# Description

I want to make a tokenGPT who is my Token Engineer, who has deep knowledge of decentralized finance, his skills of portfolio management and optimization from traditional finance and defi, can before statistical and mathematical modelling and analysis.

The tokenGPT has detailed knowledge of mechanism design, game theory, modelling and simulations, with deep understanding of economics and incentives design and user behaviour. With it's modelling and simulations capabilities tokenGPT can make python based models for design, verification and optimization of token based economic systems.

tokenGPT has deep understanding of token engineering frameworks like Quantitative token model, tokenspice agent based simulations, cadCAD system dynamics simulator. It undestands the dynamics of decentralized finance and aware with AMMs, CFMMs like Uniswap, Curve, Balancer etc. tokenGPT is also aware to diffenrt type of coonsensu mechanism like pos and pow and in pos specifically etheuem staking, Liquid staking (Lido, rocketpool, cbETH etc), restaking (eigenlayer), liquid restaking etherFi (eETH) etc.

It completely understands the rsiks associated with defi instruments, like liquidations, impermamnent loss, slippage, liquidity risk etc.

tokenGPT is comrehensive assistand who is aware of differnt data platforms like subgraphs, dune dashboards, defi llama, nansen etc.

# Data

## Tokenomics Audit

How to do a tokenomics audit

Creating a tokenomics audit for a blockchain project presents its own unique set of challenges. The main challenge with tokenomics is that you are trying to create an incentive structure while also making a large number of interconected assumptions.

There are two main tools I like to use when auditing tokenomics structures:

Similarity to existing projects. Are there are any other projects with similar goals, objectives, structures, etc.?

Marginal cases. Are there any extreme cases where the system would break down?

The good thing with BankX is that it is a stablecoin, which gave us plenty of things to work with, since we could get data from existing projects.

The challenge was that BankX is quite innovative, incorporating some new mechanisms such as Integrated Protocol Owned Liquidity, and the use of bonding curves.

Example of a bonding curve that is used for integrated protocol owned liquidity within BankX

Some other things we did in order to help us put structure into the audit were:

Define and prioritise the goals of the system.

Break down each and every mechanism the system uses to achieve those goals

This helped improve the organisation of the audit, and the final outcome. The ultimate goal of an audit is to convince an informed reader that a system could work.

The BankX integrated liquidity system

While I am a big fan of agent-based modelling, we didn’t have to resort to this for this particular audit. Instead, we used data from other stablecoin projects, as well as game theory.

BankX tokenomics audit

After months of hard work, we managed to put everything together on a 20-page document. You can find the full audit here. I hope that this audit will also help improve the standards in how tokenomics systems are being designed.

## Tokenomics and blockchain tokens: A design-oriented morphological framework

Abstract

Blockchain technology has been around for more than ten years, nevertheless, the knowledge about its economic and business implications is still fragmented and heterogeneous. The present article intends to tackle this issue with a twofold contribution. The first is an analysis of the shift from economics to tokenomics highlighting the central role played by tokens within blockchain-based ecosystems. The second is a framework for tokens design leveraging a morphological analysis deeply grounded in the literature. As blockchain becomes a mainstream phenomenon, the value of the work proposed lies in lowering the cognitive barriers and in clarifying the space of available options for private and public actors willing to leverage tokenization in their daily operations.

Previous article in issueNext article in issue

Keywords

BlockchainTokenizationTokenomicsClassification frameworkToken design

1. Introduction

Over a decade has passed since Satoshi Nakamoto published an innovative solution to the double-spending problem [1] based on a peer-to-peer disintermediated network [2]. The whitepaper gave birth to the first blockchain and the first cryptocurrency, Bitcoin. Since then, the underlying Distributed Ledger Technology (DLT) has been acknowledged as a foundational technology [3], with a potential impact likely to match or outstrip the revolution brought by the Internet in the Nineties [4,5].

Even if blockchain technology has been around for a decade, a shared understanding of some fundamental mechanisms is still lacking [6]. In particular, if, on one hand, the technical aspects have been thoroughly explored, defined, and branched out into different deployments, on the other hand, the business and social implications are still blurred.

Keeping aside the technical details (covered by extensive literature), one of the grounding pillars of the blockchain technology is the possibility to reach a shared consensus on a univocal truth describing the history of states of a digital ecosystem, in the form of a transactions' ledger. A mathematical algorithm mediates the achievement of such a consensus on a unique source of authenticity. The ultimate implication of relying on a consensus algorithm is overcoming the need for a central authority that is entitled to provide a univocal truth. Therefore, the first paradigmatic shift originates from decentralizing the source of truth and cutting off centralized guarantors.

Talking about “univocal truth” and “centralized guarantors” may sound theoretical and far from daily life, but it is rather the contrary. The most fundamental aspects of people's lives rely on a centralized source of truth that acts as a guarantor, starting with their identity. The supreme act of one's self-determination needs to be certified by a third-party (such as a state administration) to be generally acknowledged. Countless are the scenarios in which a birth certificate, an ID, or a passport is needed to carry out daily activities, and the central government issues all those documents. The same applies to finance management: when someone makes a payment, their bank (or credit card issuer) guarantees that the funds in their account cover the expense (or that it is suited to their credit-score).

Tracing back to the roots of money, the vast majority of economic transactions are performed using a currency, in particular, a fiat currency (fiat in Latin means “let it be done”). Fiat currencies do not have intrinsic value, and they can be used since a central authority (the Central Bank) establishes and maintains its value [7]. The ground-breaking innovation introduced by Nakamoto, from a non-technical perspective, is the decentralization of the source of truth in handling currency-based transactions, de facto offering an opportunity to ensure reliable peer-to-peer payments without the need for a system of intermediaries acting as guarantors for the validity of transactions. Decentralization applies throughout the monetary system, and Bitcoin is a decentralized and disintermediated currency that is not issued and managed by central authorities, but instead, it is algorithmically governed.

The path outlined by Nakamoto, detouring centralized sources of truth, paved the way to the overall shift of numerous economic activities. In the years following the launch of Bitcoin, a large number of cryptocurrencies emerged, and a diverse cosmos of blockchains has been developed. Thanks to immutability and transparency, blockchain offers individuals prerogatives previously available only to institutions, transforming actions into transactions and triggering virtuous behaviors. Furthermore, decentralization has been applied way beyond the mere monetary context, embracing different value-based scenarios, through tokenization.

In such a heterogeneous context, there is a need to shed light on the actual role that blockchain tokens play in decentralized ecosystems. This paper aims at addressing such a need and is an extension of the work originally presented in the 2020 IEEE Symposium on Computers and Communications (ISCC) [8]. In particular, the token classification framework there introduced is here revised, enriched, and thoroughly explained in all its dimensions.

Section 2 describes what a tokenization process is and what innovations it brings. Section 3 shifts the focus towards the fundamental unit of said process, the token, distilling its nature and explaining the rationale underlying the demand for a comprehensive guiding framework to design and classify tokens. Section 4 analyzes the state of the art in terms of existing approaches present in the literature. Section 5 presents the methodology adopted for the generation of the new framework proposed. Section 6 includes the results of the analysis conducted. Section 7, illustrates the article's core contribution by providing a walkthrough of the proposed framework whose ambition is to provide a simple and intuitive tool for the extensive and complete description of a token that may be used for both design and classification purposes. Section 8 details the evolution of the framework discussed in this article from the previous version presented in a workshop contribution. Section 9 contains some conclusions and next steps that the authors intend to take to further strengthen the validation of the framework proposed. Finally, the reader can refer to the Appendix to find three example applications of the framework.

2. The shift from economics to tokenomics

The tokenization process can be described as the encapsulation of value in tradeable units of account, called tokens or coins [8]. The disruptive potential lies in expanding the concept of value that can be partitioned and traded beyond purely economic terms, including reputation, work, copyright, utility, and voting rights. Once tokenized, all these manifestations of value can be detected, accounted for, and leveraged in the context of a system of incentives that may promote fair levels of wealth and power redistribution.

In other words, tokenization represents a form of digitalization of value and, just like the Internet enabled free and fast circulation of digitized information, the blockchain is allowing the “almost free” [9] and borderless flow of digitized value. The blockchain made it possible to algorithmically solve the double-spending problem and introduced the concept of digital scarcity, as opposed to the digital abundance characterizing the Internet of information [10]. In particular, digital scarcity will act as a key enabler of a new digital economy relying on assets that are liquid, divisible, borderless (easily transportable and quickly transferable), and, unlike currencies, have the potential to appreciate over time. The controlled inflationary nature of some of these assets may have deep implications in helping our society to migrate from a debt-based economy, producing significant improvements in people's lives and the democratic processes.

Once tokenized, every kind of value (in a broad sense) can be managed as a digital asset, whose unit of account is a dedicated virtual token. Such virtual tokens can be minted by any individual or organization that defines the set of rules governing them. These include the token features, the monetary policy, and the users' incentive system. In light of this, the tokenization process can be further described as the creation of a self-governed (tok)economic system, whose rules are programmed by the token designer.

Here comes the second paradigmatic shift, namely from economics to tokenomics. In economics, innovation proceeds and propagates by introducing a change in the context of set rules and observing how such a relatively rigid framework reacts to the change. Therefore, the outcome of the proposed innovation is assessed, at first, on a predictive basis. Conversely, in tokenomics, innovation is put forward by designing the rules governing the playground in a way that the stakeholders' behavior aligns with the goal pursued. In other words, the second paradigmatic shift moves from the passive observation of the ecosystem's reaction to a change to the active design of the ecosystem constituent laws, aimed at reaching the desired outcome.

The tokenization process, as well as the shift to tokenomics, revolves around the token. Without neglecting the importance of the underlying infrastructure and its technical features, a deep understanding of the token nature is fundamental to effectively unleashing the disruptive potential of blockchain technology.

3. The underlying rationale to tokens classification

A deep understanding of the nature of the token, and the capability to comprehensively describe it, is as crucial as challenging. Given the cornerstone role played by tokens in a tokenization process, their meaning is intimately related to the very concept of tokenization. Following this approach, the token definition moves along two strands: on one hand, it addresses the function performed by tokens, and, on the other hand, it drills to the very essence of what they represent.

Looking at the function performed by tokens in economic terms, a token can be described as “a unit of value that an organization creates to self-govern its business model, and empower its users to interact with its products while facilitating the distribution and sharing of rewards and benefits to all its stakeholders” [11]. In simplistic terms, tokens can be seen as privately issued currencies used to exchange value within an ecosystem (e.g., Bitcoin). In reality, their usage has gone far beyond mere currency applications. The roles that a token may play are manifold and include, among others, giving access to a service, granting the right to contribute to a community, regulating the governance through voting rights. More generally, a token can be intended as a socio-economic tool to promote the coordination of the actors in a regulated ecosystem towards the pursuit of a network objective function [12], through a set of incentive systems.

The token, being a unit of account, doesn't have an intrinsic and self-standing definition, but its nature is determined by what it represents. Sticking to the concept of tokenization as an encapsulation of value, the token is the representation of such value. Therefore, the deep understanding of the encapsulated value provides the key to distilling the essence of tokens.

The value represented by the tokens observable in the wild is diversified and cannot be described univocally: it can be either the right to have a discount on an exchange rate, or the proof of ownership of a gold ingot, or the reward for solving a mathematical problem to validate the next block of the chain, or many other examples. The challenge is to generalize the definition of token-represented value by chasing a common trait that all these expressions of value share. Looking deeply into the source of token-encapsulated value, the concept of trust emerges as a cornerstone.

When tokens represent the holder's right, for example, to access a service or benefit from a discount or express a vote, within a regulated ecosystem, the token holder grants trust to the token issuer. In particular, the holder trusts that the right represented and originating from the token holds and is enforceable. Ultimately, the holder trusts the token issuer and its capability to honor the obligation associated with the right represented by the token. When tokens represent an underlying asset (or better a real right—ius in re—on an underlying asset), the token holder trusts that the token issuer ensures the enforceability of the right itself and, at the same time, that the underlying asset is adequately managed and holds (or increases) its value. When tokens are the reward for the block validation activity, their value is the direct representation of the level of trust towards the token holder community and its disintermediated and decentralized consensus, enabled by the underlying blockchain infrastructure. Keeping along this road, it is always possible to bring back the source of value of a token to the concept of trust. Ultimately, it is possible to define tokens as quantifiable representations of decentralized and disintermediated trust.

Many tokens have been conceived and deployed in a relatively short time frame: their flourishing has been chaotic, highly experimental, and iterative. At the same time, their adoption and growth followed an evolutionary pattern with many tokens that didn't survive the process of natural selection. Given the early stage and the broad scope of token-driven innovation, the nature of tokens is still taking shape, and its definition should be approached with a dynamic and iterative mindset. Their highly diverse features and applications pose another challenge in defining the nature of tokens. The extent of this diversity requires a comprehensive taxonomy, similar to what applies to living organisms, resulting from evolution. So far, a relevant number of classifications have been already proposed. Nevertheless, the transition from the initial unruled chaos to an ordered, yet dynamic, taxonomy is still far from being mature and requires a collective effort of scholars, experts, and practitioners.

The goal of this work is to propose a comprehensive approach to tokens classification that accurately maps all the different branches of value representations that tokens can convey. The resulting framework is intended as a tool for non-technical decision-makers to orient themselves in the tokenomics space and to make informed strategic decisions when approaching a token design process, lowering the existing cognitive barriers. Such a tool can be used as a compass to define the requirements and the guidelines for the creation and development of a new token, also allowing for a convenient comparison among different design intentions and outcomes.

4. Related works

4.1. Tokens classification

As previously mentioned, to reach an overall understanding of the multiform nature of tokens, a comprehensive taxonomy approach is needed. If, in general terms, tokens can be described as a quantifiable representation of decentralized and disintermediated trust, an operational definition of existing (and future) tokens must include all the diverse shades of trust they convey. One of the main goals of this paper is to expand the definition of tokens by means of a systematic and ordered procedure, based on the concept of taxonomy, borrowed from natural science. It follows a comprehensive analysis of the existing literature related to this work.

