value, part of the marginal cost would be the opportunity cost of liquidity providing minus the reward through LP tokens (IV-B), given that UNI is periodically distributed to liquidity providers even after initial distribution.[55] Marginal utility is, for now, only the right to participate in governance. There is no stabilizer for the value of UNI.

Uniswap is a representative DEX based on AMM, but its governance using UNI has free-riding challenges, a lack of stabilizer, and weak token value (i.e., weak marginal cost and marginal utility). For the first two challenges, leveraging prior studies and products presented in III-C and IV-C would be helpful. For the last challenge, Uniswap must increases at least the marginal cost or utility of UNI. A straightforward way would be to increase marginal utility by distributing a portion of the exchange fee to LP and UNI token holders (this extension, called a *fee switch*, has long been controversial in Uniswap governance [241], [242]); however, the question arises whether UNI is necessary in the first place. By analogy with stocks, we could design a simpler consensus-building if LP tokens were governance tokens. Frankly, the raison d'etre of UNI is unclear.[56]

VI. Conclusion

This paper surveyed products and studies behind cryptoeconomics and tokenomics from an economic perspective, which aims to bridge the economic and blockchain contexts. Our survey first organized the history of each term in chronological order, suggesting that cryptoeconomics and tokenomics can be novel when integrated (Section II). We then surveyed blockchain-related products and prior studies on designing consensus-building for decentralization (Section III) and designing token value for autonomy (Section IV), respectively. The former is a category related to cryptoeconomics, and the latter is to tokenomics. Finally, from the integration viewpoint, we evaluated five products as a case study (Section V).

These attempts illustrated the importance and difficulty of integration. Decentralized autonomous consensus-building requires at least simultaneous consideration of strategic behavior, spamming, Sybil attack, free-riding, marginal cost, marginal utility, and stabilizer. This task is complex and challenging for both research and implementation. This survey aims to alleviate this difficulty as a first step in bridging the contexts of economics and blockchain.

Finally, two problems are worth mentioning for future research.

A. How to Control External Incentives

Incentives outside the mechanism can also influence consensus-building. For example, the Bitcoin protocol can be attacked even by peers who earn Bitcoin (coinbase) because there remains an incentive to lower the price of Bitcoin as long as they can short-sell on external exchanges (*Goldfinger attack* [245]). The application layer has recently influenced Ethereum (consensus-building at the protocol layer), as DEXs have created new revenue opportunities through reordering transactions within blocks (*maximal extractable value*[57]; MEV [246]). Furthermore, governance issues are essential for protocols. The Bitcoin protocol and Ethereum have experienced multiple blockchain splits (i.e., intended hard forks) due to the failure of consensus-building on the protocol design itself [247].

B. How to Alleviate Rationality

This survey consistently assumed that peers are rational, i.e., they act to maximize the expect amount of reward tokens (of sufficient value); however, consensus-building would be more robust and practical if it were not always considered rational. Prior studies on *behavioral economics* may be helpful to this perspective. Behavioral economics is already being applied to blockchain-related discussions, from market analysis [248] to DApps design [249], and synergies with cryptoeconomics have also been noted [250].

Addressing these open problems will be necessary to design decentralized autonomous consensus-building.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[55] Uniswap describes its periodic distribution of rewards as *liquidity mining*. Note that the opportunity cost of the liquidity mining includes the risk of impermanent loss. Impermanent loss refers to the potential loss a liquidity provider may incur due to fluctuations in the token ratio within the liquidity pool.

[56] In reality, the mintage of UNI tokens was a response to a *vampire attack*. This type of attack involves copying an open-source project and then trying to divert its resources by offering higher incentives. In 2020, Sushiswap [243], a clone of Uniswap, tried to attract a significant portion of Uniswap's liquidity by distributing its governance token, SUSHI. As a countermeasure, Uniswap was compelled to mint its own governance tokens, despite the unclear raison d'etre. See Fan et al. (2023) [244] for more details on this incident.

[57] The term was originally *miner extractable value*, but this terminology has become outdated since the adoption of proof-of-stake in Ethereum led to the disappearance of miners.

[2] W. Dai, “B-money,” 1998.

[3] N. Szabo, “Bit gold,” *Recuperado de https://nakamotoinstitute. org/bit-gold/TVer página*, 2005.

[4] F. Brunton, *Digital cash: The unknown history of the anarchists, utopians, and technologists who created cryptocurrency.* Princeton University Press, 2020.

[5] A. Gladstein, “The quest for digital cash,” Bitcoin Magazine - Bitcoin News, Articles and Expert Insights, 10 2021. [Online]. Available: https://bitcoinmagazine.com/culture/bitcoin-adam-back-and-digital-cash

[6] C. Dwork and M. Naor, “Pricing via processing or combatting junk mail,” in *Annual International Cryptology Conference.* Springer, 1992, pp. 139–147.

[7] M. Jakobsson and A. Juels, “Proofs of work and bread pudding protocols,” in *Secure information networks.* Springer, 1999, pp. 258–272.

[8] V. Buterin *et al.*, “Ethereum: A next-generation smart contract and decentralized application platform,” vol. 7, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper

[9] G. Wood *et al.*, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[10] D. Johnston, S. O. Yilmaz, J. Kandah, N. Bentenitis, F. Hashemi, R. Gross, S. Wilkinson, and S. Mason, “Thegeneraltheoryofdecentralizedapplications, dapps,” 2014.

[11] C. Jentzsch, “Decentralized autonomous organization to automate governance,” *White paper, November*, 2016.

[12] V. Buterin *et al.*, “A next-generation smart contract and decentralized application platform,” *white paper*, vol. 3, no. 37, 2014.

[13] V. Buterin, “Bootstrapping a decentralized autonomous corporation: part i,” *Bitcoin Magazine*, vol. 19, 2013.

