Auditing Tokenomics: A Case Study and Lessons from Auditing a Stablecoin Project

Stylianos Kampakis, Centre for Blockchain Technologies, University College London, UK

Correspondence: stylianos.kampakis@gmail.com

Abstract

Tokenomics is a vital part of any blockchain project. It is the study of how crypto tokens are used within the blockchain ecosystem, their role in the project, and how they are designed to incentivise certain behaviours. There are many ways that crypto tokens can be designed for use within an ecosystem. For example, they can be designed to have a fixed supply so that there is no inflation or deflation in the system. Founding teams can also create tokens that provide voting or governance rights to holders, thereby incentivising them to hold onto their tokens rather than sell them on exchanges. They can also be used simply to pay fees.

The range of options that founding teams have when designing token economies often leaves them with more questions than answers. Even deciding whether the token economy design is robust can be a challenge. Furthermore, a blockchain project not only has to convince its founders but its prospective investors. As a result, innovative crypto-projects often create for themselves interesting narratives, but they are not always viable.

For that reason, a recent trend in the industry is "the tokenomics audit." The goal of a tokenomics audit is similar to an audit in any other industry (e.g., accounting). The auditor has to assess the viability of a project, while also suggesting potential improvements. The end goal is to provide an independent view on whether a token economy is viable or not.

This paper discusses general principles that can be followed when running a tokenomics audit. The paper uses as a case study a recent tokenomics audit, conducted for the BankX stablecoin (https://bankx.io/), by the author of this paper. The paper first discusses in general the different methods and mechanisms that a tokenomics auditor can employ to audit a project. The paper then proceeds to demonstrate how these methods were used in the audit of the BankX project.

Tokenomic auditing is still a new area, and there is no set of established methods to conduct an audit. By reviewing this case study, this paper helps provide some lessons to the community, upon which future research can improve.

Disclaimer: Nothing in this paper can be interpreted as constituting financial advice. This paper was written for academic purposes only.

Keywords: *tokenomics; bitcoin; audit; ecosystem; crypto token; structural analysis; marginal case*

JEL Classification: A10

1. Introduction

Tokenomics is a relatively new term and describes the use of tokens in the context of business models. It is a combination of two words, "token" and "economics." Tokenomics is an emerging field that studies how tokens can be used as a form of currency for digital services.

The first mention of tokenomics is believed to have been in an article by Chris Dixon, a venture capitalist at Andreessen Horowitz [1]. He discusses how tokens can be used to incentivise desired behaviours and create an economy around a product or service.

The first token was introduced in 2009 by Bitcoin [2], created as an alternative to fiat currencies. The idea was to create a decentralised currency that would not be controlled by any government or central bank.

The rise of Ethereum, and its ability to function as a virtual computer, gave birth to an explosion in blockchain projects, with each one using its own token. This popularised the concept of a token economy. The space has evolved since then, with tokenomics achieving greater depths of complexity, especially in areas such as decentralised finance.

The field of tokenomics is still nascent. As of the time of writing this paper (22 January 2022), there are only 816 search results on Google Scholar for the term "tokenomics." The combination of a field that is still in its infancy with a blockchain space that is moving and innovating very fast has often made things difficult to follow. There are not many established best practices, and the ones that exist are not necessarily easily found by entrepreneurs or prospective investors.

This has given rise to the recent practice of auditing. As in other sectors, e.g., accounting, the purpose of an audit is to provide a critical inspection of a project. This practice has elements of both an art and a science, and the auditor might combine quantitative techniques with subjective judgement.

There is no set framework for auditing tokenomics, but it is an area that is likely to grow in importance. This paper presents a case study of a tokenomics audit and some general methods that were used in order to perform the audit. This helps draw lessons from how these methods can be used in practice, and set the frame for future work. It is the hope of this author that this case study will help the community learn and eventually come up with generally accepted standards for how to audit tokenomics.

2. Methodology

It is important to note that the term "tokenomics" can be used to describe different aspects of a blockchain project:

1) The number of tokens issued and the way they are issued (vesting schedule, airdrops, etc.).
2) The economics of a consensus algorithm; largely referred to as crypto-economics.
3) The general structure of the system: game-theoretic and economic incentives.

In this paper we will mostly discuss point 3. Point 1 is also very important, but it wasn't the focus of the case study audit, and is considered a separate concern.