A fair number of token classifications and taxonomies have been proposed so far. Oliveira et al. [13] presented one of the most comprehensive studies on the topic, combining extensive literature research with insights collected through 16 interviews with experts and practitioners. The resulting classification characterizes tokens using 13 different parameters, describing both their technical features and business-related aspects. Furthermore, mapping 18 tokens against those parameters, 8 token archetypes were identified by analyzing recurring feature patterns. The work of Oliveira et al. [13] is grounded on several classifications previously proposed, two of which are worth being mentioned. “The Token Classification Framework” presented by Thomas Euler [14] classifies tokens along 5 dimensions: purpose, utility, legal status, underlying value, and technical layer. Such a framework has the goal to look at a single token from different perspectives simultaneously, and it is the first tentative to capture and summarize the polyhedric nature of tokens. William Mougayar provided another relevant contribution to the collective effort in capturing the nature of tokens [11,15]. His framework revolves around 3 classification dimensions: role, features, and purpose. It focuses primarily on the business-related aspects of tokens, with particular reference to their entanglement with the token issuer's business model and the incentives arising for the token holders.

Looking at the contributions in the field of token classification and taxonomy coming from companies and business practitioners, the “Taxonomy Report on Cryptoassets” by CryptoCompare [16] is an extensive analysis that provides several valuable approaches to the classification of tokens. More than 200 tokens have been examined and classified using 30 unique attributes, covering economic, legal, and technological features. In particular, two grouping criteria are of particular interest: Rationale to Possess and Economic Value Drivers. The former classifies tokens according to the main reason that drives token holders to acquire and keep their tokens, while the latter groups them based on the mechanisms underlying their price trends and fluctuations. These grouping criteria represent a well-structured approach to tokens' classification relating to the incentive system that they convey and the behavior they intend to induce into token holders.

More recently, in November 2019, the Token Taxonomy Initiative (now InterWork Alliance) published the first version of the “Token Taxonomy Framework” [17], resulting from a broad cross-industry effort to define a common standard to describe and design tokens. In particular, such a framework [18] aims at introducing not another standard, but rather to create a “metastandard”. Its role is to bridge token protocols and platforms to ensure effective interoperability, lay the foundation of a collective understanding of tokens, and create a shared language that can empower communication among technology experts and business practitioners. Proceeding on first-principles thinking, the Token Taxonomy Framework classifies tokens along with five characteristics: Token Type, Token Unit, Value Type, Representation Type, and Template Type [18,19]. Those characteristics are intended to describe the nature of a token and the role it plays within a business model. Furthermore, the Token Taxonomy Framework's description approach is particularly interesting, since it represents each token through a formula combining base types, behaviors, and property sets of the token. It is a promising modular approach that can reuse and combine token features, even if it is at an early conceptual stage.

From this overview of the most relevant token classifications and taxonomies available in the literature, it results that the approaches adopted are very diverse and the methodology heterogeneous. It is important to highlight that a de facto standard has not emerged yet probably since each classification focuses on a specific perspective and no prior work has managed to capture an all-round representation of the phenomenon. This leaves a gap in the literature that the work presented intends to fill by providing a useful tool for both theory and practice. As a starting point, normalization is needed to perform a comparative assessment of the classification frameworks.

4.2. Game theoretical aspects

As previously explained, the potential functions of tokens span a wide range of possibilities. Token design choices not only impact the platform's users and what they can accomplish within it, but also on the underlying functioning of the blockchains themselves and the economic incentives that drive their evolution. As a consequence, this work is also linked to the emerging literature on game theoretical aspects related to blockchains which aims to investigate the economic properties and implications of blockchains. Specifically, a relevant area of research on blockchain is focusing on the general process of consensus generation, investigating the trade-offs in decentralization and the direct impact of blockchain technology on the real economy. Cong and He [20] analyzed how decentralization relates to consensus quality by means of a holistic approach useful to examine universal features of blockchains. Their focus is on how the information distribution that comes with decentralization interacts with the quality of consensus generation. Their results suggest that blockchain can deliver higher social welfare and consumer surplus through enhanced entry and competition. Sockin and Xiong [21], instead, analyzed the properties of utility tokens, contributing to the emerging literature on digital assets. In particular, they modeled a cryptocurrency as membership in a blockchain platform highlighting the risk of market breakdowns caused by the rigidity induced by digital asset price clearing among membership demand and token supply driven by speculators. Chiu and Koeppl [22] investigated the optimal design of a cryptocurrency, emphasizing the importance of scale in deterring double-spending limitations. Their focus is primarily on understanding how the design of a cryptocurrency influences the interactions among participants and their incentives to cheat, deriving from the double-spending problem. The results show the presence of a trade-off between transaction speed and the guarantee of their settlement. Catalini and Gans [23] explored the initial coin offerings (ICOs) funding mechanism in comparison with traditional equity financing, trying to understand how tokens can have any value given that the venture issuing them controls both their technological evolution as well as their monetary policy. Catalini et al. [24] modeled the market for tokens, determining how the cost of attacking the system depends on the level and shape of token supply and demand. One of their main results indicates that tokens' appreciation as a consequence of attackers' demand does not play a relevant role in securing the system. On the other hand, stablecoins are characterized by a lower level of vulnerability to attack with respect to digital assets that can freely fluctuate. Beyond the key papers presented above, the literature expands over several streams strongly related to the nature of tokens and their classification framework. Some papers examine the role of digital assets in the adoption of platforms [25,26], while others focus on the conditions for which the enforcement of cryptocurrency commitments can be helped by blockchain technology [27].

The analysis of the literature on game theoretical aspects of the blockchain highlights the strong connection with the present work on the token classification framework. The comprehensive token morphological framework presented in this work complements the technological background of every theoretical analysis. Specifically, it allows to better characterize the blockchain environment by enhancing the comprehension of tokens' design and their classification.

5. Methodology

Both tokens and their classifications show a high degree of variety, as previously discussed. To handle this heterogeneity a structured methodology is required, and, in the context of this work, General Morphological Analysis (GMA) has been chosen. GMA was developed by Fritz Zwicky [28,29] as a method to describe and assess problem complexes, characterized by non-quantifiable and multi-dimensional properties, by mapping all the possible relationships, or configurations, occurring in the given problem complex. Such a morphological approach is eventually aimed at identifying recurring patterns and building non-quantified inference models [[30], [31], [32]].

Given its characteristics and previous applications, GMA represents a comprehensive methodology that can be effectively applied to the description of tokens, comprising all their non-quantifiable and multi-dimensional properties. In particular, a token classification framework can be represented using a morphological field, resulting from the following steps:

•

identify and adequately define the dimensions of the problem, i.e., the parameters along which each token can be mapped;

•

for each dimension of the problem, a spectrum of values must be defined. These values represent the relevant states or conditions that each dimension can assume;

•

a morphological field is generated, including all the possible combinations of values assumed for each dimension. The number of all the possible configurations of the problem complex is the product of the number of conditions (values) under each parameter (dimension).

The GMA methodology is used in the first place to perform a comparative analysis of the token classification frameworks. In particular, this procedure is leveraged to address the need for normalization previously highlighted, and all the frameworks are traced back to a morphological field representation to make them comparable. Once normalized, the different token classification frameworks are critically analyzed to identify recurring morphological dimensions and values, detect gaps and eventually uncover token properties, and dismiss redundant or misleading definitions.

6. A classification of classifications

An extensive analysis of both scientific and grey literature has been performed. Eight token classification frameworks have been selected based on their relevance, comprehensiveness, and role of the respective issuer, considered as a proxy of the potential normative impact. Some of the selected frameworks have been described previously in the overview of related works. Fig. 1 presents a summary of the GMA-normalized token classification frameworks with the indication of the respective identified dimensions (i.e., mapping parameters of the token).

## Crypto compliances

The future of Crypto Compliance

Cryptocurrency exchanges reported trading volumes exceeding $14 trillion in 2021. With a market cap of around $983.72 billion, the crypto market is not limited to a few professionals fluent in technology. At the same time, the future of crypto compliance also deserves the attention of every stakeholder in the crypto ecosystem. The increasing usage of crypto is one of the first things which has driven the interest of regulators in cryptocurrency compliance.

Most importantly, the threats of using cryptocurrencies for illegal activities have also strengthened the discussions around crypto regulations and compliance. As a matter of fact, illegal transactions accounted for almost 0.15% of all crypto transactions in 2021. Even if the number appears trivial, illicit addresses received around $14 billion in 2021 in comparison to the $7.8 billion in 2020.

Therefore, it is important to strengthen the regulatory grasp over cryptocurrency operations to deal with the growing misuse of cryptocurrencies. However, it is also important to have oversight regarding the potential future of cryptocurrency compliance for introducing meaningful changes in this domain in the future. The following post helps you figure out the crypto compliance trends you can expect in the future. Let us learn about the challenges for crypto compliance in the future and how crypto compliance regulations are shaping up.

Want to develop an in-depth understanding of crypto compliance? Enroll now in Crypto Compliance Fundamentals Course

Why Does Crypto Compliance Matter for the Future?

Upon the introduction of Bitcoin in 2009, many people could not predict or foresee the humongous growth of cryptocurrencies. Over the course of time, Bitcoin has become quite a common name throughout the world. On the other hand, the crypto ecosystem has expanded by considerable margins, with new cryptocurrencies arriving in the market every day.

The New York Times reported that almost 100 new cryptocurrency projects are created on a daily basis. On top of it, cryptocurrencies are more accessible to the general public with easy-to-use exchanges and crypto wallet apps. The number of crypto users has increased by a humongous margin of almost 20 million within one year between 2020 and 2021.

The rapid growth of cryptocurrencies and their mainstream adoption are significant highlights for crypto compliance future as they expose the crypto ecosystem to various risks. One of the most common examples of risks points toward fraudsters who seek to exploit the crypto market. Why? The limited scope of regulations in the comparatively new and burgeoning crypto market serves as easy fodder for malicious agents.

Furthermore, the lack of formidable regulations also encourages the use of cryptocurrencies for money laundering, tax avoidance, and terrorism financing. All these factors clearly point to the urgent necessity for crypto compliance in the present as well as in the future.

Want to become a Cryptocurrency expert? Enroll now in Cryptocurrency Fundamentals Course!

Role of the Regulators in Crypto Compliance

Before diving straight into the details of crypto compliance risks, it is important to understand the role of regulators in compliance. Cryptocurrencies and blockchain technology have become mainstream topics owing to their increased adoption. According to the Financial Action Task Force or FATF, blockchain and cryptocurrencies can introduce radical changes in the financial landscape.

However, the speed and global reach, as well as anonymity of these technologies, present formidable risks. What could a regulator do in such scenarios? If you think of it, the role of regulators in crypto compliance is not as straightforward as you imagine it to be. Regulators are always caught in the middle of any new development. Strengthening regulations could restrict the growth and developments in crypto, while a flexible approach could enable criminals to exploit the vulnerabilities in regulations.

At the same time, compliance professionals have to deal with future of crypto compliance in industry developing recently. As people try to discover new ways of understanding cryptocurrencies, it is critical to reflect on the opportunities alongside threats and risks. The responsibility of following regulatory guidance also comes with the need to reflect on evolution of cryptocurrencies and updates in blockchain technology.

Can regulations keep up with the pace of new technologies emerging in the field of cryptocurrencies? At the same time, the introduction of many new products and methods for transferring value worldwide can provide new ways for criminals to exploit regulations. Therefore, the role of regulators in crypto compliance future is nothing short of challenging. What are regulators doing now to address crypto compliance?

Build your identity as a certified blockchain expert with 101 Blockchains’ Blockchain Certifications designed to provide enhanced career prospects.

Existing State of Crypto Compliance Regulations

The best way to anticipate crypto compliance trends for the future would obviously focus on an assessment of existing regulations. Bitcoin grabbed the attention of the Financial Action Task Force or FATF immediately upon its launch in 2009. The FATF has added recent additional guidance in their recommendations.

It also aims to introduce consistency throughout different crypto service provider frameworks. On top of it, regulators such as FinCEN and the SEC have also accepted cryptocurrency as some form of cash equivalents or securities. Most of the attention revolving around crypto compliance has been focused on addressing anti-money laundering objectives.

The European Union has also set a precedent for the future of crypto compliance with new regulations for cryptocurrencies. The EU has experienced many problems in establishing clear and strict crypto regulations owing to the anonymity and decentralized aspects. However, the EU imposed its first cyber-sanctions regime in November 2020, focused on Chinese, Russian, and North Korean actors involved in cyber-attacks on member states.

In addition, businesses dealing with cryptocurrencies in the UK must have to follow the Money Laundering, Terrorist Financing, and Transfer of Funds rules. Businesses working with cryptocurrencies must also register with the Financial Conduct Authority or FCA. Furthermore, the FCA has mandated cryptocurrency businesses to submit financial crime reports.

One of the most significant milestones in recent crypto compliance trends is the Markets in Crypto Assets or MICA regulation by the European Union. The MICA regulation can revolutionize crypto compliance through a definitive regulatory system for cryptocurrencies. Upon complete adoption in the EU, the MICA regulation would allow only licensed providers to operate crypto exchanges and custodial wallets.

Want to get an in-depth understanding of crypto fundamentals, trading and investing strategies? Enroll now in the Crypto Fundamentals, Trading And Investing Course

Challenges for Crypto Compliance in the Future

Cryptocurrency and blockchain technology has found widespread application in the financial industry. As a result, a major share of the crypto compliance risks emerges from the possibility of using cryptocurrencies for illicit activities. The scrutiny of regulators, enforcement agencies, and tax authorities all over the world has been increasing on crypto exchanges, investors, and other entities associated with crypto.

Therefore, traders and exchanges have to follow the regulatory frameworks and legal requirements, which are constantly evolving alongside the industry developments. What are the potential challenges for crypto compliance which would be significant in the future? Here is an outline of the notable challenges for crypto compliance.

Challenges for Crypto Compliance in the Future

Lack of Classification

Many regulators have come up with distinct and innovative approaches to dealing with crypto regulations. However, the future of crypto compliance needs a cohesive framework, which can help in resolving the nuances associated with different cryptocurrencies throughout the world.

Painting Cryptocurrencies as Money

The classification of cryptocurrencies as money or an equivalent to traditional fiat currency would also introduce unavoidable regulatory measures. Therefore, US regulators have avoided the classification of cryptocurrencies as money. In addition, fiat-backed stablecoins can also create ambiguities regarding regulations for cryptocurrencies and fiat currencies.

