

Work Project Format: Field Lab

Group Component Title:

**TOKENOMICS MODELS FOR A MULTI-COMPANY LOYALTY  
PROGRAM: A MONTE CARLO METHOD APPROACH**

Individual Component Title:

**TOKENOMICS MODELS FOR A MULTI COMPANY LOYALTY  
PROGRAMS: A MONTE CARLO METHOD APPROACH - REGULATORY  
IMPLICATIONS IN THE EU**

**MARTINA CROCE**

Group part

A Work Project, presented as part of the requirements for the Award of a Master Degree in Business Analytics from the NOVA – School of Business and Economics.

# TOKENOMICS MODELS FOR A MULTI-COMPANY LOYALTY PROGRAM: A MONTE CARLO METHOD APPROACH

MARTINA CROCE  
MORITZ ZENG MÁRQUEZ  
UTKU SERDAROĞLU

A Project carried out on the Master in Business Analytics, under the supervision of:

Advisor: Leid Zejnilovic  
Co-Advisor: Lénia Mestrinho

February 25th, 202



## **Abstract**

The research aims to provide Celfocus with a comprehensive comparative analysis of tokenomics models for multi-company loyalty programs, highlighting their strengths and weaknesses to aid informed decision-making. This involves an in-depth analysis of current loyalty schemes, assessing the impact of tokenization in the digital economy, and exploring how blockchain and gamification can transform customer loyalty experiences. The study includes the development of three unique token-based loyalty programs, designed to optimize benefits for both partner companies and customers. It also addresses challenges and regulatory considerations, with a particular focus on GDPR compliance. The effectiveness of these models was validated through a Monte Carlo analysis, which involved simulating various scenarios to identify critical elements and evaluating key performance indicators for a more profound understanding.

**Keywords:** Loyalty program, Gamification, Blockchain, Tokenomics, Monte Carlo simulation, Technology, Marketing,

## List of abbreviations

|      |                              |
|------|------------------------------|
| LP   | Loyalty Program              |
| MCLP | Multicompany loyalty program |
| TKN  | Token                        |
| PoS  | Proof of Stake               |
| PoW  | Proof of Work                |
| KPI  | Key Performance Indicator    |

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

## Introduction

This master's thesis aims to develop innovative tokenomics models for a multicompany loyalty program tailored specifically for our client, Celfocus. The proposed models will leverage the synergies between partner companies and customers, the two primary agents in this ecosystem. By strategically utilizing these interactions, the models are designed to maximize the benefits for both groups, ensuring a mutually advantageous system. In detail, customers can use loyalty points earned through transactions made from a partner across all the others; partners, on the other hand, maintain customers' fidelity, which is a common problem traditional loyalty programs<sup>1</sup>.

Our client commissioned the exploration of different Tokenomics options, so we started our research by exploring academic and industry literature to establish which types of models already exist, what are the typical components of the models, how are the operational rules designed to ensure engagement, and how to ensure sustainability. The research developed three distinct models characterized by unique features and mechanisms. As can be seen in the following chapters, the first model is based on a private blockchain with a fixed token value along the lines of different already existing projects on the market (Wang et al., 2018); Moreover, given the objective provided by the client, it was decided to realize the remaining models with a different approach: the second model is based on a public blockchain with a volatile token price, while the third model is based on a sidechain with a fixed token price.

We used the Monte Carlo analysis to simulate a wide range of scenarios to validate the models' effectiveness, thereby exposing potential weaknesses and identifying sensitive aspects. The goal of the research is to provide a comparative analysis of different tokenomics models for our

---

<sup>1</sup> <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-making-blockchain-real-for-loyalty-rewards-programs.pdf>

client, to provide the tools to understand the strengths and weaknesses of each one and to make better-informed decisions.

## **Loyalty Programs**

A crucial tool in marketing that encourages periodic business and building relationships with customers are loyalty programs (LPs). A loyalty program is defined as a strategy where a business acts as a service provider to create value for its customers, aiming to promote their loyalty behaviors. In this context, the clients serve as recipients of the service, finding value in elements such as relationships, status, and habits (Henderson, Beck, & Palmatier, 2011). A LP's debut aids in creating a sense of perceived value, which encourages customers to sign up for, remain with a LP, and strengthens their relationship with the company and their purchasing habits. Customers can accrue points, miles, or other currencies as incentives and exchange them for prizes. (Chen, Mandler & Waarden, 2021). The word "loyalty program" is being used to refer to all these concepts and several types of programs designs that ought to have the following features. (Dorotic, Bijmolt & Verhoef, 2012).