[14] F. Santos and V. Kostakis, “The dao: a million dollar lesson in blockchain governance,” *School of Business and Governance, Ragnar Nurkse Department of Innovation and Governance*, 2018.

[15] R. Morrison, N. C. Mazey, and S. C. Wingreen, “The dao controversy: the case for a new species of corporate governance?” *Frontiers in Blockchain*, vol. 3, p. 25, 2020.

[16] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, “Decentralized autonomous organizations: Concept, model, and applications,” *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 870–878, 2019.

[17] Y. El Faqir, J. Arroyo, and S. Hassan, “An overview of decentralized autonomous organizations on the blockchain,” in *Proceedings of the 16th international symposium on open collaboration*, 2020, pp. 1–8.

[18] Q. Ding, D. Liebau, Z. Wang, and W. Xu, “A survey on decentralized autonomous organizations (daos) and their governance,” *Available at SSRN 4378966*, 2023.

[19] J. Poon and T. Dryja, “The bitcoin lightning network,” *Scalable off-chain instant payments*, pp. 20–46, 2015.

[20] S. Voshmgir, M. Zargham *et al.*, “Foundations of cryptoeconomic systems,” *Research Institute for Cryptoeconomics, Vienna, Working Paper Series/Institute for Cryptoeconomics/Interdisciplinary Research*, vol. 1, 2019.

[21] K. Ito, “Contributed report: Cryptoeconomics as an academic discipline through a survey of previous studies (kikou report: Senkou-kenkyuu wo tooshite kangaeru gakumon to shite no cryptoeconomics),” Dec 2018. [Online]. Available: https://hashhub-research.com/articles/2018-12-23-cryptoeconomics-from-academic-view

[22] “Home — The Ethereum Foundation — ethereum.foundation,” https://ethereum.foundation/, [Accessed 22-11-2023].

[23] V. Zamfir, “What is cryptoeconomics?” www.youtube.com, 02 2015. [Online]. Available: https://www.youtube.com/watch?v=9lw3s7iGUXQ

[24] V. Buterin, “Visions, part 1: The value of blockchain technology,” Ethereum Foundation Blog, 04 2015. [Online]. Available: https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology

[25] ——, “Introduction to cryptoeconomics - vitalik buterin,” YouTube, 02 2017. [Online]. Available: https://www.youtube.com/watch?v=pKqdjaH1dRo

[26] ——, “Schellingcoin: A minimal-trust universal data feed,” Mar 2014. [Online]. Available: https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed

[27] S. Davidson, P. De Filippi, and J. Potts, “Economics of blockchain,” *Available at SSRN 2744751*, 2016.

[28] T. Obasi, *The Economics of Cryptocurrency. Incentivizing Decentralisation*, 2017. [Online]. Available: https://www.grin.com/document/435228

[29] J. K. Brekke and W. Z. Alsindi, “Cryptoeconomics,” *Internet Policy Review*, vol. 10, no. 2, 2021.

[30] S. Au and T. Power, *Tokenomics: The crypto shift of blockchains, ICOs, and tokens.* Packt Publishing Ltd, 2018.

[31] W. Mougayar, “Startup management tokenomics – a business guide to token usage, utility and value,” Startupmanagement.org, 06 2017. [Online]. Available: http://startupmanagement.org/2017/06/10/tokenomics-a-business-guide-to-token-usage-utility-and-value/

[32] J. P. Ennis, J. Waugh, and W. Weaver, “Three definitions of tokenomics,” www.coindesk.com, 03 2018. [Online]. Available: https://www.coindesk.com/markets/2018/03/17/three-definitions-of-tokenomics/

[33] S. Blémus and D. Guégan, “Initial crypto-asset offerings (icos), tokenization and corporate governance,” *Capital Markets Law Journal*, vol. 15, no. 2, pp. 191–223, 2020.

[34] S. Kampakis, “Auditing tokenomics: A case study and lessons from auditing a stablecoin project,” *The Journal of The British Blockchain Association*, p. 34696, 2022.

[35] J. Fischer and R. N. Wright, “An application of game-theoretic techniques to cryptography,” *Discrete Mathematics and Theoretical Computer Science*, vol. 13, pp. 99–118, 1993.

[36] J. Katz, “Bridging game theory and cryptography: Recent results and future directions,” in *Theory of Cryptography Conference.* Springer, 2008, pp. 251–272.

[37] N. Nisan and A. Ronen, “Algorithmic mechanism design,” in *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, 1999, pp. 129–140.

[38] ——, “Algorithmic mechanism design,” *Games and Economic behavior*, vol. 35, no. 1-2, pp. 166–196, 2001.

[39] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic game theory.* Cambridge university press, 2007.

[40] J. Feigenbaum, C. Papadimitriou, and S. Shenker, “Sharing the cost of muliticast transmissions (preliminary version),” in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, 2000, pp. 218–227.

[41] J. Feigenbaum and S. Shenker, “Distributed algorithmic mechanism design: Recent results and future directions,” in *Current Trends in Theoretical Computer Science: The Challenge of the New Century Vol 1: Algorithms and Complexity Vol 2: Formal Models and Semantics.* World Scientific, 2004, pp. 403–434.

[42] A. Marshall, “The principles of economics,” McMaster University Archive for the History of Economic Thought, Tech. Rep., 1890.

[43] J. Handa, *Monetary economics.* Routledge, 2008.

[44] M. Rubinstein, *A history of the theory of investments: My annotated bibliography.* John Wiley & Sons, 2011, vol. 335.

[45] J. P. Conley *et al.*, “Blockchain and the economics of crypto-tokens and initial coin offerings,” *Vanderbilt University Department of economics working papers*, no. 17-00008, 2017.

[46] J. B. Taylor, “A historical analysis of monetary policy rules,” in *Monetary policy rules.* University of Chicago Press, 1999, pp. 319–348.