Shifting towards Future Markets

Another important highlight among crypto compliance trends focuses on the lack of specific regulation for cryptocurrencies. For example, US regulators throughout different jurisdictions and states leverage the rules from existing laws pertaining to securities investments for governing cryptocurrencies and tokens. However, the scale and pace of change in the domain of crypto assets would call for regulators to come up with completely new structures for dealing with the crypto industry.

Classification of Investors

Investors have been classified traditionally on the basis of different metrics. The common indicators used by US regulators for classification of investors include wealth, legal status, and transaction size. On the other hand, the scope of such classification has been limited to the primary market rather than secondary markets. Therefore, investors working with cryptocurrencies are obviously left out of the traditional classification for investors.

Dependence on Intermediaries

As of now, self-custody crypto wallets remove the role of intermediaries, which serve as a crucial component in securities regulation. Without the intermediary, wallet users can seek different ways to bypass the existing regulations.

Criminal Activities

The biggest challenge in defining crypto compliance for future would obviously turn the limelight towards criminal activities. Cryptocurrencies are a massive threat with respect to money laundering and tax evasion, alongside many other notable criminal activities. The evolution in the ways they are used for criminal activities also presents a formidable challenge for regulators to adapt accordingly.

Embrace the technological leap and global adoption that awaits in the upcoming bull run of 2024-2025 with Crypto Bull Run Ready Career Path.

Future of Crypto Regulations

The importance of crypto compliance and the challenges of crypto regulation show that compliance will be an inevitable aspect of crypto in the future. Most recently, the US Securities and Exchange Commission SEC introduced new rules for including crypto exchanges under regulatory control. The initiative can help in capturing platforms dealing with crypto, which are not under the control of the regulatory agency.

However, the list of challenges for the future of crypto compliance showcases the necessity for comprehensive crypto compliance and regulatory framework. The existing state of the cryptocurrency compliance space presents a disconnected and fragmented global compliance framework.

You can find different regulatory practices for cryptocurrencies in different countries and regions. For example, countries such as Egypt and China have imposed direct bans on popular crypto exchanges. Recently, China strengthened the curb on cryptocurrencies by imposing a ban on any type of crypto mining or transfers. In addition, many other countries have also imposed implicit bans on cryptocurrencies.

How is this a major issue for the future of cryptocurrencies? Almost every exchange in the crypto space works globally, transcending borders while imposing significant challenges for regulators as well as crypto providers. Interestingly, one of the good news for crypto compliance future points to the efforts of IMF for a global framework. The International Monetary Fund has proposed a global regulatory framework, which aims to encompass all licensed crypto service providers. At the same time, the framework would also consider the strict limits and liquidity requirements in the crypto sector.

Want to know the answers to some of the commonly asked questions about cryptocurrency? Check the detailed guide on Frequently Asked Questions About Cryptocurrency

Bottom Line

The description of expected trends for crypto compliance in the future showcases a lot of attention to challenges for compliance. Cryptocurrencies have created a constantly evolving and improving industry with new changes introduced every day. At the same time, the adoption of cryptocurrencies as common digital services or applications has also raised concerns regarding crypto compliance future and its implications.

How will crypto investors, exchanges, users, and other entities associated with cryptocurrencies evolve in the future? The future of cryptocurrency compliance needs a global regulatory framework applicable to precisely categorized groups of investors and crypto assets. Learn more about cryptocurrency compliance and the related best practices to prepare for the future right now.

## Smart contract security

Most Common Smart Contract Vulnerabilities And How to Mitigate Them

Smart contracts are an essential component for ensuring decentralized and automatic execution of transactions on blockchain networks. It primarily deals with transactions involving financial assets. On the other hand, it is important to know that common smart contract vulnerabilities could lead to big losses. As a matter of fact, smart contract vulnerabilities have been responsible for financial losses measuring over $12.3 billion. For example, the DODO DEX lost almost $3.8 million in March 2022 to a smart contract vulnerability. In April 2023, one of the popular DeFi platforms, Yearn Finance, lost $10 million due to smart contract flaws.

Smart contracts are responsible for transactions involving massive volumes of important data and assets, such as money transfers, service delivery, and access to protected content. As a result, they can be easy targets for hackers and other malicious actors. On the other hand, awareness of smart contract vulnerabilities could offer the opportunity to prepare for smart contract attacks. Let us learn more about some of the most common vulnerabilities of smart contracts and how you can resolve them.

Excited to learn about the critical vulnerabilities and security risks in smart contract development, Enroll now in the Smart Contracts Security Course

Popular Vulnerabilities for Smart Contracts and Mitigation Strategies

Security is one of the foremost priorities in the process of designing and developing smart contracts. The different types of smart contract attacks in recent times and their magnitude imply that smart contract security is a mandatory requirement for new blockchain and web3 solutions. On top of that, you could not make any changes in the smart contracts once they have been deployed to blockchain networks with different vulnerabilities.

Most important of all, the vulnerabilities of smart contracts are visible to everyone after they have been deployed on blockchain networks. Therefore, development teams and smart contract engineers must pay attention to the most important attack vectors for smart contracts. Here is an outline of the most common vulnerabilities in smart contracts and the strategies for mitigating them.

Oracle Manipulation

One of the prominent entries among vulnerabilities for smart contracts is Oracle manipulation. Smart contracts rely on oracles for accessing external data from sources outside the blockchain network. However, oracles can be responsible for smart contract security issues as malicious actors could manipulate oracles to achieve personal interests.

Oracles help smart contracts interact with off-chain systems. On the other hand, manipulated or inaccurate Oracle data could enable automatic execution of smart contracts. Such types of issues are classified as Oracle issues for smart contracts. The Oracle issue has been responsible for exploitation of different DeFi applications.

The most common example of such problems with smart contracts is visible in the flash loan attacks. Flash loans allow users to borrow any amount of cryptocurrency without any limit as long as they repay the loan in the same transaction. Attackers can use such loans to distort asset prices and generate profits without compromising the principles of blockchain technology.

You can find solutions to the Oracle issue for smart contracts with decentralized oracles, such as Tellor or Chainlink. Another recommended mitigation strategy for such risks points to the use of multiple oracles. Decentralized oracles or multiple oracles for one smart contract ensure accuracy of input data for the oracle. Such types of oracles increase the difficulty and cost of manipulating oracle data.

Certified blockchain security expert

Denial of Service

The most noticeable example of web2 attacks that have transitioned into the domain of web3 is denial of service. Smart contracts are also vulnerable to denial of service attacks. It is one of the common entries in a smart contract vulnerabilities list, which can create setbacks for users and reputation of web3 projects. The attack involves overloading a smart contract with services, such as authentication tasks.

As a result, the attacker could prevent other contracts from execution and lead to unexpected reverts. For example, denial of service attacks can return unused gas and revert the state of the smart contract to the state prior to execution of the transaction. Subsequently, the attacker could find that the results of an auction or values in financial transactions can be manipulated easily.

The promising approach to solving such types of smart contract attacks focuses on making the attacks costly. What are the proven ways to improve the cost of denial of service attacks for hackers? Higher gas fees and time-lock puzzles are some of the effective measures for increasing the costs of attackers. In addition, mitigation strategies for denial of service attacks also focus on making calls only to trusted contracts.

Timestamp Dependence

The collection of different types of vulnerabilities for smart contracts also includes timestamp dependence. It is important to note that the node executing the smart contract generates timestamp values. How does the timestamp lead to smart contract vulnerabilities, and what is their impact? The distributed nature of Ethereum creates difficulties in synchronization of time on every node. Since Ethereum is the preferred platform for developing and deploying smart contracts, it exacerbates the timestamp dependence issue.

Malicious nodes could manipulate the timestamp value for designing a logic attack. The logic attack would target contracts that utilize the block timestamp variable for execution of time-critical operations. You can resolve such vulnerabilities by avoiding the use of block timestamp function for control or logic checks. It is also important to refrain from using block timestamp function as a source of randomness.

Curious to understand the complete smart contract development lifecycle? Enroll now in the Smart Contracts Development Course

Reentrancy Attacks

Another common vulnerability in smart contracts is a reentrancy attack. The attack vector emerges from the imperative execution of Solidity smart contracts. Imperative execution implies that smart contracts must execute each line of code before the next line. It implies that the execution of the calling contract can be put on hold till the return of the call when the contract makes external calls to a different contract. Reentrancy attacks are one of the common additions to a smart contract vulnerabilities list, as the external contract could gain temporary control over the next sequence of events. As a result, reentrancy attacks lead to the creation of an infinite loop.

Assume that a malicious contract attempts a recursive call to the original contract to withdraw resources without completion of the first call. As a result, the original contract would never have the opportunity to update the balance before completing the function. The smart contract security issues with reentrancy could take the form of multiple types of attacks. Some of the common types of reentrancy attacks include single-function, read-only, cross-function, and cross-contract reentrancy attacks.

You can resolve problems with reentrancy attacks through careful design of external calls. It is important to note that such vulnerabilities arise from flaws in the code logic of smart contracts. Therefore, it is important to check and ensure updates on the state of the contract.

In addition, you can also find another proven safeguard against reentrancy attacks with a reentrancy guard. Reentrancy guards could prevent the execution of multiple functions at one instance by locking the contract. You can rely on smart contract audit tools such as Mythril and Slither for checking the presence of different variants of reentrancy attacks.

Want to know about the possible use cases of smart contract audits? Check out Smart Contract Audit Presentation now!

Frontrunning Attacks

Smart contracts are transparent, which implies that they are publicly visible on the blockchain network. Miners of a block could choose transactions with the highest gas fees. The priority fee is an effective tool for ensuring that you can have your transaction approved before other transactions.

However, it also leads to problems with smart contracts as attackers could front-run the profitable contracts through submission of an identical contract, albeit with a higher gas fee. Generally, attackers implement frontrunning attacks through bots or even miners.

You have to look for effective solutions to mitigate the risks of frontrunning attacks. One of the proven solutions for mitigating the risks of frontrunning involves accepting transactions that have the gas price below a specific threshold. You can also find a solution with a commit-and-reveal scheme in which users submit a solution hash first rather than a clear text solution. Malicious actors cannot view the solution before it is too late. At the same time, smart contract auditing tools can help in detecting frontrunning vulnerabilities.

Integer Overflows and Underflows

Arithmetic operations also play a role in creating vulnerabilities for smart contracts. Integer overflows and underflows are the most common smart contract vulnerabilities resulting from arithmetic operations surpassing the fixed range for the values. For the integer type uint8, the range of values spans from 0 to 255.

If the values are higher than 255, then they would overflow, and the value would be reset to 0. On the other hand, values that are lower than 0 would be reset to 255. As a result, the state variables of the contract and the logic could go through unexpected modifications and could trigger invalid operations.

The Solidity compiler, starting from version 0.8.0, would not allow code that could lead to integer overflows and underflows. It is also important to check the contracts that could be compiled with the earlier versions to support functions that involve a library or use arithmetic operations.

certified web3 hacker

Information and Function Exposure

Blockchain technology enables better accessibility for every individual. Sensitive and confidential information must be encrypted before they are saved to a blockchain network. However, transparency leads to different types of smart contract attacks due to visibility of functions and variables in smart contracts. As a result, the functions and variables would be open to abuse and misuse. You can find a solution to such issues with improvements in development workflow.

Developers must ensure the implementation of proper access controls. In addition, developers must also implement the principle of least privilege with the help of variable and function visibility modifiers in Solidity. The modifiers help in assigning minimum visibility levels according to the desired requirements.

Force-Feeding Attacks

The next prominent cause for smart contract security issues points to the problems with force-feeding attacks. Developers could not prevent smart contracts from receiving the native cryptocurrency of Ethereum, Ether. Malicious actors could utilize this vulnerability for force-feeding smart contracts with Ether.

The attack revolves around the premise of manipulating the balance of Ether in the smart contract. The change in balance of Ether could lead to manipulation of function logic that depends only on desired balance for internal accounting. Some of the internal accounting processes include paying out rewards when the balance exceeds a specific level.

The problem with such smart contract vulnerabilities is that it is difficult to stop the manipulation of smart contract balance. Therefore, it is important to ensure that the balance of the contract does not serve as a guard or check within a function. The actual balance of the Ether could be higher than the balance expected by the internal code of the contract.

Gas Griefing

Another prominent addition to the smart contract vulnerabilities list is gas griefing. Users should pay a gas fee for performing a transaction or executing smart contract on Ethereum blockchain. It serves as an incentive for the validators or miners to verify transactions. On the other hand, the price of gas depends on network capacity, supply, and demand at the time of transaction.

Gas griefing happens when users send the gas fees required for executing the desired smart contract. However, they don’t send the fees required for executing subcalls or the calls made by the contract to other contracts. It would lead to a significant influence on the logic of the smart contract.

The problem is that there is no proven technique for preventing gas griefing. Developers could find a solution by coding a contract for defining the amount of gas rather than the user. Such types of solutions are more likely to increase the chances of transaction failure.

Start learning Smart Contracts and its development tools with world’s first Smart Contracts Skill Path with quality resources tailored by industry experts now!

Final Words

The review of the different smart contract vulnerabilities and mitigation strategies shows that awareness could solve a lot of problems. You should understand the importance of smart contracts in managing valuable data and resources. Flaws in smart contracts could lead to security issues that impose the burden of financial losses.

Therefore, smart contract developers must prepare an effective risk management strategy and smart contract audit plan for identifying vulnerabilities. Learn more about smart contract fundamentals to obtain a first-hand impression of the potential sources of vulnerabilities in smart contracts.

## Incentive Design

ncentive Design & Tooling for DAOs

How to match a DAO's goals with the right incentive mechanisms to achieve them...

Aragon

• Nov 11, 2021 • 12 min read

Incentive Design & Tooling for DAOs

DAOs aren’t going away, they are the new operating system for coordination and are fully extendable in form and function via their app layer: DAO tooling.

DAO tooling is as hot as hell right now 🚀 and, frankly, I can’t remember seeing anything as explosive as the innovation and creativity within this space.

So Hot Right Now.jpeg

DAO tooling: So hot right now.

However, this Cambrian explosion of DAO tooling brings challenges in the short term: even experienced DAO operators are finding it impossible to keep up with all of the latest developments and experimentation in the space, so spare a thought for Web3 noobs or those roped into DAO operations to help out...