- Foster loyalty: Promotes and rewards members' behavioral and attitudinal loyalty, which in turn promotes customer retention and share development. This is the primary goal of an LP. Successful LPs cultivate relationships with customers to persuade them to buy from the program provider more frequently, make more purchases overall (such as upgrades and cross-purchases), and raise their share of wallet (SOW) at the focal provider or brand.
- Reward: A LP should provide its members with a means of accumulating LP currency based on their purchasing behavior as a way of showing appreciation for their loyalty, either now or in the future. Discounts, products, services, customized offers, or special treatment are all extended to cardholders.

A typical loyalty program encourages repeat purchases by providing points that may be used for redeeming the future discounts. Customers that visit infrequently could not be interested in the program since they receive their rewards too slowly, which would discourage them from visiting more often. Alternatively, stores with comparatively long purchase cycles might profit from signing up for a loyalty program, which offers incentives that can be accrued and used. Because of this, the aim of incentive programs is to create brand loyalty by giving out points to customers who stick with a certain company. You can trade in your accrued points for gifts, discounts, or ascend to higher LP tiers. This process is influenced by three primary processes (Blattberg et al. 2008). First, there is the loyalty point accumulation system, which operates on the principle of point pressure: members are more inclined to make more purchases if they believe they will soon receive a reward. Second, a behavioral reward system affects how participants behave and think after getting one, strengthening their bond with the organization in the process (Waarden & Benavent, 2009). Third, members' behavioral and attitudinal reactions are improved by the personalized marketing method (appendix, fig. 1).

With the active engagement in LPs on the decline, their impact on fostering loyalty is diminishing (Wollan et al., 2017). According to Shugan (2005) one of the most important reasons of this decline is motivations and preferences are not met in the standard programs. This inconsistency in results highlights the need for more comprehensive research into how LPs influence consumer behavior and how companies can make their LPs stand out from those of their competitors. Multi-brand loyalty programs have emerged as a dynamic alternative to traditional single-brand loyalty programs, aiming to offer a wide range of options and selections among partner companies while seeking to meet customer preferences by creating a symbiotic ecosystem. These collaborative initiatives, involving multiple and often diverse brands, allow customers to earn and redeem rewards across a diverse range of goods and services, thereby

enhancing the perceived value of the rewards. Unlike single-brand programs that are limited to the offerings of one brand, multi-brand loyalty programs transcend these limitations by providing a network of options for customers. This approach not only broadens the scope for customer engagement but also introduces a degree of complexity. Managing a multi-brand loyalty program requires sophisticated coordination between different entities, each with its own unique objectives, customer engagement strategies, and values. Aligning these diverse elements into a cohesive and effective program is a significant challenge. However, despite these complexities, multi-brand loyalty programs offer a compelling proposition. They cater to the more omni channel customer by offering diverse rewards and experiences across various brands. Even though multi-brand loyalty programs represent a complex, networked approach to customer loyalty, their potential to offer a richer and more varied experience makes them an attractive option in today's diverse market.

## **Community & Marketing**

Studies suggest that engaging clients to engage in brand communities—organized social networks involving brand users—is beneficial. Programs sponsored by organizations that give members a sense of community and transfer support organizations to them are known as community loyalty programs. The shared interest amongst the members of the group leads to a sense of belonging. A brand community strengthens the bonds between consumers and the brand or brands, as well as between customers and each other. According to McMillian and Chavis (1986), people experience a feeling of community when they benefit in four different ways from contributing to a particular group. These advantages are (Rosenbaum, Ostrom & Kuntze, 2005):

- Membership and a feeling of inclusion
- Influence, a feeling of significance

- Needs integration and satisfaction, or the perception that group membership will lead to the fulfillment of members' needs
- Common emotional ties, the dedication and conviction that members have shared and will continue to share a history, locations, time spent together, and comparable experiences. Shared locations, quality time, and analogous experiences.

The "brand community" revolves around the needs of the consumer; client experiences are what give the community its existence and significance. A community is made up of patrons who have similar interests in a particular brand or product. In today's competitive marketing landscape, brand community provides a novel, efficient, and viral method of brand development. Consequently, marketers can use this tactic to set their goods, services, and businesses apart from the competition and gain advantages (Kohlmeyer, 2016). Establishing a brand community can help create significant exit barriers that encourage consumers to stay involved with the product or brand over the long run. One particularly effective marketing approach is to encourage customers to join brand communities, which are characterized as "specialized, non-geographically bound communities" or as structured social relationships among brand users (McAlexander et al., 2003).