[47] M. Raskin and D. Yermack, “Digital currencies, decentralized ledgers, and the future of central banking,” National Bureau of Economic Research, Tech. Rep., 2016.

[48] M. R. Hoffman, L.-D. Ibáñez, and E. Simperl, “Toward a formal scholarly understanding of blockchain-mediated decentralization: A systematic review and a framework,” *Frontiers in Blockchain*, vol. 3, p. 35, 2020.

[49] L. Zhang, X. Ma, and Y. Liu, “Sok: Blockchain decentralization,” *arXiv preprint arXiv:2205.04256*, 2022.

[50] L. LAMPORT, R. SHOSTAK, and M. PEASE, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[51] “Nouns DAO — nouns.wtf,” https://nouns.wtf/, [Accessed 31-10-2023].

[52] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” *self-published paper, August*, vol. 19, no. 1, 2012.

[53] V. Buterin, D. Hernandez, T. Kamphefner, K. Pham, Z. Qiao, D. Ryan, J. Sin, Y. Wang, and Y. X. Zhang, “Combining ghost and casper,” *arXiv preprint arXiv:2003.03052*, 2020.

[54] U. Pavloff, Y. Amoussou-Guenou, and S. Tucci-Piergiovanni, “Ethereum proof-of-stake under scrutiny,” in *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 2023, pp. 212–221.

[55] D. C. Parkes, “On learnable mechanism design,” in *Collectives and the design of complex systems*. Springer, 2004, pp. 107–131.

[56] A. Dasgupta and A. Ghosh, “Crowdsourced judgement elicitation with endogenous proficiency,” in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 319–330.

[57] E. Tardos and V. V. Vazirani, “Basic solution concepts and computational issues,” *Algorithmic game theory*, pp. 3–28, 2007.

[58] W. Vickrey, “Counterspeculation, auctions, and competitive sealed tenders,” *The Journal of finance*, vol. 16, no. 1, pp. 8–37, 1961.

[59] E. H. Clarke, “Multipart pricing of public goods,” *Public choice*, pp. 17–33, 1971.

[60] T. Groves, “Incentives in teams,” *Econometrica: Journal of the Econometric Society*, pp. 617–631, 1973.

[61] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, “A survey on applications of game theory in blockchain,” *arXiv preprint arXiv:1902.10865*, 2019.

[62] H. Halaburda, G. Haeringer, J. Gans, and N. Gandal, “The microeconomics of cryptocurrencies,” *Journal of Economic Literature*, vol. 60, no. 3, pp. 971–1013, 2022.

[63] M. Warren, *Bitcoin: A Game-Theoretic Analysis*. Walter de Gruyter GmbH & Co KG, 2023.

[64] F. Saleh, “Blockchain without waste: Proof-of-stake,” *The Review of financial studies*, vol. 34, no. 3, pp. 1156–1190, 2021.

[65] X. Chen, C. Papadimitriou, and T. Roughgarden, “An axiomatic approach to block rewards,” in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 124–131.

[66] J. D. Leshno and P. Strack, “Bitcoin: An axiomatic approach and an impossibility theorem,” *American Economic Review: Insights*, vol. 2, no. 3, pp. 269–286, 2020.

[67] J. M. Keynes, “The general theory of employment,” *The quarterly journal of economics*, vol. 51, no. 2, pp. 209–223, 1937.

[68] R. Marx and M. Lehmann-Waffenschmidt, “The keynesian beauty contest revisited,” *Journal of Economic Behavior & Organization*, vol. 204, pp. 164–181, 2022.

[69] H. Moulin, *Game theory for the social sciences*. NYU press, 1986.

[70] R. Nagel, “Unraveling in guessing games: An experimental study,” *The American economic review*, vol. 85, no. 5, pp. 1313–1326, 1995.

[71] “The P + epsilon Attack — Ethereum Foundation Blog — blog.ethereum.org,” https://blog.ethereum.org/2015/01/28/p-epsilon-attack, [Accessed 13-11-2023].

[72] A. Asgaonkar and B. Krishnamachari, “Token curated registries-a game theoretic approach,” *arXiv preprint arXiv:1809.01756*, 2018.

[73] Y. L. Wang and B. Krishnamachari, “Enhancing engagement in token-curated registries via an inflationary mechanism,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 188–191.

[74] G. Tsoukalas and B. H. Falk, “Token-weighted crowdsourcing,” *Management Science*, vol. 66, no. 9, pp. 3843–3859, 2020.

[75] J. Mehta, C. Starmer, and R. Sugden, “The nature of salience: An experimental investigation of pure coordination games,” *The American Economic Review*, vol. 84, no. 3, pp. 658–673, 1994.

[76] T. C. Schelling, *The Strategy of Conflict: with a new Preface by the Author*. Harvard university press, 1980.

[77] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, “A bayesian approach to filtering junk e-mail,” in *Learning for Text Categorization: Papers from the 1998 workshop*, vol. 62. Madison, Wisconsin, 1998, pp. 98–105.

[78] P. Hayati, V. Potdar, A. Talevski, N. Firoozeh, S. Sarenche, and E. A. Yeganeh, “Definition of spam 2.0: New spamming boom,” in *4th IEEE International Conference on Digital Ecosystems and Technologies*. IEEE, 2010, pp. 580–584.

[79] J. R. Douceur, “The sybil attack,” in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[80] A. Back *et al.*, “Hashcash-a denial of service counter-measure,” 2002.

[81] “Introducing UNI — blog.uniswap.org,” https://blog.uniswap.org/uni, [Accessed 08-11-2023].

[82] “Gitcoin,” www.gitcoin.co, 2017. [Online]. Available: https://www.gitcoin.co/

[83] “Worldcoin,” www.worldcoin.org, 2023. [Online]. Available: https://worldcoin.org/

[84] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, “Decentralized identity: Where did it come from and where is it going?” *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019.