Additionally, with regard to point 1, many projects adopt a formulaic approach when issuing and releasing tokens, and this approach can be enough to avoid a project's token crashing. The long-term viability of a project mostly depends on point 3. If a project's token economy does not provide the right incentives, or if it does not have a compelling business case, then it's unlikely to survive. However, it should be noted that the success of blockchain projects as a whole, as well as initial coin offerings (whether on an exchanged, often called IEOs, or a decentralised exchanged, often called IDOs), depends on multiple factors [3], which might also themselves be shifting as the technology evolves.

Point 2 is relevant not so much for tokens, as for coins (e.g., like ETH) and layer 1 solutions, and is not discussed in this paper, which is focused on a token case study.

3. Core Principles

Auditing tokenomics before the official launch of a project is a challenging endeavour; first and foremost because the analyst is being asked to create a model of something that doesn't exist. The study of existing real-world economies is challenging, but at least economists have access to proven data which they can use to develop econometric models and test their theories.

In contrast, a tokenomics audit for a project in its pre-launch phase needs to find ways through which the auditing and thinking processes can be structured. Also, a tokenomics audit needs to have a particular goal. This can be different depending on the purpose of a project. However, in general, we can define the goal of a tokenomics audit as follows:

"The goal of a tokenomics audit is to convince an informed but sceptical reader that the properties and claims of a project are true, given the current and foreseeable conditions in the world."

This is an open-ended definition, because different projects have different priorities. However, some possible goals can be:

1) Price stability (for stablecoins) or appreciation.
2) Creating a store of wealth against inflation.
3) Ensuring real-world utility of the token.

An example of such goals is provided for the case study analysed in Section 3.

To that extent, an audit can use different tools, some of which are described below.

It is important to note that the list of the methods outlined here is not, necessarily, exhaustive. It is very likely that other auditors might prefer a slightly different set of methods, or even use their subjective judgement. These methods, however, provide a good template and can be adapted to various circumstances.

Empirical Proof, Data Analysis, and Benchmarking

The first method an audit should always employ is that of learning from similar cases. When coin offerings were initially invented, there was a high chance that a new project was creating a proposition or mechanics never encountered before. Now, it is likely that a new project will find at least some points of similarity with existing projects.

For example, there is a lot that can be learned from the successes and failures of different types of stablecoins. From the controversy that has surrounded USDT [4], to the success of Terra/Luna or the bank run and the eventual collapse of Iron Titanium [5], it is likely that a project can learn a lot through similarities with existing projects.

The analysis becomes even more useful if data is available which can be used to make an argument. An example of this approach is seen in an audit of the tokenomics of Frax by Albaron Ventures, where they compared the peg stability of Frax and other stablecoins, as shown in Figure 1.
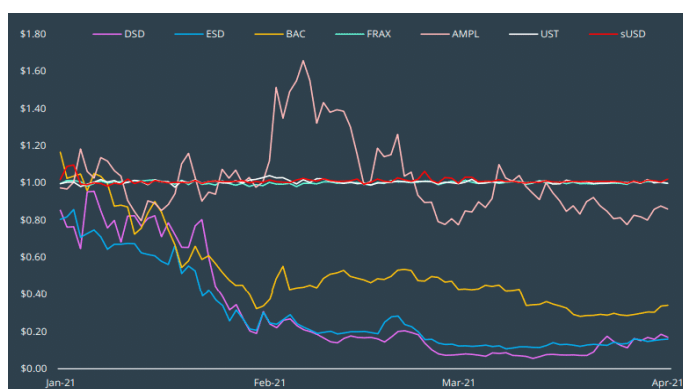

Figure 1. Comparison of peg stability of different stablecoins. Source: [6]

Agent-Based Modelling

One of the methods suggested by the author in the past is agent-based modelling [7]. Agent-based modelling is used to study complex systems and to solve problems that are difficult or impossible to solve analytically.

The agent-based modelling process starts with the identification of the system's components and their relationships. The next step is to identify the rules governing how these components interact with each other, which can be done by observing the system in operation or by using expert knowledge. The final step is to run simulations with different sets of initial conditions and parameters and compare them against one another in order to find an optimal solution.

The flexibility of agent-based modelling has given rise to different flavours of this approach. For example, some simulations might incorporate intelligent agents, through the use of reinforcement learning, a famous example of this being the multi-armed bandit problem.