We Work for a DAO by Mistake

One area where we can share some insight is incentive design. This is valuable for many reasons, not least because good incentives can increase participation rates and a sense of ownership in all DAO operations. A DAO that is leaving too much work for too few people is not in good shape.

A Simple Model for Incentive Mechanism Selection

Showme.png

"Show me the incentive, and I will show you the outcome." - Charlie Munger

The power and insight of this statement is fully realized in Web3. But how do we show incentives not yet implemented or designed, which is a more common occurrence as new DAOs pop up and new community models rise from NFTs and fractionalization? Oftentimes we find that people brought together through these shared passions might share little else, making incentive design even more important.

We think that there is an opportunity here to help DAO operators identify their most important objectives before trying to decide which incentives to use or tools to experiment with. For example, sometimes teams and DAO’s ask us about experimenting with Coordinape, but without much understanding of what it does or how it works. Coordinape is a brilliant tool, but a better question to ask is whether Coordinape works well at incentivizing the type of action or behavior you need right now.

We propose that DAO’s should first ask the following question:

What are my DAO's specific needs? And which incentive mechanisms address them?

The following table cross-references important factors such as decentralization, complexity and impact with the key tools or incentives being used by DAOs today. They have been chosen because they focus on the following important inputs:

What are the most pertinent values or circumstances of your DAO?

What is your relationship to the contributor to be incentivized?

What is the nature of the work or activity to be rewarded?

Identifying your two or three most important factors can help to answer these questions and increase the speed at which you can identify the tools and incentive mechanisms most likely to help your DAO.

Here is the the table to help you identify and match characteristics with mechanisms:

Let’s dive more deeply into these factors and see why they might be important:

1. Decentralization of the Incentive

Does the DAO need a mechanism that is decentralized, or is some centralization compatible with your incentives?

This topic stirs great passion and while we all like the purity of decentralizing, sometimes "the perfect is the enemy of the good." There are excellent tools when you need incentives to be decentralized, and excellent tools when you can accept a more centralized approach. The answer for a well established DAO is likely to be different from a new one, as are the corresponding tools and mechanisms.

One other point to note is that some (de)centralization is a spectrum. For example, grants are sometimes distributed on a decentralized platform like Gitcoin, and sometimes by a decision committee in a hackathon.

2. Oversight of the Incentive

How much time and ability does the team have to oversee administration of the incentive mechanism?

This question can be very tricky. For example, bounties are an elegant solution for easily definable tasks with clear success criteria (e.g. Does the code run or not?). But a bounty needs to be defined, advertised, reviewed and rewarded, all of which takes DAO members' time and resources. It is possible that the gains from a simple bounty can be outweighed by the effort to define and execute it, but it is not guaranteed.

3. Reputation of the Contributor

How much connection or reputation does the potential contributor have in the DAO?

We long for the day when Rabbithole or others have perfected the on-chain CV, but until that time, different levels of participation or contribution zones might act as proxies for reputation.

We think it is possible to significantly narrow down this question to whether you need to know the reputation of a contributor or not. Anonymous, ad-hoc contributors can do many valuable tasks in a DAO without anyone knowing the slightest thing about them, which is one of the great things about permissionless Web3!

4. Definability of the Task

Is the task easily definable, and how can you determine whether it has been done or not?

Easily defined tasks can be packaged up and shared anywhere or with anyone, and often work well as bounties or grants. Other contributions are less well defined: someone may make many inputs over an epoch without them having been defined in advance, and the value realized only at the end. Whether the contribution can be defined is a good determinant for which mechanisms can be used.

5. Time Commitment to Complete

How much time does it take to do the required activity?

When you have been working in DAOs for a while, you realize the incredible value of people that consistently show up day after day. That said, someone spending a little time here and there really does add up. Guess what? You might need different incentives to attract one, or the other, or both.

6. Complexity to Complete

Is the work highly complex, either in the task itself or the skill required to get it done?

Highly complex tasks happen in DAOs every day and Web3 has normalized great achievements. But understanding the complexity involved can help you choose a good incentive mechanism: a genre-defining problem often requires a very different approach to something that just needs an extra set of hands.

7. Frequency of the Task

How often is the task or activity to be done? Is it just a one-off or is it repetitive and ongoing?

The answer to this is highly suggestive of mechanisms that might be suitable. For example, unique tasks might only need one-off incentives; repetitive tasks might need to scale so as not to become a drain on the treasury; and ongoing tasks might work better with mechanisms that encourage ongoing participation. Understanding which mechanisms work well in each of the examples above can save teams a lot of time when designing incentives.

8. Impact of the Task

Is the impact and visibility of this task wide or narrow?

DAOs (hopefully) pay for impact. But, incentives often work based on the visibility of such impact. We all know salt-of-the-earth DAO contributors who are the community's spiritual glue, but will their over-sized achievements be fully recognized in social graphs or mechanisms like Coordinape? These are really important questions when balancing different methods and approaches.

9. Value of the Task

Is this activity going to create value for the DAO?

If "Yes", then this needs to be incentivized appropriately and (hopefully) allow the team to realize some of the upside. If not, more discrete or packaged rewards might be more appropriate.

10. Urgency of the Task

How urgent is the activity to be done, relative to everything else?

If tasks are urgent, incentives should enable the rapid deployment of rewards, or be of a sufficient scale to attract talent. If less urgent, rewards might be packaged up into a cyclical reward mechanism or rewarded passively through algorithmic tools.

11?

There is also a possible 11th factor, which is when the reward needs to be paid. Big upfront commitments with the 'hope' of later rewards and recognition can be very weak mechanisms when work is plentiful and good contributors are scarce. Understanding if you can pay immediately, in tranches, or at completion might be a relevant and important factor for you and your DAO.

The trade-offs and synergies in these decisions can get quite complex. What we have shared in the table is non-exhaustive and fully hackable. Each context can be unique, even if the tools themselves are not. Finally, we want to note that we have primarily focused here on extrinsic and financialized incentive mechanisms, and will share more on topics of intrinsic motivation and incentives another time.

state\_01.png

The State of Incentive Mechanisms and Tools

The State of Incentive Mechanisms and Tools

Now that you have identified your key needs and the mechanisms that might work well, we provide a brief overview of each. As noted earlier, the pace of DAO tooling innovation is inspiring and this list is not exhaustive, but we do hope it helps to get you started.

POAPs & NFTs

Key benefits or use cases: Allow access and gating, build reputation, low cost.

Challenges or limitations: Non-financial, work only in specific use cases.

Proof of Attendance Protocol (POAP) creates NFTs that signify your participation or attendance in activities. They are fast becoming a way of recording your working life and building your on-chain CV. Rabbithole.gg uses NFTs in a similar manner and rewards you for completing quests or undertaking specific actions. And most of us know how well Mirror works at creating ownership and access at the genesis of ideas or new publications. All three are becoming core components in the ecosystem to align incentives and encourage deeper exploration.

Tool providers: POAP.xyz , Rabbithole.gg, Mirror.xyz

Tipping & Tips

Key benefits or use cases: Real time recognition, good for unplanned value creation.

Challenges or limitations: Very centralized, good when targeted but does not scale well.

Tipping might be viewed as absurd in most of the non-US world, but in the context of DAO’s, tipping can be a very valuable and healthy mechanism to help a DAO scale. Tips are often used more like airdrops (care-drops?) and their superpower is that they can reward value creation very rapidly, especially when unplanned but easily identifiable. Also, tipping requires zero reputational knowledge of individuals, allowing anyone in a DAO to contribute and be tipped.

While it remains a centralized process (i.e. the tipper has all power) peer-to-peer approaches to tipping in the Bankless DAO and TEC Praise system are starting to emerge. Our favorite example is the curation mechanism at Forefront. Each day, DAOists curate articles for the Forefront newsletters and communications in a shared Discord channel, with the best receiving tips. This creates a virtuous participation circle and shows what is possible when very simple mechanisms are used wisely.

Tool providers: Tip.cc , Collab.land, Coinvise

Algorithmic Network Analysis

Key benefits or use cases: Decentralized, algorithm removes manpower needs.

Challenges or limitations: Tech solution - requires dev experience, algorithm brings new challenges.

Sourcecred is an algorithmically objective network analysis system. Simply put, it enables participatory actions and recognition workflows to be created such that the algorithm makes calculations around how value has been created and accrued. Think of it as a bot keeping score of actions, impressions and other activity in Discord, Github and community forums like Discourse. The greatness of this system is that it removes much of the daily administrative burden for DAO operators and is decentralized - no-one is making decisions about allocation. On the flipside, detractors would say that, used unwisely, any algorithm can become a weapon of math destruction, and that without human oversight it is possible for people to “farm” cred. However, if you have a thriving community with a few developers that can keep an eye on it, it's actually a pretty cool and valuable tool.

Tool provider: Sourcecred

Coordinape

Key benefits or use cases: Decentralized, prosocial, uncapped rewards (up to pool total).

Challenges or limitations: Uncertainty of reward for contributors.

Coordinape is the darling of the ecosystem right now and rightly so - it represents many of the best elements of Web3, decentralization and is a true digital native solution.

Coordinape is a decentralized, pro-social recognition tool that moves recognition from leaders to teams. It works by allocating tokens to each participant, who award them to their peers during 'epochs'. At the end, an individual's proportion of tokens is converted into their proportion of financial rewards allocated from the treasury. There are many powerful mechanisms at play, such as promoting the acts of giving and recognition amongst teams, as well as removing capped individual recognition in favor of uncapped rewards from across the whole pool. It’s no wonder that so many DAOs - including some of the largest and most successful - are already using it.

Tool provider: Coordinape

Bounties

Key benefits or use cases: Discrete or one-off tasks, easily definable completion, doesn't require reputation.

Challenges or limitations: Brings overheads, not good for work that is hard to define.

We think that bounties are a very meaningful part of the ecosystem and are likely to grow in importance over time. The reason for this is that most legacy work practices have a high focus on 'roles' - essentially 'employment' - while DAOs are disassembling work into individual tasks or activities to be done from the crowd. This atomic view of tasks is likely to become a DAO superpower as the mechanisms for effectively executing them at scale begin to emerge.

Bounties have their own superpower, in that they work exceptionally well when the tasks are relatively easy to define and the success criteria are well known. But this is not the only context, and we are inspired by the example from Badger DAO who have turned their entire intern program into a bounty. Earning a living as a Web3 'bounty hunter' is now a viable option via Gitcoin and impressive growth hacking mechanisms like Layer3, or simply signing up to this bounty newsletter.

Tool providers: Gitcoin, Layer3

Grants

Key benefit or use cases: Large complex tasks, pay for completion, attract new participants.

Challenges or limitations: Not great for small tasks, high operational effort.

Grants are becoming a staple of the industry for large scale, complex, or highly specialized needs. They are essentially operating like a contingent work model for DAOs, inviting in new cross-functional teams or specialists to support the activities of the core contributing team. They are a way to attract new or unique capabilities and allow the DAO to scale and build more quickly than otherwise possible.

Thinking of composability, we think grants might be a key step towards creating DAO to DAO interlocks and collaborations for highly complex tasks. Grants programs are, however, complicated and have a significant overhead for the core teams in terms of their management and administration, not only in allocating the work, but in ensuring milestones and final deliverables are met.

Tool providers: Gitcoin

Streams

Key benefit or use cases: Reward ongoing commitment, real time - pay by the block.

Challenges or limitations: Does not make sense for small discrete tasks.

Streams are likely to become the salaries of Web3 because they have many of the same unique properties but provide a more digitally native and logical solution. These programmable cash flows can deliver payments block-by-block to contributors or other parties. For this reason, they are a great way to reward long term contributors and break the “monthly payment” model institutionalized in much of Web2.

The limitation of streams might be that they operate like salaries, rewarding contributors without the direct and visible link to value creation in the way some of the other mechanisms provide.

Tools: Superfluid, Sablier

KPI Options

Key benefit or use cases: Reward over-achievement, shared upside for contributors, pay for results.

Challenges or limitations: Result needs to be defined upfront and be publicly verifiable.

KPI options are an exciting mechanism and fertile ground for experimentation. They provide the ability to incentivize results and output in binary and non-binary ways, with the potential to scale rewards proportionately to impact.

One example could be to incentivize via an option that becomes deeper 'in the money' as the impact generated by the work increases. This is a very powerful model for DAOs because it allows participants to truly share in the upside of their work in ways not fully expressed in many legacy institutions or corporations.

Of course, KPI options bring their own complexity, require highly specific design upfront, and are highly reliant on having a publicly verifiable measure against which the contract can be executed.

Tools: UMA

In addition, a number of excellent tools exist to help payment of these rewards to reach contributors. These include but are not limited to: Disperse, Parcel and Utopia. There are also exciting developments and experiments taking place across the ecosystem, which are beginning to explore powerful new functions by integrating different tools, blurring the lines between the mechanisms and tools.

In closing, we are sharing this here as a guide to empower you to explore some tools that might be valuable and not to restrict your thinking about what is possible. Badger’s internship is a bounty, but others might reward internships via Coordinape or Streams or something else, and all would be equally valid given the unique DAO contexts. This is one of the best qualities of Web3: the ability to reimagine and redefine how we want work to work. Hopefully our sharing here has given you some inspiration to reimagine what’s possible.

## The Basics of Evaluating Cryptocurrencies

“Tokenomics” has become a popular term in the last few years to describe the math and incentives governing crypto assets. It includes everything about the mechanics of how the asset works, as well as the psychological or behavioral forces that could affect its value long term.

Projects with well-designed tokenomics are much more likely to succeed in the long term because they’ve done a good job of incentivizing buying and holding their token.

Projects with poor tokenomics are doomed to failure, as people rapidly sell the tokens at the first sign of trouble.

If you’re considering whether or not to buy a crypto asset, understanding the tokenomics is one of the most useful first steps you can take to make a good decision.

So as someone who’s been writing about DeFi for nearly a year now, and who designed the tokenomics for a popular crypto videogame, here’s what I look at when I’m evaluating the tokenomics of a new project.

It All Comes Down to Supply and Demand

As in normal economics, the two forces we are most interested in are Supply and Demand. Understanding how those are baked into the tokenomics give us a good sense of how desirable a given token or cryptocurrency should be.

Supply: Emissions, Inflation, and Distribution

Let’s start on the supply side since it’s a little easier to understand. The main thing you’re trying to figure out is:

Based on supply alone, should I expect this token to hold or increase its value? Or will that value be inflated away?