[85] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, “Decentralized identifiers (dids) v1. 0,” *Draft Community Group Report*, 2020.

[86] I. Androutsopoulos, E. F. Magirou, and D. K. Vassilakis, “A game theoretic model of spam e-mailing.” in *CEAS*, 2005.

[87] E. Reshef and E. Solan, “The effects of anti-spam methods on spam mail,” in *3rd Conference on Email and Anti-Spam, Mountain View, ca*, 2006.

[88] J. M. Rao and D. H. Reiley, “The economics of spam,” *Journal of Economic Perspectives*, vol. 26, no. 3, pp. 87–110, 2012.

[89] R. Gatti, S. Lewis, A. Ozment, T. Rayna, and A. Serjantov, “Sufficiently secure peer-to-peer networks,” in *Workshop on the Economics of Information Security*, 2004.

[90] N. B. Margolin and B. N. Levine, “Informant: Detecting sybils using incentives,” in *International Conference on Financial Cryptography and Data Security*. Springer Berlin Heidelberg Berlin, Heidelberg, 2007, pp. 192–207.

[91] B. Kumar and B. Bhuyan, “Game theoretical defense mechanism against reputation based sybil attacks,” *Procedia Computer Science*, vol. 167, pp. 2465–2477, 2020.

[92] A. K. Samanta and N. Chaki, “A game-based approach for mitigating the sybil attacks on blockchain applications,” in *International Conference on Computer Information Systems and Industrial Management*. Springer, 2023, pp. 108–123.

[93] F. Stodt and C. Reich, “Introducing a fair tax method to harden industrial blockchain applications against network attacks: A game theory approach,” *Computers*, vol. 12, no. 3, p. 64, 2023.

[94] B. N. Levine, C. Shields, and N. B. Margolin, “A survey of solutions to the sybil attack,” *University of Massachusetts Amherst, Amherst, MA*, vol. 7, p. 224, 2006.

[95] L. Ramaswamy and L. Liu, “Free riding: A new challenge to peer-to-peer file sharing systems,” in *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE, 2003, pp. 10–pp.

[96] R. Hardin and G. Cullity, “The free rider problem,” 2003.

[97] K. Ito, “Consensus-building on citations in peer-to-peer systems,” *Available at SSRN 3936833*, 2021.

[98] M. Thum, “The economic cost of bitcoin mining,” in *CESifo Forum*, vol. 19, no. 1. München: ifo Institut-Leibniz-Institut für Wirtschaftsforschung an der …, 2018, pp. 43–45.

[99] J. Soria, “Tullock contest: A model of proof-of-work mining in cryptocurrencies,” *Available at SSRN 3561146*, 2020.

[100] G. Tullock, “The welfare costs of tariffs, monopolies, and theft,” *Economic inquiry*, vol. 5, no. 3, pp. 224–232, 1967.

[101] B. Faltings and G. Radanovic, *Game Theory for Data Science: Eliciting Truthful Information*. Morgan & Claypool Publishers, 2017.

[102] B. Faltings, “Game-theoretic mechanisms for eliciting accurate information,” www.ijcai.org, p. 6601–6609, 08 2023. [Online]. Available: https://www.ijcai.org/proceedings/2023/740

[103] D. Prelec, “A bayesian truth serum for subjective data,” *science*, vol. 306, no. 5695, pp. 462–466, 2004.

[104] N. Miller, P. Resnick, and R. Zeckhauser, “Eliciting informative feedback: The peer-prediction method,” *Management Science*, vol. 51, no. 9, pp. 1359–1373, 2005.

[105] V. Shnayder, A. Agarwal, R. Frongillo, and D. C. Parkes, “Informed truthfulness in multi-task peer prediction,” in *Proceedings of the 2016 ACM Conference on Economics and Computation*, 2016, pp. 179–196.

[106] N. Goel, A. Filos-Ratsikas, and B. Faltings, “Peer-prediction in the presence of outcome dependent lying incentives,” in *29th International Joint Conference on Artificial Intelligence-Pacific Rim International Conference on Artificial Intelligence, 2020*. International Joint Conferences on Artificial Intelligence Organization, 2020, pp. 124–131.

[107] N. Goel, C. Van Schreven, A. Filos-Ratsikas, and B. Faltings, “Infochain: a decentralized, trustless and transparent oracle on blockchain,” in *Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence*, 2021, pp. 4604–4610.

[108] M. H. Moti, D. Chatzopoulos, P. Hui, B. Faltings, and S. Gujar, “Orthos: A trustworthy ai framework for data acquisition,” in *International Workshop on Engineering Multi-Agent Systems*, 2020, pp. 100–118.

[109] K. Ito and H. Tanaka, “Token-curated registry with citation graph,” *Ledger*, vol. 4, 2019.

[110] Y. Cai, G. Fragkos, E. E. Tsiropoulou, and A. Veneris, “A truth-inducing sybil resistant decentralized blockchain oracle,” in *2020 2nd Conference*

on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, 2020, pp. 128–135.

[111] A. B. Bondi, "Characteristics of scalability and their impact on performance," in *Proceedings of the 2nd international workshop on Software and performance*, 2000, pp. 195–203.

[112] "visa.co.uk," https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf, 2018, [Accessed 23-11-2023].

[113] M. Bedawala and A. Wijeyekoon, "Visa Crypto Thought Leadership – A deep dive on Solana — usa.visa.com," https://usa.visa.com/solutions/crypto/deep-dive-on-solana.html, 2023, [Accessed 23-11-2023].

[114] R. Linus and L. George, "Zerosync: Introducing validity proofs to bitcoin," 2023.