In the domain of networks, diffusion models are a popular choice, and they have been used in many different areas from biology [8] to social networks [9].

Also, agent-based modelling is often implemented via Monte Carlo methods, whose objective is to use repeated random sampling in order to identify equilibria and possible evolutionary paths in a model [10], [11].

Agent-based modelling is an excellent method for analysing token economies, given their complexity and the interconnected parts.

Game Theory

Game theory is a branch of mathematics that studies the mathematical models of conflict and cooperation between rational decision-makers, first devised by Von Neumann [12]. Game theory is mainly used in economics, political science, and psychology in order to understand how humans interact with each other when there is limited, or no, trust.

Game theory has an integral significance to blockchain, given that the root of the blockchain lies in how, through the use of algorithms, trust can be ensured in a network without trust. It therefore follows that game theory can be a useful tool for a tokenomics audit.

One of the best examples of this is probably OlympusDAO. While OlympusDAO did not go through

a tokenomics audit (it has gone through a smart contracts audit only) [13], the project is well known for its use of game-theoretic analyses to prove the sustainability of its protocol [14]. A famous image depicting the game theory behind this project is shown in Figure 2.

	Stake	Bond	Sell
Stake	(3, 3)	(1, 3)	(-1, 1)
Bond	(3, 1)	(1, 1)	(-1, 1)
Sell	(1, -1)	(1, -1)	(-3, -3)

Figure 2. Olympus DAO game theory. Source [15]
Structural/Balance-of-Forces Analysis

Another type of analysis, closely related to game theory, is what we will term "structural" analysis but which can also be called "balance-of-forces" analysis. This is a higher level of abstraction, where the analysis lists all possible dynamics and their impact upon a token economy, but without explicitly creating an incentives matrix.

The dynamics and the tools employed create a narrative, which aims to convince an informed reader that they should work as expected when deployed in real life. The balance of the different forces that are applied to a token and an ecosystem should ideally be driven by a clear objective, such as token appreciation, stability, or sustainability.

While this is not explicitly stated, the majority of new blockchain protocols follow this logic, starting with Satoshi Nakamoto's original bitcoin paper [2]. A more recent example of a successful project outlying this is Terra/Luna's documentation [16].

However, the aim of a structural analysis for a tokenomics audit should be to formalise the different dynamics at play in a more structured way, and troubleshoot for issues that might arise, thereby highlighting weaknesses.

Marginal Cases

Another mechanism which is often employed, albeit informally, is the study of marginal cases. These are purely hypothetical scenarios that could break a system, though they never happen in practice. This is similar to the stress test practice which financial institutions undergo. It has become popular for analysts to publish these types of analyses on Twitter, as a series of posts. An example of such an analysis is shown in Figure 3.

Figure 3. Example of a popular thread discussing a potential scenario was Terra/Luna crashes. Source: [17]

Probability Theory

Some analyses prefer to resort to probability theory and stochastic models, sometimes also combining aspects of some of the previous tools mentioned, like game theory and agent-based modelling. A good example of this approach is the analysis of Bitcoin's defences against attack vectors [18] and mining pools [19].

3. Case Study: The BankX Audit

Overview

This case study presents the way in which the BankX audit was conducted. While the full audit can be found in the references list [20], this case study will present an overview of the thinking processes governing this audit.

The audit was broken down into a series of steps.

1) Foundation
   a. Define the goals of the system
   b. Define the tools of the analysis
   c. Define the assumptions
2) Analysis
   a. Balance-of-forces analysis
   b. Empirical and data analysis
   c. Game theory analysis
   d. Marginal cases analysis

Foundation

BankX is a stablecoin that has been inspired by elements of two other blockchain projects, Hex [19] and Frax [16], while also adding its own mechanisms. Both Hex and Frax seem to have flourished since their inception (both of them were launched in 2020). At the time of writing, Hex is at position 201 of Coinmarketcap [21] and Frax is at position 204.

The goals of the analysis were tied to the goals of the system in a hierarchical manner, with the most important goals at the beginning. The goals are copied and pasted below from the original audit [22].