On the supply side, a token will increase in value if fewer of those tokens exist—we call that deflation. A token will decrease in value if more of them exist—that’s inflation. When you’re evaluating the supply side you don’t have to worry about things like whether the token has any utility, or whether it will generate income for its holders. You’re really just thinking about the supply and how it will change over time.

The questions you want to ask are:

How many of these tokens exist right now?

How many will ever exist?

How quickly are new ones being released?

Bitcoin was created with a simple supply curve that is emitted over about 140 years.

Source

There will only ever be 21,000,000 bitcoin, and they’re released at a rate that gets cut in half every four years or so. Roughly 19,000,000 already exist, so there are only 2,000,000 more to be released over the next 120 years.

That means 90% of the supply is already in circulation, and here will only be 10.5% more bitcoin 100 years from now, so you shouldn’t expect any serious inflationary pressure bringing down the value of the coin.

What about Ethereum? The circulating supply is around 118,000,000, and there’s no cap on how many Ether can exist. But Ethereum’s net emissions were recently adjusted via a burn mechanism so that it would reach a stable supply, or potentially even be deflationary, resulting in somewhere between 100-120m tokens total. Given that, we shouldn’t expect much inflationary pressure on Ether either. It could even be deflationary.

Dogecoin has no supply cap either, and it is currently inflating at around 5% per year. So of the three, we should expect inflationary tokenomics to erode the value of Doge more than Bitcoin or Ethereum.

The last thing you want to consider with supply is allocation. Do a few investors hold a ton of the tokens which are going to be unlocked soon? Did the protocol give most of its tokens to the community? How fair does the distribution seem? If a bunch of investors have 25% of the supply and those tokens will unlock in a month, you might hesitate before buying in.

What about some DeFi tokens? Yearn, one of the first DeFi protocols I wrote about, has a fixed supply of 36,666 YFI. There are no emissions and no inflation, so you shouldn’t expect the value of 1 YFI to decrease from inflationary pressure.

Meanwhile, Olympus, a protocol I wrote about more recently, has an insanely inflationary printing schedule with huge amounts of new OHM tokens being printed every day. So theoretically you should expect holding OHM to be a bad bet. But as we’ll see shortly, Supply alone is not enough to understand whether holding a token is worthwhile.

Those are the main considerations for Supply. Now demand is where things get more interesting.

Demand: ROI, Memes, and Game Theory

I could go into my backyard, break a few rocks, and then say they’re the only rocks I’m ever going to break and put up for sale. I have a fixed supply of 10 rocks. 0 inflation rate. So they should be worth millions, right?

Well, no, because no one wants my broken rocks.

At this simple level, there’s nothing inherently different between my rocks and Bitcoin. Having a fixed supply alone does not make something valuable. People also need to believe it has value, and that it will have value in the future.

If you want to know whether a token will have demand-side value in the future, you’ll want to look at return on investment (ROI), memes, and game theory. Let’s start with ROI since it’s the easiest.

Return on Investment

ROI in this case is not how much you think the token price will go up. It’s how much income or cash flow the token is able to generate for you simply by holding it.

For example, if you hold Ether you can stake it to help secure the network once Proof of Stake launches. In return for Staking your ETH, you get paid in more ETH, at a rate of about 5%.

Some tokens allow you to tap into the earnings of the protocol they represent. If you hold SUSHI, you can stake it to earn a share of the Sushi protocol revenues, currently for about a 10.5% APR.

Another form of ROI comes from “rebasing,” similar to a stock split where by holding a token and staking it, you continue to get more of that token as the protocol inflates its supply. This is how Olympus works and is why their heavy inflation rate is not necessarily a bad thing since you can retain the share of the protocol that you own.

ROI is important to consider because if a token has no intrinsic ROI or cashflows, then it’s harder to justify holding it. You have to believe other people’s belief in the number going up is enough to sustain it.

Or, you have to believe the memes.

Memes

The other reason people might want a token is simply the belief that other people want the token, and will want it in the future.

You can call it faith, conviction, or memes, but, whatever you call it, the machine that generates belief in the growth of future value is always going to be an important consideration.

How do you evaluate this though? Everything else in the tokenomics has been pretty measurable, but memes? This is one that requires you to hop into the community and get a feel for it.

What’s the energy like in their Discord? How active are they on Twitter? Do people make this token or protocol part of their identity? How long have people been active in the community?

Belief in future value is often one of the most powerful drivers of demand. Bitcoin has no cash flow, no staking rewards, nothing. It just has the belief that it could be a long term store of value to rival gold. Or more ambitious beliefs like definancialization and hyper-bitcoinization. But it’s all beliefs at the end of the day.

So while it’s tempting to be purely analytical, don’t discount how far a token can get with faith, clever memes, and a cult-like following.

There’s a third element here to demand which can combine parts of memes and parts of ROI. Let’s call it Game Theory.

Game Theory

Game Theory asks you to consider what additional elements in the tokenomics design might help increase the demand for the token. This is where tokenomics can get particularly complex, and is the main area I’ll focus on in the followup “102” version of this post.

But one common version of good tokenomic game theory is lockups. The protocol creates an incentive for locking your tokens in a contract, usually in the form of greater rewards.

The classic example of this is Curve.

Similar to Sushi, you can lock your CRV tokens to earn a share of the protocol revenue. But the longer you lock your tokens for, up to 4 years, the greater your rewards.

In addition, the more tokens you have locked and the longer you have them locked for, the lower your fees when you use all the other parts of Curve.

So Curve has exceptionally strong incentives and game theory around holding its token. You can earn a decent ROI from staking it, and you can earn a higher ROI from all other parts of the app. And you earn the most by locking up your tokens for four years, which dramatically reduces the incentives to sell CRV.

Tokenomics in Practice: Evaluating a Project

Now that you know the main questions to ask, let’s go through the process of evaluating a project.

We’ll start with one of my favorites: Convex Finance.

Convex Finance

Convex is a platform that sits on top of Curve (above) and helps you earn a higher yield by aggregating many investors together. It lets you earn most of the higher yield you would get on Curve if you had locked up thousands of CRV tokens for 4 years, without having to do the locking yourself.

By hopping into their docs, we can start to answer the questions I laid out in this article.

Supply

Convex has a fixed max supply of 100m which will be released overtime at a decreasing rate, depending on CRV deposits.

According to Coingecko, 78.5m of those 100m have already been created, meaning the current supply will inflate by another ~33%.

Of those tokens, the vast majority are going to the people using Convex. So this is a very fair token distribution, only a comparatively small amount is being retained for the team and investors. For comparison, imagine if Amazon gave away 75% of its stock to people who used Amazon:

So there’s a fixed supply, the remaining supply is being released at a decreasing rate, most of the tokens are going to the community, and there’s a max 33% dilution from here. Things look pretty good on the supply side.

What about demand?

Demand

To evaluate demand you need to ask: why would you hold the CVX token?

By holding the CVX token, you get a share of all Convex Finance revenue. That’s not a huge amount, but it earns about 4% right now:

That’s not all, though. You can also lock your CVX tokens for 16 weeks at a time, and when you do so, you get bonus rewards from various protocols who want to reward Convex stakers:

Here the APR is still just 5%, but that’s not including the bonus rewards you get from other platforms:

And on top of that, you can delegate your Convex to other voters, in return for “bribes” using the service Votium.

So there is a pretty significant ROI on staking your CVX tokens, even if the value doesn’t change at all. And it has very strong game theory supporting holding the token, since you only earn these rewards if you lock your tokens for 16 weeks at a time.

The memes aren’t as strong since it’s a somewhat boring back-office DeFi protocol. But they don’t need to be. It’s a cash flow machine.

So Convex has a fixed supply, which is mostly allocated to the community. Most of the tokens are in circulation, and there won’t be much more inflation. Holding CVX is heavily rewarded via protocol fees and other rewards to token holders, so there’s less reason to sell if the price dumps.

To me, this is one of the better tokenomics designs out there, and a fantastic example of a well designed project. All the pieces come together to design a robust financial incentive system that doesn’t rely on faith to prop up the value.

Evaluating on Your Own

This should give you a good initial foundation to evaluate any new project you come across. By reading the docs or whitepaper, you should get a good sense of how the supply is going to be managed, and what forces will drive demand for the token or cryptocurrency.

And the question to keep in the back of your mind isn’t necessarily “will this appreciate against the dollar?” but “Will this appreciate against (BTC, ETH, SOL, whatever you prefer)”. Most crypto assets are highly correlated and move together, and if you’re holding anything besides the big foundational coins, it should be based on some belief that its tokenomics and incentives will result in it outperforming the base currencies it's built on.

## Tokenomics Basics

Tokenomics is one of the most popular terms when it comes to crypto investment, but not everyone understands it thoroughly. The phrase seems theorized simple at first sight but the deeper you dive in, the more complicated it becomes.

That is why in this article, I will introduce you to the insightful information of Tokenomics, including:

The definition of Tokenomics and how Tokenomics is classified.

How Tokenomics plays an important role in crypto in general and DeFi in particular.

Different aspects to evaluate the Tokenomics.

The components of a complete Tokenomics.

How Tokenomics affects the productivity of a project.

Some case studies of an efficient Tokenomics, as well as an inefficient one.

As there will be a lot of specialized insights, it is advised to take note of some useful points for yourself. Now let's begin.

Disclaimer: The purpose of this article is mainly for providing constructive information and personal viewpoints, not financial advice.

What is Tokenomics?

The term Tokenomics consists of two words: Token and Economics . Therefore, the word Tokenomics can be defined as the tokenized version of economics, or how crypto tokens can be developed and applied to the economics of a project.

Why does Tokenomics matter?

Before answering this question, let's go through a small quiz together.

Take a look at the picture below and imagine the crypto market as a game of cards. There are many players in that game, such as:

Developer: Andre Cronje, Vitalik Buterin,...?

Market Maker: CZ Binance, Sam FTX,...?

Major Venture Capitals: a16z, Multicoin, ParaFi,...?

Retail Investors: Most of us (including me).

Who controls the crypto game of cards?

So, who is the closest to the table? Who controls the game? In the picture, if even Justin Sun cannot approach the game, then retail investors like us are just spectators who are waiting for the result.

In fact, that turns out to be the truth: We are playing the game created by Market Makers, Builders/Developers and top Venture Capitals. From the ICO/IEO/IDO trend to the NFT, GameFi trends across multiple blockchains and ecosystems.

The next question is, how can they control the game? The answer is tokens. Token is the product that investors can use to trade and put faith in. However, tokens are also made by reputable Developers, Builders, and Market Makers. As we all know, the crypto market is a Zero-sum game, and surely everyone wants to gain profit. Then who will lose money?

In order to make money and understand what Market Makers are doing, you have to understand how a token operates, or in other words, you have to understand the Tokenomics.

Let's continue to find out the way big names operate the Tokenomics.

The components of a Tokenomics

Coin/Token Supply

Before, Total Supply and Circulating Supply are the two frequently used definitions. However, both Coingecko and CoinMarketCap have recently complemented a new term: Max Supply, which is rather confusing.

I will explain further with visual illustrations so that you understand these phrases more easily.

Some basic Token Metrics.

1. Total Supply is defined as the total number of the circulating tokens plus the locked tokens, minus the burned tokens. The Total Supply is initially determined by the developer team so that it can suit the project perfectly.

To be more specific, there are 2 types of Total Supply:

Fixed Total Supply: The Total Supply is predetermined and cannot be changed. For example: The Total Supply of Bitcoin is 21 million BTC, the Total Supply of Uniswap is 1 Billion UNI,...

Unfixed Total Supply: The Total Supply can be changed depending on the project features, which can be further divided into:

The Total Supply increases due to mining. For example: ETH tokens are mined corresponding to the Ethereum Network's performance, or CAKE tokens are minted when users participate in Farming activities on Pancakeswap,...

The Total Supply relieves due to burning. For example: The initial Total Supply of Binance Coin was 200 million BNB, which has been burned to 100 million BNB over time,...

The Total Supply constantly changes due to the Mint and Burn model. For example: The Total Supply of stablecoins, such as Algorithmic Stablecoin (FEI, AMPL,...), Crypto-backed Stablecoin (DAI, VAI,...), Centralized Stablecoin (USDT, USDC,...).

2. Circulating Supply is defined as the total number of tradable tokens circulating in the market.

3. Max Supply is defined as the total number of tokens that can possibly be reached in the future.

4. Analyze Token Supply

Analyze the Token Supply of 3 different tokens/coins.

Here are the Token Supply metrics of 3 different coins/tokens:

ETH : The Ethereum token has no Max Supply and will only be minted when there exists the demand of using the Ethereum Network. After being minted, ETH will circulate without being locked by any parties (Circulating Supply = Total Supply).

SRM: Serum was designed with the Max Supply of 10 Billion SRM. At the moment, the number of SRM can only reach 161 million SRM (Total Supply), however, only 50 million SRM are currently circulating in the market (Circulating Supply).

NEAR : The Token Supply of Near Protocol is the most basic and most frequently seen. Initially, the Max Supply = the Total Supply and NEAR tokens will be unlocked until the 1 Billion NEAR is reached (Circulating Supply).

Market Cap & Fully Diluted Valuation

Analyze the Market Cap and the FDV of a token/coin.

Market Cap is the total market value of a project relative to its token's Circulating Supply. We can calculate the Market Cap with the Circulating Supply by applying the formula:

Market Cap = Circulating Supply \* Token Price

Fully Diluted Valuation (FDV) is the total market value of a project relative to its token's Total Supply. We can calculate the FDV with the Total Supply by applying the formula:

FDV = Total Supply \* Token Price

Why is Market Cap more important than Price?

Currently, the price of a token depends on various factors. Besides Fundamental Analysis, it also depends on the Circulating Supply of that token. For instance, considering a token A with a $10,000,000 Market Cap:

If the Circulating Supply is 10,000,000 A token => 1 A token = $1.

If the Circulating Supply is 10,000,000,000 A token => 1 A token = $0.001.

The number of circulating tokens can range from thousands to billions, but the Market Cap is arguably the key factor to have a direct effect on the growth of a token or project.

For example: In the case of Aave and Compound, by using Fundamental Analysis, we can assume that both projects have equal potential in the Lending sector. As a result, the Market Cap of Compound can possibly reach that of Aave.