[115] "Arbitrum: Blockchain-based Arbitration — Princeton Bitcoin seminar final project — youtube.com," https://www.youtube.com/live/BpzrLOk4Zy0?si=SK0hUelnIYAj1mHP, 2015, [Accessed 24-11-2023].

[116] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1353–1370.

[117] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct {Non-Interactive} zero knowledge for a von neumann architecture," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 781–796.

[118] J.-J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, and S. Guillou, "How to explain zero-knowledge protocols to your children," in *Conference on the Theory and Application of Cryptology*. Springer, 1989, pp. 628–631.

[119] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A survey on zero-knowledge proof in blockchain," *IEEE network*, vol. 35, no. 4, pp. 198–205, 2021.

[120] V. Buterin, "An Incomplete Guide to Rollups — vitalik.ca," https://vitalik.ca/general/2021/01/05/rollup.html, 2021, [Accessed 28-11-2023].

[121] ——, "An approximate introduction to how zk-SNARKs are possible — vitalik.ca," https://vitalik.ca/general/2021/01/26/snarks.html, 2021, [Accessed 14-11-2023].

[122] A. Altarawneh, T. Herschberg, S. Medury, F. Kandah, and A. Skjellum, "Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 0727–0736.

[123] T. Nakai, A. Sakurai, H. Shiori, and K. Shudo, "The blockchain trilemma described by a formula," *Proc. 6th IEEE Int'l Conf. on Blockchain (IEEE Blockchain 2023)*, 2023.

[124] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, p. 103232, 2021.

[125] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, 2022.

[126] "What is finality in blockchain, and why does it matter? — cointelegraph.com," https://cointelegraph.com/explained/what-is-finality-in-blockchain-and-why-does-it-matter, [Accessed 15-11-2023].

[127] A. De Vries, "Bitcoin's growing energy problem," *Joule*, vol. 2, no. 5, pp. 801–805, 2018.

[128] "Bitcoin Hashrate Chart — bitinfocharts.com," https://bitinfocharts.com/comparison/bitcoin-hashrate.html#alltime, [Accessed 31-10-2023].

[129] C. Stoll, L. Klaaßen, and U. Gallersdörfer, "The carbon footprint of bitcoin," *Joule*, vol. 3, no. 7, pp. 1647–1661, 2019.

[130] M. Khazzaka, "Bitcoin: Cryptopayments energy efficiency," *Journal of Insurance and Financial Management*, vol. 7, no. 3, 2022.

[131] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," *July 7th*, vol. 1, no. 6, 2013.

[132] N. Shibata, "Proof-of-search: combining blockchain consensus formation with solving optimization problems," *IEEE Access*, vol. 7, pp. 172 994–173 006, 2019.

[133] N. Z. Benisi, M. Aminian, and B. Javadi, "Blockchain-based decentralized storage networks: A survey," *Journal of Network and Computer Applications*, vol. 162, p. 102656, 2020.

[134] M. I. Khalid, I. Ehsan, A. K. Al-Ani, J. Iqbal, S. Hussain, S. S. Ullah *et al.*, "A comprehensive survey on blockchain-based decentralized storage networks," *IEEE Access*, 2023.

[135] J. Benet and N. Greco, "Filecoin: A decentralized storage network," *Protoc. Labs*, vol. 1, pp. 1–36, 2018.

[136] S. Williams, V. Diordiiev, L. Berman, and I. Uemlianin, "Arweave: A protocol for economically sustainable information permanence," *arweave. org, Tech. Rep*, 2019.

[137] D. Vorick and L. Champine, "Sia: Simple decentralized storage," *Retrieved May*, vol. 8, p. 2018, 2014.

[138] T. NEM, "Nem technical reference," *URL https://nem.io/wpcontent/themes/nem/files/NEM_techRef. pdf*, 2018.

[139] E. A. Posner and E. G. Weyl, "Voting squared: Quadratic voting in democratic politics," *Vand. L. Rev.*, vol. 68, p. 441, 2015.

[140] E. G. Weyl, "The robustness of quadratic voting," *Public choice*, vol. 172, no. 1-2, pp. 75–107, 2017.

[141] S. P. Lalley and E. G. Weyl, "Quadratic voting: How mechanism design can radicalize democracy," in *AEA Papers and Proceedings*, vol. 108. American Economic Association 2014 Broadway, Suite 305, Nashville, TN 37203, 2018, pp. 33–37.

[142] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.

[143] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," *arXiv preprint arXiv:1707.01873*, 2017.

[144] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Sok: Consensus in the age of blockchains," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 183–198.

[145] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," *arXiv preprint arXiv:2001.07091*, 2020.

[146] Q. Ding, W. Xu, Z. Wang, and D. K. C. Lee, "Voting schemes in dao governance," *Forthcoming in Annual Review of Fintech*, 2023.

[147] K. J. Arrow, "Social choice and individual values," 2012.

[148] "Controlled supply - Bitcoin Wiki — en.bitcoin.it," https://en.bitcoin.it/wiki/Controlled_supply#cite_note-1, [Accessed 30-10-2023].

[149] "Difficulty - Bitcoin Wiki — en.bitcoin.it," https://en.bitcoin.it/wiki/Difficulty, [Accessed 30-10-2023].

[150] R. Kher, S. Terjesen, and C. Liu, "Blockchain, bitcoin, and icos: a review and research agenda," *Small Business Economics*, vol. 56, pp. 1699–1720, 2021.

[151] S. Magnusson, D. Renhage, and J. Borges, "Initial exchange offerings (ieos) and initial dex offerings (idos)," 2022.

[152] V. Buterin, "Launching the Ether Sale — Ethereum Foundation Blog — blog.ethereum.org," https://blog.ethereum.org/2014/07/22/launching-the-ether-sale, 2014, [Accessed 25-11-2023].

[153] "Smart contract blockchain with a community-managed treasury — Edgeware — edgeware.io," https://www.edgeware.io/, 2019, [Accessed 25-11-2023].