Goals of the Analysis

1. *The peg doesn't break. This is the number 1 goal of any stablecoin system.*
2. *The BankX token's price will not crash completely, or spike to unsustainable heights. In other words, the BankX token's price should either be stable, or slowly appreciate over time.*
3. *The BankX token is a store of wealth.*
4. *The system is moving towards increased usage of the BankX token as collateral to mint XSD (meaning there is more and more demand for XSD).*
5. *BankX has autonomous, sustainable liquidity pools.*
6. *BankX token can achieve the goal of being Always Net Deflationary (A.N.D.).*

The audit then proceeds to define the tools of the analysis (presented below, copied and pasted from the audit).

Tools of the Analysis

1. *Empirical proof: If something has been proven to work in other systems, then it is assumed that it can also work for BankX.*
2. *Balance-of-forces analysis: It is assumed that if an action, within the system, applies an inflationary or deflationary force, this can always be balanced against another action/force within the same system. The actual magnitude forces applied depend on the economic levers in the protocol.*
3. *Numerical analysis: When relevant, we will apply numerical techniques and simulations.*
4. *In this analysis, points 3 and 1 refer to the first mechanism discussed in the previous section. The audit also employed game theory, but in a minor role.*

Analyses

Once this foundation is established, the audit then proceeds to describe the various mechanisms and how they interact. The audit also contains a full table of the dynamics at play and describes whether they work in an inflationary or deflationary way.

The audit then proceeds to an analysis of the peg stability of different stablecoins, demonstrating through empirical evidence that Frax, at least at the time of the audit, could perform just as well, or even better, than "traditional" stablecoins, such as USDT and USDC. The similarity of BankX's and Frax's mechanics is, therefore, considered a positive aspect, which provides evidence that the stablecoin can work as expected and maintain its peg.

The audit then goes on to use game theory in order to analyse BankX's bonding curve mechanism, before moving on to the marginal cases analyses. One of the marginal cases includes data from the Terra/Luna crash that took place in 2021 (shown in Figure 4), therefore combining empirical evidence with hypothetical structural analysis.

The analysis tries to unravel whether something similar could take place for the BankX token, and what is the likelihood of such an event occurring. The audit also analyses one more marginal case relating to the interest rate provided by BankX and the collateral ratio, analysing some of the vulnerabilities of the system, and how the system can intervene to prevent a crash.

The audit finally concludes with a summary of all economic incentives provided by the system, shown in Figure 5.
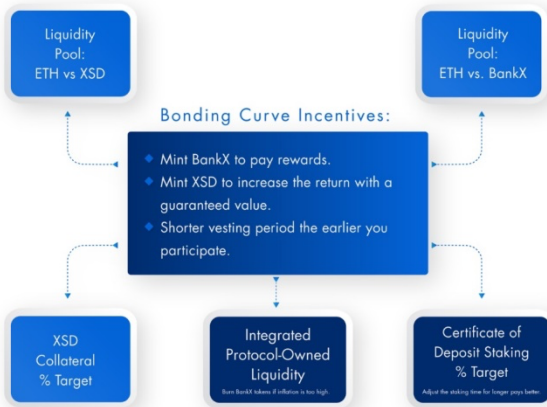
Figure 4. The Terra/Luna crash. Source: [16]

Figure 5. Listing different mechanisms, each one functioning as a deflationary/inflationary dynamic. Source: [23]

5. Conclusion

This paper discussed the different methods and techniques that can be used in order to conduct a tokenomics audit and provided a case study of one such audit.

It is clear that as blockchain adoption grows across multiple industries, tokenomics will play an ever-larger role in this process. Therefore, being able to audit and analyse tokenomic designs objectively, and suggest potential improvements, is a process that is only destined to grow in significance over the next few years.

This is still a new area, and it is likely that many of these methods will adapt and evolve over time, as more audits are published.

The audit presented in this paper was one of the first of its kind. Therefore, some of the methods employed might seem rough, especially from the perspective of traditional econometrics that are more data driven.

Nevertheless, the rapid expansion of blockchain, and methodologies such as agent-based modelling, are going to allow for more complicated audits as

new knowledge is built on top of existing knowledge.

Future work should focus on verifying some of the methods used in this paper and extending them. Also, an important research topic for future work is the development of a more concrete framework which can be used to analyse projects end to end. Right now, such a framework is missing.

Perhaps, in the near future, auditing tokenomics will be an integral process of launching a project, much like smart contracts auditing is currently. It is the author's hope that this paper helps achieve this vision.

_____

_____

References

[1] C. Dixon, "Crypto Tokens: A Breakthrough in Open Network Design," Jun. 01, 2017. [Online] https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef (accessed Feb. 20, 2022).