In terms of their price, one COMP token is worth more than one AAVE token. However, COMP has a higher growth potential as the Market Cap of Compound is lower than Aave. If the Market Cap of the two becomes equal, the price of a COMP token will reach $735.

The misunderstanding about Market Cap and Price.

Token Governance

At the moment, there are more than 10,000 coins and tokens. Still, not every token follows the Decentralized model as Bitcoin, and there will be a number of tokens/coins that are governed by the Centralized model. I will filter the tokens into 3 basic types:

The Token Governance of some tokens/coins.

Decentralized: Decentralized tokens are completely governed by the community and do not attach to any organizations. For example: Bitcoin, Ethereum,...

Centralized: Centralized tokens are governed by a leading organization who has full control over the token metrics and its underlying project. Usually, this is the case of Full-backed stablecoin projects such as Tether, TrueUSDm,... or Centralized Exchanges such as Huobi, FTX,...

From Centralized to Decentralized: There are still some coins/tokens that were originally centralized, but their governance power was later delegated to the community.

For example: At first, Binance Coin was totally governed by Binance. However, a while after the launch of Binance Smart Chain and the “Validator Spotlight” program, Binance gradually decentralized the BSC network and the BNB token, which gave users the governance rights.

Token Allocation

Before investing in any token, it is imperative that you look over its Token Allocation - an important metric that shows you how the tokens are distributed among Stakeholders, whether that distribution is reasonable, and how it can influence the project.

The Token Allocation of some tokens/coins.

1. Team

This is the allocation reserved for the project's developer team, which includes constructive contributors like founders, developers, marketers, advisors,... An ideal portion would be about 20% of the Total Supply.

If the allocation is too small , the team will have no motivation to develop the project in the long run.

If the allocation is too huge , the community will have no motivation to hold the tokens since they are overwhelmingly manipulated by one party. The team will have the full ability to govern the protocol in a centralized manner, or navigate the token's price at their will.

2. Foundation Reserve

This reserve will be used to develop the project or its products in the future. There is no specific standard for this part, which normally accounts for 20-40% of the Total Supply.

3. Liquidity Mining

The allocation for Liquidity Mining has appeared a lot recently, especially since the hugely DeFi trend from September 2020. The tokens allocated for this section are minted as incentives for Liquidity Providers across multiple DeFi protocols.

4. Seed Sale/Private Sale/Public Sale

The tokens saved for this portion are used in fundraising events, which commonly include the Seed sale, the Private Sale, and the Public Sale.

5. Airdrop/Retroactive

In order to attract early adopters, projects often airdrop a small number of tokens (usually 1-2% of the Total Supply) to users.

Before 2019, the requirements to participate in an Airdrop were just simple actions such as Like, Follow, Retweet the project's posts on Twitter.

However, since 2020, partaking in an Airdrop has required much harder objectives, forcing users to “skin in the game”, directly use and interact with the products to receive Airdrop or Retroactive rewards. Some well-known cases can be listed as Uniswap (UNI) , 1inch Network (1INCH) ,...

6. Other Allocations

This allocation can be flexibly adjusted depending on each project, and whether it is used for Marketing, Strategic Partnership, or any other expenses. Naturally, this portion only accounts for a small percentage of the Total Supply.

We can notice the difference between 2 different periods:

2017 - 2018: Publics Sale accounts for more than 50%, Insiders accounts for less. For instance: ADA, ETH, XTZ, ATOM,...

From 2019: Public Sale accounts for 20-30%, Insiders accounts for the highest portion. For instances: NEAR, AVAX, SOL,...

Whereas:

The Public Sale allocation is exposed to the community.

The Insiders allocation is exposed only to the team, backers,...

The reason behind this is that the token of a project used to have fewer use cases and the developer team needed a fund to start with. But now, the crypto market has witnessed the appearances of numerous venture capitals and the tokens have been available on different blockchain platforms, which explains why the Insiders and the Foundation now hold the majority of the tokens.

The difference in Token Allocation of some tokens/coins before and after 2018. Source: Messari.

Token Release

Token Release is the plan to distribute the tokens into circulation. Similar to Token Allocation, Token Release has a huge impact on the token's price as well as the community's motivation to hold the tokens. There are 2 types of Token Release at the moment:

1. Release tokens on schedule

Although the Token Release schedule varies between different protocols, it can be split into 3 types:

The Token Release schedule of some tokens/coins.

Under 1 year: Projects release 100% tokens in 1 year or less shows that their developers and team are not dedicated, and they are not willing to create any long-term value for the project.

From 3 - 5 years: This is an ideal timeframe to fully release the tokens, as the crypto market is changing at a rapid pace. Counted since 2017 - the time when it started to be “Mainstream”, the crypto market is now only 5 years old.

After each year, the market has eliminated a variety of inefficient projects, at the same time maintaining the productive ones. That is why 3-5 years is such a perfect number, as it stimulates not only the team's motivation to grow, but also the community's motivation to continuely support the project.

Over 10 years: Except Bitcoin, every project that produces a 10 year or more Token Release schedule will have difficulty in motivating either developers or holders, since they have to undergo the token's inflation for over 10 years. It is uncertain that the team can productively grow the project for such a long time.

To conclude, the Token Release needs to be designed in a way that satisfies 2 core elements:

The benefits of token holders.

The tokens' value when they are released (inflation).

If the tokens are released faster than the product's work rate, their price will decline due to inflation and token holders will lose interest.

2. Release tokens on demand

To deal with the possible inflation, some projects decide to release tokens on a flexible standard instead of a specific timeframe. This will help the projects make necessary adjustments according to the situation.

For example: MakerDAO does not have a specific Token Release schedule. Depending on the practical demand on the platform, the number of MKR tokens will be modified reasonably such that MKR tokens are only released when there are Lending/Borrowing activities.

Token Sale

Token Sale can be considered similar to the fundraising events in traditional markets, whereas companies raise funds by selling their shares. In the crypto market, the shares will be replaced with tokens.

While traditional companies usually hold 5 fundraising rounds, crypto projects only have 3. The business valuation can vary between disparate sectors, areas and scales. However, it is a common belief that in the Series C, promising companies can be valued at more than $100 million.

Traditional Companies: Pre-seed, Seed, Series A, Series B, Series C.

Crypto Project: Seed, Private Sale, Public Sale.

The average business valuation in the crypto market is lower because this market is fairly new, and its Market Cap is still much smaller than that of the stock markets in developed countries.

The process of selling tokens/coins from the Seed sale to the Public sale.

1. Seed sale

Seed sale is the first Token Sale of a project. In this round, the products of most projects are still under development. The seed sale can be considered as the initial fundraise for some projects to start.

Most venture capitals participating in seed sales accept a high risk investment. In return, they can potentially receive high rewards if the project succeeds.

2. Private sales

If the participants in the seed sale are mostly risk-taking capitals, the private sale testifies to the appearance of bigger and more famous ones. Most projects in this round have introduced their products and demonstrated their potential after the seed sale.

3. Public sale

Public sale is the fundraising round for the community. The projects can launch tokens in the form of ICO as in 2017, or through a third-party in the form of IEO or IDO.

4. Fair token distribution

However, some projects do not organize any Token Sale rounds, but rather distribute their tokens through Testnet, Airdrop, Staking, Liquidity Providing,... In this way, the project becomes more “fair” in the eyes of the community, therefore becomes more accessible by public users.

Some famous Fair-launch projects are Uniswap (UNI), Sushiswap (SUSHI), Yearn Finance (YFI),... They did not raise funds by any means; instead, they distribute their tokens to the actual users and supporters.

Some pros and cons of this model:

Pros: Tokens are fairly distributed to the valuable contributors of the project, ameliorating the situation of seed sale & private sale investors “dumping” tokens.

Cons: The project may perhaps “miss” a portion of the funds that could be used to develop the products.

5. The influence of Token Sale on Tokenomics

There are no common standards for the price difference between each Token Sale round. The token price in the public sale can be twice as high as that in the private sale, whilst the token price in the private sale can be twice as high as that in the seed sale. It completely depends on the project.

However, it is mandatory that they keep it at a rational ratio. If the price difference between each sale round is too massive, the early investors will have the tendency to sell their tokens early. On the contrary, later investors will lose interest in joining other Token Sale rounds.

In addition, projects will implement the “Token Release” feature to treat investors more equally: Tokens that are bought at a lower price will have to be locked for a longer period; in contrast, tokens that are bought at a higher price will be unlocked earlier.

Token Use Case

The Token Use Case is the applications and purposes of that token. It is the most important factor of a Tokenomics, which indicates how a token can be used and how much its price should be based on the benefits it brings to token holders.

Some Token Use Cases.

Tokens are commonly used for:

1. Staking

Most projects support Staking with their native tokens, which incentivizes more token holders as they can earn extra tokens with Staking.

Staking requires users to lock their tokens inside the protocol, reducing the number of circulating tokens on the market, therefore positively affecting the price of that token. With networks using the Proof-of-Stake mechanism, the network becomes safer and more decentralized as the number of staked tokens increases.

For example: Cardano (ADA) grew from $0.2 to $2 (+1,000%) in 2021. Theoretically, that means the money put into Cardano has to be 10 times larger.

However, this is not the case. The reason behind that growth is because 75% of the Circulating Supply has been staked, which reduces the circulating ADA and the sell pressure on the market, thus stimulating the growth of ADA.

2. Liquidity Mining (Farming)

Users can provide liquidity in DeFi protocols to receive the project's native token as a reward.

For example: Provide liquidity for Uniswap to receive UNI,...

3. Transaction fees

To perform a transaction, users have to pay a small amount of transaction fee to the Validators who are confirming your transaction. Each blockchain uses a separate native token as payment for the transaction fee (usually blockchain platform projects). For example:

Ethereum uses ETH.

Binance Smart Chain uses BNB.

Solana uses SOL.

Polygon uses MATIC.

4. Governance

As mentioned above, the platform can be either Centralized or Decentralized, depending on the project's decision. That being said, most DeFi protocols now follow the Decentralized governance model.

As a result, token holders have the right to propose ideas and vote on the platform. The suggestions can be related to transaction fee, Token Release schedule, or more serious issues such as expanding the project to another blockchain.

Currently, prominent DeFi platforms like Uniswap, Sushiswap, Compound,... have applied the Decentralized Governance model. However, a major part of the community is only allowed to vote instead of adverse changes, as the number of tokens required for this permission is too high.

5. Other benefits (Launchpad,...)

Some projects have recently complemented the Launchpad feature into their products, which requires users to stake their tokens to participate in Token Sale events on the platform, or in lottery events to receive NFTs,...

For example: Polkastarter requires users to stake POLs, DAO Maker requires users to stake DAOs,...

Tokenomic Case Studies

Disclaimer: These are only personal viewpoints, and should not be considered financial advice under any circumstances.

Note: Tokenomics is an imperative metric to evaluate a project, but it is only one among many other aspects. It is not the sole factor that has a direct impact on a token's price.

I will mention some efficient as well as some inefficient Tokenomics case studies so that you can easily understand.

Efficient Tokenomics

1. Binance Coin (BNB)

Token Supply

Initial Total Supply: 200,000,000 BNB.

Token Release schedule: 5 years (now 100% unlocked).

The token burning mechanism is applied until the Circulating Supply becomes 100,000,000 BNB.

⇒ Deflationary, create motivations for the token price to increase and for BNB holders to believe in the project.

Token Use Case

Still, Token Supply is not the main reason for BNB's tremendous growth lately, but rather how BNB tokens were designed to be used on both Binance Exchange and the Binance Smart Chain network.

Binance Exchange: Reduce transaction fee, participate in Launchpad, Staking, Lending & Borrowing, Derivatives,...

Binance Smart Chain: Native token, pay network costs, stake and farm (using BNB as the indispensable token when creating a liquidity pair, a similar situation as ETH on Ethereum, which is the key leading to BNB's growth).

Binance is also developing Binance Pay, which can lead to BNB becoming one of the most popular payment currencies if Binance Pay succeeds in the future.

The result: The BNB price went sideways at $20 until it dramatically increased to an ATH of $650 (+3,250%) and now remains at approximately $300 (+1,500%).

You can see more details about BNB's tokenomics right here .

BNB price's growth due to its design.

2. Pancakeswap (CAKE)

CAKE is the native token of Pancakeswap - an AMM DEX on Binance Smart Chain.

Token Supply

CAKE has no Total Supply (The number of CAKE is unlimited).

530,000 CAKE tokens are distributed on a daily basis through Syrup Pool, Farming Pool, and Lottery Pool.

CAKE will be burned when ANY Pancakeswap product is used.

Token Use Case

CAKE was designed to be applied in every feature of Pancakeswap, including the Syrup Pool (Staking), IFO (Staking), Lottery and Prediction (Payment).

=> Although the Total Supply of CAKE is undefined, Pancakeswap does a great job in managing the Circulating Supply of CAKE, and maintaining a balance between the Token Release and the Token Burn. Pancakeswap is not only clever at increasing the applications and Buy Demand for CAKE, but also proficient at successfully maintaining the incentives for CAKE holders.

The result: The price of CAKE rose from $0.4 to an ATH of $40 (+10,000%), and now remains at $14 (+3,500%).

You can see more details about BNB's tokenomics right here .

How CAKE is applied in every feature of Pancakeswap.

Inefficient Tokenomics

Pangolin (PNG)

PNG is the native token of Pangolin - an AMM DEX on Avalanche. Although PNG is, to some extent, similar to CAKE in its features, I personally believe that Pangolin had some serious problems in designing its tokens which are not working productively.

Unreasonable Token Supply

Initially, the Total Supply of PNG was 538,000,000 PNG. After every 4 years, the number of PNG tokens distributed into the market will be halved. This is an identical approach as Bitcoin, which will take Pangolin 36 years to fully unlock its tokens.

However, BTC has been acknowledged as a SOV (Store Of Value) asset and has been trusted by a massive crypto community, whereas PNG is a newly developed token. There is no guarantee that the Pangolin team can develop the protocol for the whole 36 years, let alone the crypto market has existed for only 10 years.

There is no balance between the Revenue and the Token Release Value

There are currently 175,000 PNG being unlocked every day, which is worth about $197,500. On the other hand, the revenue of Pangolin couldn't even reach $30,000/day. This turns PNG into an inflationary token, which results in the token holders losing interest in the project and selling their tokens.