[154] "Plasm Lockdrop — lockdrop.astar.network," https://lockdrop.astar.network/#/lock-form, 2019, [Accessed 25-11-2023].

[155] D. W. Allen, C. Berg, and A. M. Lane, "Why airdrop cryptocurrency tokens?" *Journal of Business Research*, vol. 163, p. 113945, 2023.

[156] C. Liu, "Crypto-asset valuation: A review and analysis of current methods," *Cryptofinance: A New Currency for a New Economy*, pp. 171–190, 2022.

[157] A. Hayes, "A cost of production model for bitcoin," *Available at SSRN 2580904*, 2015.

[158] A. S. Hayes, "Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin," *Telematics and informatics*, vol. 34, no. 7, pp. 1308–1321, 2017.

[159] ——, "Bitcoin price and its marginal cost of production: support for a fundamental value," *Applied economics letters*, vol. 26, no. 7, pp. 554–560, 2019.

[160] D. Yermack, "Is bitcoin a real currency? an economic appraisal," in *Handbook of digital currency*. Elsevier, 2015, pp. 31–43.

[161] E. Pagnotta and A. Buraschi, "An equilibrium valuation of bitcoin and decentralized network assets," *Available at SSRN 3142022*, 2018.

[162] A. Meynkhard, "Fair market value of bitcoin: Halving effect," *Investment Management and Financial Innovations*, vol. 16, no. 4, pp. 72–85, 2019.

[163] G. Fanti, L. Kogan, and P. Viswanath, "Economics of proof-of-stake payment systems," in *Working paper*, 2019.

[164] S. Simeonov, "Metcalfe's law: more misunderstood than wrong?" https://blog.simeonov.com/2006/07/26/metcalfes-law-more-misunderstood-than-wrong/, 2006, [Accessed 25-11-2023].

[165] Coinbase, "What is Ethereum? — coinbase.com," https://www.coinbase.com/learn/crypto-basics/what-is-ethereum, [Accessed 15-11-2023].

[166] The-Eth-Maxi-Blog, "If bitcoin is digital gold. ethereum is digital oil," https://www.publish0x.com/the-eth-maxi-blog/if-bitcoin-is-digital-gold-ethereum-is-digital-oil-xeezgrn, 2022, [Accessed 15-11-2023].

[167] H. Mutie, "Ask cryptovantage: Why is bitcoin digital gold? and is ethereum digital oil?" https://www.cryptovantage.com/news/ask-cryptovantage-why-is-bitcoin-digital-gold-and-is-ethereum-digital-oil/, 2023, [Accessed 15-11-2023].

[168] A. Lehar and C. A. Parlour, "Decentralized exchanges," *Available at SSRN 3905316*, 2021.

[169] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–50, 2023.

[170] "Home — Uniswap Protocol — uniswap.org," https://uniswap.org/, [Accessed 02-11-2023].

[171] "curve.fi," https://curve.fi/#/ethereum/swap, [Accessed 02-11-2023].

[172] L. Ante, "Non-fungible token (nft) markets on the ethereum blockchain: Temporal development, cointegration and interrelations," *Economics of Innovation and New Technology*, pp. 1–19, 2022.

[173] K. Ko, T. Jeong, J. Woo, and J. W.-K. Hong, "Survey on blockchain-based non-fungible tokens: History, technologies, standards, and open challenges," *International Journal of Network Management*, p. e2245, 2023.

[174] CryptoKitties, "CryptoKitties — Collect and breed digital cats! — cryptokitties.co," https://www.cryptokitties.co/, 2017, [Accessed 25-11-2023].

[175] "CryptoPunks — larvalabs.com," https://www.larvalabs.com/cryptopunks, 2017, [Accessed 25-11-2023].

[176] L. Oliveira, L. Zavolokina, I. Bauer, and G. Schwabe, "To token or not to token: Tools for understanding blockchain tokens." ICIS, 2018.

[177] Y. C. Lo and F. Medda, "Assets on the blockchain: An empirical study of tokenomics," *Information Economics and Policy*, vol. 53, p. 100881, 2020.

[178] A. Eshraghi, "Approaches to cryptocurrency valuation," in *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*. Emerald Publishing Limited, 2023, pp. 171–184.

[179] T. Peterson, "Metcalfe's law as a model for bitcoin's value," *Alternative Investment Analyst Review Q*, vol. 2, 2018.

[180] B. Van Vliet, "An alternative model of metcalfe's law for valuing bitcoin," *Economics Letters*, vol. 165, pp. 70–72, 2018.

[181] L. W. Cong, Y. Li, and N. Wang, "Tokenomics: Dynamic adoption and valuation," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1105–1155, 2021.

[182] A. C. Brucker, "De-fi protocol token valuation by projecting token flows and estimating an appropriate risk premium," 2022.

[183] R. Kräussl and A. Tugnetti, "Non-fungible tokens (nfts): A review of pricing determinants, applications and opportunities," *Applications and Opportunities (May 17, 2022)*, 2022.

[184] M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the nft revolution: market trends, trade networks, and visual features," *Scientific reports*, vol. 11, no. 1, p. 20902, 2021.

[185] F. Horky, C. Rachel, and J. Fidrmuc, "Price determinants of non-fungible tokens in the digital art market," *Finance Research Letters*, vol. 48, p. 103007, 2022.

[186] C. Lamon, E. Nielsen, and E. Redondo, "Cryptocurrency price prediction using news and social media sentiment," *SMU Data Sci. Rev*, vol. 1, no. 3, pp. 1–22, 2017.

[187] J. Abraham, D. Higdon, J. Nelson, and J. Ibarra, "Cryptocurrency price prediction using tweet volumes and sentiment analysis," *SMU Data Science Review*, vol. 1, no. 3, p. 1, 2018.