## **Tokenomics strategies**

Tokenomics first came up in academic discussions in the 1970s but really caught on after 2017, thanks to the popularity of Bitcoin. Essentially, tokenomics involves the study and design of economic systems that use digital tokens. These tokens are used to motivate certain actions within a community, with the goal of creating a self-sustaining micro-economy. This idea has become more important in the world of digital currencies, marking a notable change in how we use economic concepts in the digital age (Au & Power, 2018).

In this context, understanding the utility of a token becomes crucial. According to FINMA (2018, p. 3), tokens have three functions. Payment tokens are designed to function as a digital means of payment. They represent value and can be transferred, stored, or traded electronically, much like traditional currency. These tokens are not specific to any project or service but are intended as a general medium of exchange for goods and services, such as Bitcoin (BTC). As a secondary, utility tokens, on the other hand, provide access to specific products or services within a particular project or platform. They can be likened to digital 'coupons' or 'tickets', granting holders certain rights or privileges within their respective ecosystems. These tokens are usually project-specific and can enable functionalities like voting in governance decisions or using features of a platform. Ethereum's Ether (ETH) is an example of a utility token. While it holds value and can be traded, its primary function is to facilitate operations on the Ethereum network, such as executing smart contracts and paying transaction fees. Asset tokens represent digital ownership of an asset, which could range from real estate and stocks to commodities. These tokens digitize real-world assets, making them more accessible and tradable on blockchain platforms, such as the Aspen token issued by St. Regis Aspen Resort in Colorado, United States of America.

Tokens are typically created during the project's launch. This can be done all at once (pre-mined) or over time (as in Bitcoin, where tokens are created as mining rewards). In Proof of Work (PoW) systems that encourage overtime mining, the degree of influence that miners have on the blockchain's progression is determined by their computational efforts or work invested in maintaining the system. This effort involves solving computational puzzles, a concept initially suggested by Dwork and Naor. They recommended using pricing functions to control access to specific information. This concept has been further developed by shifting its application from an authentication tool to a means of verifying the computational resources

expended over a certain period (Jakobsson & Juels, 1999).

In Proof of Work (PoW) blockchain systems, such as Bitcoin, mining rewards play a crucial role. Here, tokens are created and awarded to miners who successfully validate and add new blocks of transactions to the blockchain. This mechanism not only incentivizes the ongoing maintenance and security of the blockchain but also methodically increases the supply of tokens in circulation (Narayanan et al., 2016).

Alternatively, Proof of Stake (PoS) systems employ staking rewards, wherein validators, or stakers, are allocated new tokens for contributing to network security by holding and staking their tokens. This system is lauded for its energy efficiency compared to PoW and serves as a robust incentive for sustaining network integrity (Saleh, 2021).

In Proof of Burn (PoB) systems, such as Slimcoin, miners secure the right to mine new blocks by sending tokens to a non-recoverable 'burn address', effectively removing these tokens from circulation and reducing the overall token supply. This action benefits the remaining token holders as the value of the system is now spread over fewer tokens. The miner who burns the most tokens gets to mine the next block and earn transaction fees. This system, which aligns with the miners' profit motives, ensures network security through the economic cost associated with burning tokens.

The distribution of tokens is integral to the concept of tokenomics, offering diverse methodologies tailored to the unique needs and strategies of different projects. Initial Coin Offerings (ICOs) have emerged as a method for token distribution, primarily used by emerging projects to gather capital, such as Ripple Coin. In this approach, tokens are exchanged for established cryptocurrencies like Bitcoin or Ethereum. The ICO model has attracted considerable attention, especially from a regulatory standpoint, underscoring the need for more

explicit regulatory frameworks in the cryptocurrency domain (Catalini & Gans, 2020).

Airdrops represent another distribution strategy, where tokens are freely distributed to existing cryptocurrency holders' wallets, often based on a predetermined blockchain snapshot. For instance, Basic Attention Token (BAT) has been known to use airdrops to incentivize user participation in the Brave browser ecosystem. This technique is employed to promote broader token distribution and adoption, functioning both as a marketing instrument and a means to incentivize community engagement and loyalty (Zetsche et al., 2019).

Another tokenomic consideration to be made is the concepts of governance and democratic voting, particularly in the realms of decentralized finance (DeFi) and decentralized autonomous organizations (DAOs). These systems leverage blockchain's inherent transparency, security, and inclusivity to revolutionize decision-making processes. Blockchain governance pertains to the mechanisms that guide decision-making in the development and management of blockchain networks or decentralized applications. In blockchain projects, however, governance is often democratized, granting token holders the power to influence key decisions a shift toward more egalitarian and participatory governance structures (De Filippi & Loveluck, 2016). By integrating token-based voting systems, the projects are pioneering new forms of digital democracy, not only empowering token holders but also aligning their interests with the long-term viability and success of the platform.