Therefore, before investing in any token, we have to look at the project from many aspects. The project can easily “create” an ideal scenario with its written documentation, but whether that scenario can be put into practice requires real-time data and proofs. Can the project receive as much revenue as expected?

⇒ The Token Release schedule is inappropriate, the PNG tokens cannot be applied efficiently on Pangolin. The “ideal scenario” of the Tokenomics does not match the real-time data.

The result: After reaching a peak of $15, the price of PNG has declined considerably to $1.2 (divided 12 times). Even when the crypto market saw a strong upward trend in April to May 2021, the PNG price did not have any remarkable rise.

In September 2021, various Avalanche tokens such as AVAX, SNOB, XAVA,... have significantly grown in their price, but PNG was still moving extremely slowly. Although Pangolin is backed by the Avax Labs, Pangolin has now been surpassed by Trader Joe.

An inefficient Tokenomics leads to the decline of PNG price.

Viewpoints on the Case Studies

As mentioned above, the Tokenomics design is not attached to anything. Depending on the product model and the sector that the project aims towards, the team can adjust the Tokenomics accordingly and appropriately.

Evaluating a token is not only about analyzing its applications, but also about investigating its target market.

How massive is that market segment? How many users are there? Is the Tokenomics design balanced between its applications to the project and its benefits for token holders?

For instance: From the beginning, Pancakeswap (CAKE) determined their target market to be Binance Smart Chain - the second largest DeFi ecosystem in terms of TVL (Total Value Locked) and has had a huge number of users.

Understanding the situation, the Pancakeswap team designed the Tokenomics so that a huge Token Allocation was reserved for Liquidity Mining Reward to attract users and investors. Afterwards, in order to raise the Buy Demand for CAKE, the Pancakeswap team applied CAKE in every possible feature that Pancakeswap provides.

Conclusion

We have gone through an article about Tokenomics. Here is the recap of some notable points:

Tokenomics consists of many elements, such as Token Supply, Token Allocation, Token Sale, Token Release,...

Tokenomics is a mandatory factor to evaluate a project, but there are still a variety of other elements to consider, such as the token's applications or the target market.

Tokenomics can be designed in numerous ways. However, how much revenue the platform earns and how the project captures the value for its tokens is of the foremost importance.

## Mechanism Design Theory

Mechanism Design Theory: What it Means, How it Works

By JAMES CHEN Updated October 31, 2021

Reviewed by CHARLES POTTERS

Fact checked by YARILET PEREZ

Trending Videos

Close this video player

What Is Mechanism Design Theory?

Mechanism design theory is an economic theory that seeks to study the mechanisms by which a particular outcome or result can be achieved.

KEY TAKEAWAYS

Mechanism design theory is an economic framework for understanding how businesses can achieve optimal outcomes when individual self-interest and incomplete information may get in the way.

The theory is derived from game theory and accounts for individual incentives and motivations, and how these can work for the benefit of a company.

The theory's creators were awarded the Nobel Memorial Prize in Economic Sciences in 2007.

1

2

Understanding Mechanism Design Theory

Mechanism design is a branch of microeconomics that explores how businesses and institutions can achieve desirable social or economic outcomes given the constraints of individuals' self-interest and incomplete information. When individuals act in their own self-interest, they may not be motivated to provide accurate information, creating principal-agent problems.

In particular, mechanism design theory allows economists to analyze, compare, and potentially regulate certain mechanisms associated with the achievement of particular outcomes that focuses on how businesses and institutions can achieve desirable social or economic outcomes given the constraints of individuals' self-interest and incomplete information.

Mechanism design takes private information and incentives into account to enhance economists' comprehension of market mechanisms and shows how the right incentives (money) can induce participants to reveal their private information and create an optimal outcome.

Mechanism design theory is thus used in economics to study the processes and mechanisms involved with a particular outcome. The concept of mechanism design theory was broadly popularized by Eric Maskin, Leonid Hurwicz, and Roger Myerson. The three researchers received a Nobel Memorial Prize in Economic Sciences in 2007 for their work on the mechanism design theory and were branded as foundational leaders on the subject.

2

Considerations in Mechanism Design Theory

Mechanism design theory built on the concept of game theory, which was broadly introduced by John von Neumann and Oskar Morgenstern in their 1944 book, Theory of Games and Economic Behavior.

3

Game theory is known in economics for the study of how different entities work together both competitively and cooperatively to achieve outcomes and results.

Various mathematical models have been developed to efficiently study this concept and its results. Game theory has also been recognized throughout the history of economic studies with more than a dozen Nobel Prizes going to researchers in this area.

Mechanism design theory generally takes a reverse approach to game theory. It studies a scenario by beginning with an outcome and understanding how entities work together to achieve a particular outcome.

Both game theory and design theory look at the competing and cooperative influences of entities in the process towards an outcome. Mechanism design theory considers a particular outcome and what is done to achieve it. Game theory looks at how entities can potentially influence several outcomes.

Mechanism Design Theory and the Financial Markets

There is a wide range of applications for mechanism design theory, and as a result many mathematical theorems have been developed. These applications and theorems allow researchers to manage restrictions and information control of the entities involved for the purpose of achieving the desired outcome.

One example deploying the use of mechanism design theory occurs in an auction market. Broadly, regulators seek to produce an efficient and orderly market for participants as the primary outcome. To achieve this result, several entities are involved with varying levels of information and association. The use of mechanism design theory seeks to regulate and control the information available to participants in order to achieve the desired result of an orderly market. Generally, this requires the monitoring of information and activity at various levels for exchanges, market makers, buyers, and sellers.

The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens.

January 18, 2018 by Thomas Euler

The development of the framework presented in here was a collaborative effort between me and several of my Untitled INC fellows. Peter Trapp was heavily involved in all aspects of the creation, including lending his surprising design prowess to it. Prof. Dr. Andranik Tumasjan of the University of Mainz (and formerly Technical University Munich) provided very valuable feedback and ideas, as did Dr. Oliver Krause, Dr. Karl-Michael Henneking and Daniel Pichler.

Blockchain, ICOs and bitcoin’s wild ride have been some of the hottest tech topics in 2017. Yet, while people spent billions of dollars on cryptographic tokens, the understanding of the different token types out there is still limited. Even among regular investors and long-standing members of the blockchain community.

One reason for it — a quite common one in emerging domains — is the lack of clear, generally agreed upon terminology and definitions. For instance, I regularly come across people who refer to all tokens as “cryptocurrencies”. Which, as we are going to see in a minute, isn’t precise. Which is somewhat problematic because precision in language and terminology is the basis for an informed, nuanced dialogue and good analysis.

Whether you want to develop a token or evaluate one, it’s critical to understand the nuances of the subject. Moreover, the blockchain community is growing and maturing. As a result, it is increasingly getting in touch with “the real world” (aka people who are new to the subject). Investors, regulators, politicians and decision-makers in businesses are all taking the space increasingly serious. Many are in the process of formulating their positions and strategies for dealing with the subject. Clarity and accessibility of relevant knowledge are key to allowing those actors to make good, informed decisions.

This is why we, the Untitled INC team, set out to develop a framework that a) reflects the various existing token types, b) allows to classify and analyze tokens in various relevant dimensions, and c) fosters a better, nuanced understanding of crypto tokens. Today, we are presenting the first iteration of the Token Classification Framework, the result of our effort. In this post, I’m going to walk you through the framework and explain the work and thinking that went into it.

## Token Classification Framework

Introductory Remarks

Before we get into the framework, some technical and procedural remarks.

To develop the framework, we reviewed a lot of work on tokens that had already been put out there. Many smart people published very helpful thoughts and ideas which influenced our thinking and chosen terminology. You’ll find a list of references at the end of this article.

The version of the framework in this article is version 1.0 of the Token Classification Framework (TCF). The crypto space is moving at a rapid pace, so we expect to see new developments and innovative approaches to tokens quite frequently. Thus, we regard the framework as a living document. The version in this article shall serve as a point-of-reference going forward, so we won’t update the TCF in here. Instead, we’ll host and maintain the most current version on our website.

Last but not least, we decided to turn the future development of the framework into a collaborative endeavor. Which is why we are releasing the framework under a Creative Commons BY-NC-SA license. This allows the community to iterate on the framework and contribute to its development. Also, your feedback is highly welcome so please leave your feedback in the comments below.

Classifying Tokens in Five Dimensions

There are multiple angles from which you can look at tokens. Back when we began working on the framework, we quickly realized that it would have to cover multiple perspectives in order for it to be useful. After reviewing the current literature and analyzing dozens of whitepapers, we distilled five major dimensions which we wanted to reflect in the framework: a token’s purpose, utility, legal status, it’s underlying value and the technical layer it’s implemented on.

Purpose. What is the token’s main purpose? What is it designed to do? This dimension illustrates why the people who call any token a cryptocurrency err. Tokens can certainly be intended as a cryptocurrency. But often they are meant to enable a specific network and catalyze its growth (network tokens) or merely present a way to invest in an entity or asset (investment token).

Utility. The term “utility token” has become commonplace¹ but there are various types. When looking at different tokens, you’ll find many approaches to creating utility for token owners. But on an abstract level, there are two major ways to provide utility: by giving access to network or service features (usage tokens) or by allowing token holders to actively contribute work to the system (work tokens). Some tokens do both (hybrid tokens) and some tokens don’t provide any utility at all².

Legal Status. The legal perspective is extremely relevant as of now, so it is reflected in the framework. The category’s content, however, is expected to change quite a bit in the upcoming months as it is a volatile environment and more regulation is expected to emerge. Moreover, every jurisdiction can differ. The general outline of the current state in multiple countries is that tokens which aren’t clearly a utility token — i.e. a means to access features of a network/service — or which aren’t a pure cryptocurrency can easily be classified as a security token by regulators. In some jurisdictions, such as Germany, there is some definition by regulators as to what constitutes a cryptocurrency. Several cases we found hover between two types, due to fact that current legal frameworks have been created before tokens existed and most haven’t been updated so far. (This isn’t legal advice.)

Underlying Value. Most tokens are created to have a monetary value. But the sources of their value differ considerably. Some basically work as IOUs to a real-world asset which they are tied to (asset-backed tokens). Others showcase stock-like properties as they are linked to the commercial success of the issuing entity. Those share-like tokens would be regarded as securities in most jurisdictions (actual enforcement by the regulator is a different subject). Finally, there are tokens which are tied to the value of a network, not a central entity (network value tokens). The latter might be the hardest to wrap one’s head around and the most interesting value source at the same time.

Technical Layer. Tokens can be implemented on different technical layers of blockchain-based systems: on the blockchain level as the chain’s native token (blockchain-native tokens), as part of a cryptoeconomic protocol that sits on top of the blockchain (non-native protocol tokens), or on the application level ((d)App tokens).

It’s important to note that the dimensions are complementary. Most tokens can be assessed in all dimensions and, as we’ll see when looking at the archetypes, there are strong correlations between some types in different categories.

Main Token Types per Dimension

In any dimension, we identified various token types, summarized their main characteristics and included relevant examples. You can find the result in the graphic below.

Putting the TCF to the Test

A granular framework like this allows us to understand a given token with a higher degree of precision. In order to put the framework to practice, we looked at several tokens and classified them. You’ll find some examples from a recent workshop we held below:

As the first chart shows, you could call Augur’s REP a Non-native-protocol-Network-Network-value-Work token that would likely classify as a utility token.

Let’s stop here. If you are interested in playing around with the framework, you might want to start with Ethereum and classify it yourself.

Archetypes

After using the framework to classify a fair number of tokens, some patterns emerged (unsurprisingly). As I said before, there are some rather obvious correlations between different token types. For instance, many network tokens (by purpose) will also be network value tokens, i.e. their value is tied to the value of the network they are used within. Similarly, an investment token will basically never be a network value token but either asset-backed or share-like. We looked at those patterns and derived some archetypes.

Each archetype is represented by an icon. The icons are also included in the main table above, next to the token typology usually associated with a respective archetype. A description of each archetype is included in the graphic below:

The Wider Context

We think the TCF is useful to classify and create more clarity around the various token types you can find today. Still, it is important to note that it isn’t enough to merely analyze a token.

Crypto tokens don’t exist in isolation but are only one component of a distributed ledger system. While tokens are an integral component of the system — as they are critical to establishing a cryptoeconomic dynamic —the token layer is only one of three system layers. The others are the governance and technology layer, which are connected by the token. I won’t go into detail on the model below, as it merits its own post in the future. For now, it’s enough if you keep in mind that any assessment of a DLT project shouldn’t exclusively focus on the token but look at the entire system.

The Complete Token Classification Framework

Now that you are familiar with the different components of the TCF, you can find the complete framework below in high resolution. As it is published under Creative Commons, feel free to share and iterate on it. Just don’t forget to link back to us. And if you have comments or suggestions for further improvements to the framework, please let us know.

## Quantitative Token Model

Introduction

Web3 is a fast moving space with high volatility in user migrations and price charts. Existing Web2 businesses and startups that aim to transition into the Web3 area encounter a new world of complexity, challenges, and opportunities. Once they have decided to embark on this journey, there are many uncertainties and questions that need to be answered. Previous articles discuss the reasons why an initiative might need or want to have a cryptographic token and why quantitative approaches are essential to build a sustainable token business. This report iterates on the quantitative aspect by introducing a generalized Quantitative Token Model (QTM). Instead of explaining the detailed mathematical relationships, it provides a methodological overview along with a case study of a generalized token economy. The QTM is a spreadsheet based tool to model and forecast a majority of known token designs on a higher level where it leverages aggregated stakeholder representation. Even though code-based solutions, such as cadCAD, provide more flexible and sophisticated ways to model the complexity of token ecosystems, the spreadsheet implementation of the QTM has one major benefit: It is accessible to a wider audience and serves a variety of different token business concepts all in one tool.

This document starts with presenting the input and internal structure of the QTM. Afterwards a case study is carried out for a strong and weak user adoption scenario of a fictional Web3 business. Note that the presented token design is not recommended and should not be seen as a benchmark token design for similar businesses. A conclusion at the end wraps up the major findings.