[2] S. Nakamoto, "Bitcoin P2P e-cash paper," Satoshi Nakamoto Institute. Oct. 31, 2008. https://satoshi.nakamotoinstitute.org/emails/crytography/threads/1/ (access Feb. 20, 2022).

[3] P. Roosenboom, T. van der Kolk and A. de Jong, "What determines success in initial coin offerings," *Venture Capital*, vol. 22, no. 2, pp. 161-183, 2020.

[4] F. Zeke, "Anyone Seen Tether's Billions?," Oct. 07, 2021. [Online]. https://www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether. [Accessed Feb. 20, 2022].

[5] K. Reynolds, "In Token Crash Postmortem, Iron Finance Says It Suffered Crypto's 'First-Large-Scale-Bank Run,'" Jun. 17, 2021. [Online] https://www.coindesk.com/markets/2021/06/17/in-token-crash-postmortem-iron-finance-says-it-suffered-cryptos-first-large-scale-bank-run/. [Accessed Feb. 20, 2022].

[6] "Frax Finance Analysis," *Albaron Ventures,* April. 30, 2021. https://albaronventures.com/frax-finance-analysis/. [Accessed February 20, 2022].

[7] D. S. Kampakis, "Is agent based modelling the best tool for tokenomics?," *The Data Scientist,* Feb. 23, 2018. https://thedatascientist.com/agent-based-modelling-tokenomics/ (accessed Feb. 20, 2022).

[8] A. Rak, A. Kuceyeski and M. Weiner, "A Network Diffusion Model of Disease Progression in Dementia," *Neuron,* vol. 73, no. 6, pp. 1204-1215, Mar. 2012.

[9] D. Kempe, J. Kleinberg, and E. Tardos, "Influential Nodes in a Diffusion Model for Social Networks," in *Automata, Languages and Programming,* pp. 1127–1138, 2005.

[10] D. Lumbroso and M. Davison, "Use of an agent-based model and Monte Carlo analysis to estimate the effectiveness of emergency management interventions to reduce loss of life during extreme floods: Emergency management interventions during extreme floods," *J. Flood Risk Management,* vol. 11, pp. S419-S433. Jan. 2018.

[11] M. Naili and M. Bourahla, "Stability-based model for evacuation system using agent-based social simulation and Monte Carlo method," *International Journal of Simulation and Process Modelling,* vol. 14, no. 1, pp. 1-16, Jan. 2019.

[12] J. Von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, 1944.

[13] Omniscia, "Algorithmic Currency Protocol Security Audit," [Online]. https://omniscia.io/olympusdao-algorithmic-currency-protocol./ [Accessed Feb. 20, 2022].

[14] OlympusDAO, "Olympus Game Theory," [Online]. https://docs.olympusdao.finance/main/whitepapers/game-theory. [Accessed Feb. 20, 2022].

[15] OlympusDAO, "The Game (Theory) of Olympus," Mar. 16, 2021. [Online]. https://olympusdao.medium.com/the-game-theory-of-olympus-e4c5f19a77df. [Accessed Feb. 20, 2022].

[16] Terra Foundation, "About the Terra Protocol" [Online]. https://docs.terra.money/docs/learn/protocol.html. [Accessed Feb. 20, 2022].

[17] D. Nine, "Ecosystem Risks – How real are they?" Jan. 12, 2022. [Online]. https://mobile.twitter.com/DU09BTC/status/1481375730869149701. [Accessed Feb. 20, 2022].

[18] Rosenfeld, M. (2014). Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009.

[19] "The gambler's guide to Bitcoin mining," Jun. 30, 2014. https://hashingit.com/blog/2014-06-30-000/ (accessed Feb. 20, 2022).

[20] BankX, "Economic Audit," January 2022. [Online]. https://bankx-1.gitbook.io/bankx-u/TvXTfD2DbXKHPHYHZgTC/audits/economic-audit. [Accessed Feb. 20, 2022].

[21] Hex, "Hex" [Online]. https://hex.com/. [Accessed Feb. 20, 2022].

[22] Frax, "Frax" [Online]. https://frax.finance/. [Accessed Feb. 20, 2022].

[23] "Coinmarketcap," [Online]. https://coinmarketcap.com/. [Accessed Feb. 20, 2022]