Token-based democratic voting is a core feature in these systems, with the number of tokens held often dictating the weight of a holder's vote. This method allows token holders to vote on a range of issues, from software and protocol changes to strategic and budgetary considerations. Such inclusive governance models embody the decentralized ethos that is central to many

blockchain projects. For instance, MakerDAO, a leader in the DeFi space, empowers its MKR token holders with voting rights on crucial decisions, such as modifying interest rates and adjusting risk parameters. This participatory model ensures that community consensus drives decision-making, aligning with the decentralized nature of the platform (Warren and Dai, 2018). In the cryptocurrency sector, Decred presents a notable example of community-driven governance. Holders of Decred's DCR tokens actively participate in the governance of the network, including protocol amendments. The project's unique combination of Proof of Work and Proof of Stake consensus mechanisms augments its governance structure, supporting a more equitable and democratic decision-making process (Yli-Huumo et al., 2016).

## **Blockchain**

Blockchain technology may have started with a 1982 paper written by computer scientist David Chaum, but it gained popularity after Bitcoin, a cryptocurrency founded by an unidentified individual or individuals known only as Satoshi Nakamoto, became well-known. A blockchain is just a simple ledger with transactions listed one after the other. Modern cryptocurrencies are digital money that is safeguarded by cryptographic techniques rather than a central database or authority. Blockchains are decentralized digital ledgers that function without a central repository or central authority, such as a bank, business, or government. They allow a community of users to record transactions in a shared ledger among the community, so that, during the normal operation of the network, no transaction can be changed once published (Yaga et al., 2019). Another definition of blockchain is described by Sheth & Dattani (2019), who define that blockchains are a distributed ledger composed of blocks. Each block consists of a header containing the block's metadata and the transaction data recorded within it. The header of each block, with the exception of the first, contains a cryptographic link to the header of the previous block. Each transaction involves one or more users of the blockchain network

and is recorded in the block once it has been digitally signed by the users who performed the transaction. Users use public and private keys to digitally sign and perform secure transactions within the system (Clarke, 1962). One aspect to be considered when discussing blockchain technology is the way in which participants agree on the validity of a transaction: one speaks in this case of 'reaching consensus'. Two diverse categories of blockchain can be identified: permissionless and permissioned. Anyone can read and write on a permissionless blockchain network without requiring authorization. Permissioned blockchains restrict participation to specific individuals or organisations and allow more detailed controls (Chand, 2018). Four key features of blockchain are:

- Registry: it uses an immutable registry to provide the whole transaction history; unlike traditional databases, transactions, and values in a blockchain are not overwritten
- Secure: blockchains are cryptographically secure, guaranteeing that the data in the ledger has not been tampered with and that the data is verifiable
- Shared: the ledger is shared between multiple participants, providing transparency between nodes participating in the blockchain network
- Distributed: the blockchain can be distributed, making it possible to increase the number of nodes in a blockchain network to make it more resistant to malicious actors' attacks.

Blockchain technology aims to provide third-party benefits such as integrity, authenticity, security, and non-repudiation in a distributed and decentralised environment. In addition to verifiability and transparency, it offers immutability (stored transactions are not modifiable once published). These features, besides being fundamental for currency systems, are useful for any transactional system that is to be used by several independent trustless parties (Wright,

2023). For blockchain networks that allow anyone to create accounts and participate anonymously (called permissionless or public blockchain networks), these features ensure a level of trust between the parties without any mutual knowledge; this trust can allow individuals and organisations to transact directly, which can result in transactions being conducted faster and at lower cost. For a blockchain network that more tightly controls access (called permissioned or private blockchain networks), where some trust between users may be present, these features help to reinforce that trust (Gupta, 2017). Going a little more specific, blockchain networks use consensus models for the publication of blocks, but such methods often do not require expenditure or maintenance of resources (as is the case with current permissionless blockchain networks).

This is because one's identity needs to be defined to participate as a member of the authorised blockchain network (Yaga et al., 2019). With the introduction of authorised blockchains, users can opt for their adoption by placing constraints and customising the behaviour of network nodes. While with classical blockchains it is possible to build a completely open and decentralised system, authorised blockchains only allow a limited number of users to have the right to validate transactions. Validators constitute a set of nodes that can be publicly elected or selected by a central authority (Belotti, 2019).

Going into more detail, blockchain technology uses well-known computational mechanisms and cryptographic primitives (cryptographic hash functions, digital signatures, asymmetric key cryptography) mixed with record keeping concepts. Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a digest) for an input of almost any size (e.g., a file, text, or image). It allows users to independently take the input data, hashing it, and derive the same result, proving that there has been no change in the data (Preneel, 1994). In conclusion, a blockchain is a read-only immutable data structure,

Group part

in which new entries (blocks) are added to the end of the ledger by linking to the 'hash' identifier of the previous block.