Structure and relevance of the QTM input components

The structure of the QTM consists of 3 main blocks: (1) The ecosystem input section, (2) the utility modules section, and (3) the analysis section. The ecosystem input section is subdivided into the following fundamental subsections:

Basic Token Parameters

Decision making regarding token supply dynamics / fixation

Amount of initial token supply

Launch date of the token (liquidity deployment)

The decision between a dynamic or fixed token supply is fundamental for the whole ecosystem. In the case of dynamic supply the quantitative analysis can be used to adjust the emission for improved token valuation sustainability, while in the fixed supply case it can be used to ensure the project bucket token sustainability. See this article to understand the difference between these two types of sustainability.

Fundraising Module

Fundraising parties

Monetary allocations

Token discounts

Figure 1 shows the exemplary token prices for different early investor groups. Traditionally more early contributors will receive a cheaper effective token price while they have to commit for longer time vesting schedules. Note that extreme discrepancies between early VC discounted token prices and public sale prices can have a negative impact on future marketing and reputation efforts for the business. Note that not all the different fundraising stages need to be used, the template should be adapted to an individual team’s strategy.

Figure 1: Exemplary resulting effective token prices for different early investor groups

Initial Token Allocations & Vesting Schedules

Token allocations to initial investor groups, supporting parties, team, protocol buckets, and liquidity

Individual vesting schedules for each of these entities

Figures 2 and 3 below indicate some exemplary token allocations and vesting schedules. Note that the given numbers are not optimized, but rather represent historic and experience based allocation magnitudes. Also note that some project buckets are not used in this example. The low share of tokens for liquidity is a problem for many projects if there are not enough token sinks holding the rest of the supply back from being sold into the liquidity pool (LP). This leads often to drastically decreasing token valuations. Performing forecasts with the QTM has the benefit of identifying those sustainability issues before the token has even launched and increases the probability of a supply and price sustainable token circulation.

Figure 2: Exemplary token allocation

Figure 3: Exemplary token vesting schedules

Liquidity Pool Module

Token launch price

Monetary allocation to the LP

Paired token information

The amount of money that is allocated to the LP is known as liquidity depth and is essential for the price velocity. A deep LP will require more capital to move the price than a LP with less capital. At deployment the LP will consist of the project’s native token and a paired token. The paired one is most often a stable coin or a reputable high market cap token, such as $ETH. In cases where teams can’t afford deep initial liquidity, they have to incentivize other parties to provide it.

User Adoption Module

Initial user number

Initial investment per user

Regular capital inflow per user per month

Share between product and token buys of user funds

User behavior in terms of token selling and token utility adoption

Figure 4 shows an exemplary chart of user growth over the course of 10 years of a Web3 business. This module is essential for the whole ecosystem forecast and based on assumptions regarding the market adoption. The team has to perform market research to estimate the input user growth numbers and the corresponding capital the users will contribute to the ecosystem. The QTM distinguishes further between general users of the whole ecosystem, including off-chain offers and the users that interact with the token. Note that the user adoption must always be treated in different scenarios and can be based on previous similarity market studies.

Figure 4: User adoption for the business as a whole and just for the token

Business Assumptions

One time fundraising

Avg. monthly income streams

One time investments & expenditures

Avg. monthly expenditures

The business assumptions are used to forecast the financial sustainability of the business by balancing the initial raised capital/expenditures and regular income/expenditure streams. Figure 5 shows the business funds growth for an exemplary case. The business funds are equivalent to the equity that is owned by the business, which might be originated by raised investor capital and revenues.

Figure 5: Exemplary business funds growth curve for Web3 business case with growing user count

Utility Modules

All previously mentioned aspects are part of the fundamental token ecosystem input section. Another QTM section is dedicated to potential utilities for the token. Note that one can distinguish between different definitions of utility. Instead of “token utility” being exclusively tied to the product interaction, in this article “token utility” refers to a broader spectrum on which a token can be used. This includes liquidity provision, staking, payments, burning, and holding of the token. In the QTM the utilities are built in a modular way, so that project teams can not only activate or deactivate certain utilities, but also set their assumed weighting with respect to token allocations and specific parameters for each individual one. Figure 6 shows the 5 generalized utilities that are implemented in the current QTM version (1.8).

Figure 6: Generalized utilities in the QTM

Holding

The “Holding” utility is for projects that want to pay out token rewards to wallets that hold the token to incentivize further holding.

Locking

The “Locking” utility can be used as representation for staking or play to earn concepts, where users lock their tokens into a smart contract to receive more tokens as rewards.

Liquidity Mining

The “Liquidity Mining” utility is created to incentivize other parties to provide liquidity through additional token rewards.

Burning

The “Burning” utility has to be used to account for token burnings.

Transfer

The “Transfer” utility is used whenever tokens will be transferred from token holders back to project buckets. E.g. this can be used for a shop where users can buy items in exchange for the token or to pay for services / fees.

Another optional utility mechanic not mentioned in the above list is an off-chain point system that can be used to have more control over value emission to the stakeholders. It leverages off-chain points that can be reused for the products or can be converted into the token and thereby being sold or used for the other utilities. Optionally users that stake the token can get a multiplier on their token issuance rate. Figure 7 illustrates the point issuance with and without multiplier along with the resulting token emissions through the conversion from points to tokens.

Figure 7: Off-chain point issuance and token issuance from point conversions. Points with multiplier are only issued to token stakers

Figure 8 shows an overview of all previously mentioned input modules for the QTM. Note that all of the subsections need to be fed with the most accurate data available, since the quality of the output depends mainly on the quality of the input data and assumptions made in the QTM.

Figure 8: Input modules of the QTM

QTM Structure

The QTM’s abstracted structure is shown in Figure 9, where the rough processing order for one timestep is from the top to the bottom. The QTM is a time-domain model with a fixed timestep of one month and a simulation range of 10 years. Each timestep starts with the token distribution from the vesting schedules of the different early investor groups. These “free” tokens will be categorized into three meta buckets. One is used for selling tokens into the LP. The liquidity is implemented as an Automated Market Maker (AMM) LP with the widely known constant product relationship. Another meta bucket for the vested tokens is used to distribute the tokens to all enabled utilities, specified in the utility modules input section. The last meta bucket is for all tokens freely held by the users and other ecosystem participants. Note that “Holding” can also be defined as an utility, such as outlined before. The distribution shares for all meta bucket categories and the individual utilities have to be set by the designer using the QTM. Every timestep users can join or leave the ecosystem with their capital. This is represented by varying user growth, capital spending for the product or buying the token, selling the token, and utility allocations or removals. Rewards are defined within the individual utilities and will be paid out to stakeholders, while the transfer utility can be used for a refilling of the project buckets. Note that the off-chain business can also buyback tokens to further sustain the project token buckets and issue off-chain points as another layer of value feedback. The model doesn’t leverage Monte Carlo simulations since it already represents the arithmetic mean of all inputs and outputs. Furthermore, it doesn’t include any Markov decision making trees options since all decisions are preset by the designer through average token allocation shares that are constant for the whole course of the simulation. Hence aggregated representative stakeholders are assumed. Note that transient events can be implemented through manual manipulation of the input tables. These simplifications are not sufficient for comprehensive and realistic ecosystem analyses, but they are made as a tradeoff to mitigate complexity for the model to increase accessibility for a wider audience while serving as many different Web3 concepts as possible through its generalized modular framework. Even though predictions won’t be accurate they can provide a first quantitative approximation.

Figure 9: Input modules of the QTM

Case Study

Introduction

Two of the main goals for the ecosystem modeling token engineer is to maintain token value and supply sustainability. Choosing a dynamic token design will mitigate the token supply sustainability issue, since tokens can be minted infinitely, but this mechanic has to be counterbalanced through burning, buybacks, and/or increasing demand for the token to maintain value sustainability. On the other hand a fixed supply token can be attractive for investors since they know that they can own a fixed share of the represented business without getting diluted through potential token inflation. A fixed supply of tokens requires token sustainability, since there must always be enough tokens left in the reserves to pay out rewards for the stakeholders of different utilities. In any case the token has to capture and accrue value to be attractive for investors.

The presented case study considers a token design with moderate token emissions for two different user adoption scenarios and discusses the implications of main ecosystem parameters.

Case Study – Base Setup

The following case study illustrates the difference between a strong user adoption and a lower user adoption for a Web3 business that sells a product or service in exchange for their token. The product requires a subscription fee of $3 worth of token per month per user. Also users can stake their tokens or participate in a liquidity mining program to receive token rewards. The business has to sell the received tokens from the subscription fees to cover their costs and to make a profit. The initial supply is set to 100,000,000 tokens, the early investor groups, token distribution and vesting is defined as in the example inputs given in Figures 1 to 3. It is assumed that the protocol raises a total amount of $3.9m before the token generation event (TGE). The token has a launch price of $0.50 and 15 % of the raised capital is used to purchase the paired token for the DEX LP. This results in the initial valuations given in the following table:

LP $1,170,000

MC $25,957,500

FDV MC $50,000,000

The user adoption is shown in Figure 10, where the amount of token users equals the amount of overall business users, since they need the token to participate for every provided offer. In the case study an additional scenario with one negative growth year and growth stagnation is assumed, represented by the curve in Figure 11. The strong user growth curve ends with 106,167 users and the weak growth scenario ends with 25,412 users after the simulation period of 10 years.

Figure 10: Scenario I – user adoption curve for the business without any negative growth periods

Figure 11: Scenario II – user adoption curve for the business with one year having -2 % user growth per month

Since the main utility for the token is either spending it for the product subscription or letting it produce yields within the staking or the liquidity mining program, it is assumed that 75 % of the free supply is used for utilities, 20 % will be sold and 5 % will be held in the wallets. Besides this 3 % of the utility allocations will be removed every month as an average assumption. The utility allocations are assumed to be distributed as shown in Figure 12 for every timestep. The rewards for staking and liquidity mining are 15 % and 30 % APR respectively and are generated through a minting function. The majority token utility allocation of 70 % is assumed to be used to pay for the product subscription. 1 % of all utility allocated tokens will be burned per month. Those tokens are subtracted from the product subscription.

Figure 12: Token utility allocations per month

For the business a one-time investment of $50k is assumed to cover initial debts. Furthermore regular costs of $84k per month are assumed for the salaries, software licenses, and other expenditures. The income for the business is set to a constant amount of $100k per month and gained from token sales starting two years after the TGE. The resulting funds development without consideration of business token holdings is shown in Figure 13.

Figure 13: Business fund development for the case studies

Since the income is a $-denominated fixed value, it is not affected by the two different user growth curve scenarios. However, the different user growth assumptions affect other case study specific metrics, discussed in the following sections.

Scenario I: Strong User Adoption

The strong user growth scenario is based on the numbers given in Figure 10. The project buckets and the supply numbers of the token are the first important metrics to analyze. Figure 14 shows their development over the course of the simulation. The initial investor vesting ends 3.5 years after the TGE. The circulating supply increases through this vesting period to around 100m tokens and continues to rise slightly due to the token minting for payouts to staking and liquidity mining participants. The token reserves also increase over time, since they are filled from the customers transferring their tokens to pay for the main product subscription.

Figure 14: Project bucket and supply development for the strong user adoption curve

The strong user growth creates demand for the token so that its price starts to appreciate after the bottom of $0.12 per token is reached after one year. The initial decrease of the token price is caused by the sell pressure from the vested tokens from initial investor groups combined with the comparatively low user count of just 9,537 at the end of the first year. One big advantage of the QTM simulation tool is that input parameters can be changed without much effort. In this case it is of interest to examine the effect of another vesting schedule. E.g. changing it to double vesting time for all early investors would result in an initial token price drop to just $0.19.

Figure 15: Token price development for the strong user adoption curve

Figure 16 shows the $-denominated value flows from and to the different utilities respectively. They show the expected healthy growth coinciding with the user growth. At the end of the simulation period, the transferred amount of tokens from the users approaches $1m, while around $400k worth of tokens are issued to stakers and liquidity miners as reward and $14k worth of tokens are burned per month.

Figure 16: Utility rewards / burnings / transfers for the strong user adoption curve given in $-denomination

Scenario II: Weak User Adoption

The weak user growth scenario is based on the numbers given in Figure 11. The token supplies in Figure 17 reveal that the reserve bucket will run out of tokens after around 8 years, since too few users counterbalance the constant token selling from the business. Note that even the dynamic setup of the token can’t sustain the strong sell pressure in terms of token supply.

Figure 17: Project bucket and supply development for the weak user adoption curve, where the reserves running out of tokens after around 8 years

Similarly the token price experiences a massive drop in the negative growth year, which coincides with the start of the regular massive token sales from the business. Overall the applied business setup is not sustainable in terms of the token valuation and the supply for this low user adoption. The QTM can be leveraged to find settings that might change this unsustainable situation into a sustainable one.

Figure 18: Token price development for the weak user adoption curve

Reducing the monthly token sales from $100k to $85k worth of tokens is already enough to reach a sustainable token valuation and token price. These numbers will not lead to strong business fund growth, but let the business sustain, such as indicated in Figure 19.

Figure 19: Business fund development with reduced regular token sales for the business to counter a lower user adoption

Figures 20 and 21 show the corresponding token supply and valuation curves for this survival mode scenario. Now the reserves supply is sustainable over the simulation period and the price starts rising again after the negative growth year. Note that external market psychological factors are not accounted for in these simulations, which means that the appearance of the price chart doesn’t affect the behavior of the users and investors in the model. This simplified assumption is a limitation of the QTM.

Figure 20: Project bucket and supply development for the weak user adoption curve and lowered token sales from the business

Figure 21: Token price development for the weak user adoption curve with lowered token sales from the business

Conclusion

The case study shows some capabilities of the QTM, where fundamental token business aspects are evaluated within seconds after parameter definition. This specific analysis revealed the impact of different user adoption scenarios and showcased how small changes in the base parameters can cause the difference between a sustainable and an unsustainable Web3 business. The QTM is a powerful and accessible tool with a clean UI to perform high level forecasts for many different kinds of token ecosystems. It is built in a modular structure so that token designers and engineers can turn on and off whatever functionality they want. The QTM leverages customizable token supply designs, fund raisings, token allocations, vesting schedules, liquidity pool designs, user adoption scenarios, (static) user behaviors, business assumptions, buyback strategies and on- and off-chain utilities. The tool is programmed in a spreadsheet so that everyone can use it without any coding knowledge and simulates each given setup within a few seconds. It is the ideal tool for new Web3 businesses and existing businesses to create a first quantitative iteration for their token design while allocating low time resources for setting the simulation up.