[188] J. Silberholz and D. A. Wu, "Measuring utility and speculation in blockchain tokens," *Available at SSRN 3915269*, 2021.

[189] F. Kjærland, A. Khazal, E. A. Krogstad, F. B. Nordstrøm, and A. Oust, "An analysis of bitcoin's price dynamics," *Journal of Risk and Financial Management*, vol. 11, no. 4, p. 63, 2018.

[190] "EIP-1559: Fee market change for ETH 1.0 chain — eips.ethereum.org," https://eips.ethereum.org/EIPS/eip-1559, [Accessed 16-11-2023].

[191] K. Saito and M. Iwamura, "How to make a digital currency on a blockchain stable," *Future Generation Computer Systems*, vol. 100, pp. 58–69, 2019.

[192] M. Iwamura, Y. Kitamura, T. Matsumoto, and K. Saito, "Can we stabilize the price of a cryptocurrency?: Understanding the design of bitcoin and its potential to compete with central bank money," *Hitotsubashi Journal of Economics*, pp. 41–60, 2019.

[193] S. Noda, K. Okumura, and Y. Hashimoto, "An economic analysis of difficulty adjustment algorithms in proof-of-work blockchain systems," in *Proceedings of the 21st ACM Conference on Economics and Computation*, 2020, pp. 611–611.

[194] S. Basu, D. Easley, M. O'Hara, and E. G. Sirer, "Towards a functional fee market for cryptocurrencies," *arXiv preprint arXiv:1901.06830*, 2019.

[195] R. Lavi, O. Sattath, and A. Zohar, "Redesigning bitcoin's fee market," *ACM Transactions on Economics and Computation*, vol. 10, no. 1, pp. 1–31, 2022.

[196] A. C.-C. Yao, "An incentive analysis of some bitcoin fee designs," *arXiv preprint arXiv:1811.02351*, 2018.

[197] T. Roughgarden, "Transaction fee mechanism design for the ethereum blockchain: An economic analysis of eip-1559," *arXiv preprint arXiv:2012.00854*, 2020.

[198] ——, "Transaction fee mechanism design," *ACM SIGecom Exchanges*, vol. 19, no. 1, pp. 52–55, 2021.

[199] M. V. Ferreira, D. J. Moroz, D. C. Parkes, and M. Stern, "Dynamic posted-price mechanisms for the blockchain transaction-fee market," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 86–99.

[200] H. Chung and E. Shi, "Foundations of transaction fee mechanism design," in *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM, 2023, pp. 3856–3899.

[201] "Transparency — tether.to," https://tether.to/en/transparency/#usdt, [Accessed 01-11-2023].

[202] "Pax Gold - The Safest Way to Own Gold — paxos.com," https://paxos.com/paxgold/, [Accessed 01-11-2023].

[203] "MakerDAO — An Unbiased Global Financial System — makerdao.com," https://makerdao.com/en/, [Accessed 01-11-2023].

[204] N. Al-Naji, J. Chen, and L. Diao, "Basis: a price-stable cryptocurrency with an algorithmic central bank," *Basis. io*, 2017.

[205] E. Kereiakes, M. D. M. Do Kwon, and N. Platias, "Terra money: Stability and adoption," *White Paper, Apr*, 2019.

[206] K. Ito, M. Mita, S. Ohsawa, and H. Tanaka, "What is stablecoin?: A survey on its mechanism and potential as decentralized payment systems," *International Journal of Service and Knowledge Management*, vol. 4, no. 2, pp. 71–86, 2020.

[207] C. Catalini, A. de Gortari, and N. Shah, "Some simple economics of stablecoins," *Annual Review of Financial Economics*, vol. 14, pp. 117–135, 2022.

[208] S. de la Rouviere, "Tokens 2.0: Curved Token Bonding in Curation Markets — simondlr," https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5, 2017, [Accessed 18-11-2023].

[209] V. Buterin, "On Path Independence — vitalik.ca," https://vitalik.ca/general/2017/06/22/marketmakers.html, 2017, [Accessed 17-11-2023].

[210] yosriady, "Bonding Curves Explained — yos.io," https://yos.io/2018/11/10/bonding-curves/, 2018, [Accessed 18-11-2023].

[211] E. Hertzog, G. Benartzi, and G. Benartzi, "Bancor protocol," 2017.

[212] Y. Zhang, X. Chen, and D. Park, "Formal specification of constant product (xy= k) market maker model and implementation," *White paper*, 2018.

[213] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, "Uniswap v3 core," *Tech. rep., Uniswap, Tech. Rep.*, 2021.

[214] "0x — Powerful APIs to build financial apps on crypto rails — 0x.org," https://0x.org/, [Accessed 02-11-2023].

[215] C. Catalini and A. de Gortari, "On the economic design of stablecoins," *Available at SSRN 3899499*, 2021.

[216] A. d'Avernas, V. Maurin, and Q. Vandeweyer, "Can stablecoins be stable?" *University of Chicago, Becker Friedman Institute for Economics Working Paper*, no. 2022-131, 2022.

[217] B. Routledge and A. Zetlin-Jones, "Currency stability using blockchain technology," *Journal of Economic Dynamics and Control*, vol. 142, p. 104155, 2022.

[218] Y. Li and S. Mayer, "Money creation in decentralized finance: A dynamic model of stablecoin and crypto shadow banking," *Fisher College of Business Working Paper*, no. 2020-03, p. 030, 2022.

[219] M. Obstfeld, "Models of currency crises with self-fulfilling features," *European economic review*, vol. 40, no. 3-5, pp. 1037–1047, 1996.

[220] D. W. Diamond and P. H. Dybvig, “Bank runs, deposit insurance, and liquidity,” *Journal of political economy*, vol. 91, no. 3, pp. 401–419, 1983.

[221] M. Kandori, *Mighty Microeconomics: A Guide to Thinking Like An Economist*. Cambridge University Press, 2023.

[222] S. Fu, Q. Wang, J. Yu, and S. Chen, “Rational ponzi game in algorithmic stablecoin,” in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2023, pp. 1–6.

[223] R. Sams, “A note on cryptocurrency stabilisation: Seigniorage shares,” *Brave New Coin*, pp. 1–8, 2015.

[224] M. Zargham, J. Shorish, and K. Paruch, “From curved bonding to configuration spaces,” in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–3.

[225] M. Zargham, K. Paruch, and J. Shorish, “Economic games as estimators,” in *Mathematical Research for Blockchain Economy: 2nd International Conference MARBLE 2020, Vilamoura, Portugal*. Springer, 2020, pp. 125–142.

[226] G. Angeris and T. Chitra, “Improved price oracles: Constant function market makers,” in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 80–91.

[227] M. Bartoletti, J. H.-y. Chiang, and A. Lluch-Lafuente, “A theory of automated market makers in defi,” *Logical Methods in Computer Science*, vol. 18, 2022.

[228] H. Adams, M. Salem, N. Zinsmeister, S. Reynolds, A. Adams, W. Pote, M. Toda, A. Henshaw, E. Williams, and D. Robinson, “Uniswap v4 core [draft],” 2023.

[229] B. Krishnamachari, Q. Feng, and E. Grippo, “Dynamic curves for decentralized autonomous cryptocurrency exchanges,” in *4th International Symposium on Foundations and Applications of Blockchain 2021*, 2021.

[230] R. Hanson, “Combinatorial information market design,” *Information Systems Frontiers*, vol. 5, pp. 107–119, 2003.

[231] A. Othman, “Automated market making: Theory and practice,” Ph.D. dissertation, Carnegie Mellon University, 2012.

[232] A. Braun, N. Häusle, and S. Karpischek, “Incentivization in decentralized autonomous organizations,” *Available at SSRN*, 2021.

[233] “What is Gitcoin Passport? — support.gitcoin.co,” https://support.gitcoin.co/gitcoin-knowledge-base/gitcoin-passport/what-is-gitcoin-passport, [Accessed 20-11-2023].

[234] A. Mekacher, A. Bracci, M. Nadini, M. Martino, L. Alessandretti, L. M. Aiello, and A. Baronchelli, “How rarity shapes the nft market,” *arXiv preprint arXiv:2204.10243*, p. 9, 2022.

[235] D. Nelson, “NounsDAO Barrels Toward Treasury Split After NFT Holders Rally for ‘Rage Quit’ — coindesk.com,” https://www.coindesk.com/markets/2023/09/09/nounsdao-barrels-toward-treasury-split-after-nft-holders-rally-for-rage-quit/, 2023, [Accessed 20-11-2023].

[236] H. Uhlig, “A luna-tic stablecoin crash,” National Bureau of Economic Research, Tech. Rep., 2022.

[237] A. Briola, D. Vidal-Tomás, Y. Wang, and T. Aste, “Anatomy of a stablecoin’s failure: The terra-luna case,” *Finance Research Letters*, vol. 51, p. 103358, 2023.

[238] J. Liu, I. Makarov, and A. Schoar, “Anatomy of a run: The terra luna crash,” National Bureau of Economic Research, Tech. Rep., 2023.

[239] T. Barbereau, R. Smethurst, O. Papageorgiou, A. Rieger, and G. Fridgen, “Defi, not so decentralized: The measured distribution of voting rights,” 2022.

[240] T. Barbereau, R. Smethurst, O. Papageorgiou, J. Sedlmeir, and G. Fridgen, “Decentralised finance’s timocratic governance: The distribution and exercise of tokenised voting rights,” *Technology in Society*, vol. 73, p. 102251, 2023.

[241] “”Fee Switch” Pilot Update & Vote — gov.uniswap.org,” https://gov.uniswap.org/t/fee-switch-pilot-update-vote/19514, 2022, [Accessed 21-11-2023].

[242] “Uniswap Proposal: An Alternative Use-Case for the Fee Switch — gov.uniswap.org,” https://gov.uniswap.org/t/uniswap-proposal-an-alternative-use-case-for-the-fee-switch/20779, 2023, [Accessed 21-11-2023].

[243] “Sushi; — sushi.com,” https://www.sushi.com/, [Accessed 28-11-2023].

[244] S. Fan, T. Min, X. Wu, and C. Wei, “Towards understanding governance tokens in liquidity mining: a case study of decentralized exchanges,” *World Wide Web*, vol. 26, no. 3, pp. 1181–1200, 2023.

[245] J. A. Kroll, I. C. Davey, and E. W. Felten, “The economics of bitcoin mining, or bitcoin in the presence of adversaries,” in *Proceedings of WEIS*, vol. 2013, 2013, p. 11.

[246] “Maximal extractable value (MEV) — ethereum.org — ethereum.org,” https://ethereum.org/en/developers/docs/mev/, [Accessed 02-11-2023].

[247] A. Badari and A. Chaudhury, “An overview of bitcoin and ethereum white-papers, forks, and prices,” *Forks, and Prices (April 26, 2021)*, 2021.

[248] B. Y. AL-MANSOUR, “Cryptocurrency market: Behavioral finance perspective,” *The Journal of Asian Finance, Economics and Business (JAFEB)*, vol. 7, no. 12, pp. 159–168, 2020.

[249] K. Toyoda, “Web3 meets behavioral economics: An example of profitable crypto lottery mechanism design,” in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*. IEEE, 2023, pp. 678–679.

[250] E. Verbin, “Behavioral Crypto-Economics: The challenge and promise of blockchain incentive design — medium.com,” https://medium.com/lunar-ventures/behavioral-crypto-economics-6d8befbf2175, [Accessed 02-11-2023].