## **Research Context and Tokenomics Models**

The burgeoning field of tokenomics presents an avenue for enhancing the efficacy of multi-company loyalty programs (MCLPs). Tokenomics offers a novel approach to loyalty programs. By incorporating tokenomics into MCLPs, we explore how digital tokens can be used as an incentive mechanism to foster customer loyalty and increase engagement across a network of partner companies.

This thesis delves into the application of tokenomics in loyalty programs, raising critical questions:

How can tokenomics be leveraged to create increased value within a Multi-Company Loyalty Program (MCLP)?

This question probes the fundamental potential of tokenomics in revolutionizing traditional loyalty schemes. It explores the dynamics of customer engagement, reward structures, and the overall value proposition offered to both customers and partner companies.

How would different Tokenomics Models, with varying design features, cater to an MCLP business model?

Here, we examine the suitability and adaptability of diverse tokenomics models to the specific needs and contexts of an MCLP. This involves a close analysis of the models' structure, economic principles, and their operational feasibility within the loyalty program ecosystem.

How can tokenomics be leveraged to increase customer loyalty by incentivizing spending?

This question addresses the direct impact of tokenomics on customer behavior, particularly focusing on spending patterns and loyalty.

Are tokenomics models apt to maintain a balance among participating partner companies with distinctive characteristics, competing in the same industry?

The competitive aspect of the partner companies within an MCLP is a critical area of study.

This inquiry explores how tokenomics can be designed to ensure a mutually beneficial

relationship among diverse and potentially competing partners.

Do the tokenomics models prove resilient to different scenarios and environmental factors?

This final question examines the robustness and adaptability of the proposed tokenomics models in the face of various market conditions.

## **Proposed Tokenomics Models**

Here, we present and differentiate proposed models, each designed to test the hypotheses and answer the questions raised earlier. These models are grounded in real-world examples and examples of previous use cases.

An essential component shared by all three proposed tokenomics models is the integration of gamification features. These features are intricately woven into the rules and system design structure of each model, aiming to enhance consumer engagement and loyalty within the Multi-Company Loyalty Program (MCLP). The following section outlines these shared gamification elements and their specific implementations in the models.

A common thread in all models is the use of tier memberships. This approach categorizes consumers into different levels based on their total spending with partner companies. The more a customer spends, the higher their position in the tier system. This system not only incentivizes increased spending but also adds a sense of achievement and progress for the consumers. For those unable to meet the spending requirements to maintain their current tier within a specified period, the models typically provide a mechanism for tier descent, ensuring a dynamic and responsive system. To further encourage consumer spending and engagement, higher token issuance rates are applied to higher tiers. This feature directly rewards more active customers,

fostering a sense of loyalty and incentivizing continuous interaction with partner companies.

Another gamification element is the leaderboard feature. In this setup, customers are ranked according to their total spending within a monthly cohort. The top performers, such as the top 1% or top 5%, are rewarded with additional tokens. This competitive aspect motivates customers to increase their spending to attain higher ranks and earn rewards, thereby driving engagement and loyalty.

The models also include a quest game feature, where customers face new challenges each month, such as shopping at specific partner companies. Successful completion of these quests results in token rewards from the central reserve. Quests can be strategically designed to direct consumer spending towards underperforming partner companies within the loyalty program. This approach ensures a balanced and equitable system for all partners. The quests are algorithmically generated based on the analysis of past transaction data, incorporating a level of decentralized decision-making into the loyalty program.

These gamification features are integral to the design and effectiveness of the tokenomics models. By embedding elements such as tier memberships, leaderboards, and quest games, the models aim to create an engaging and immersive experience for consumers. This approach not only fosters loyalty and repeated engagement but also ensures a fair distribution of benefits among all participating partner companies. The strategic use of gamification is crucial in maintaining the attractiveness and sustainability of the MCLP, making it a key factor in the success of the proposed tokenomics models.

Another important feature common to all three tokenomics models is the incorporation of a democratic voting system for the inclusion of new partner companies into the Multi-Company Loyalty Program (MCLP).

The process begins with a proposal to add a new partner company to the MCLP. This proposal should be initiated by the governing body overseeing the loyalty program upon request from potential new joiners.

Each existing partner company in the MCLP is granted voting rights. This democratic approach ensures that all partners have a say in the evolution and expansion of the network. The voting is typically carried out through a secure and transparent digital platform, integrated within the MCLP's management system. This could be facilitated by the existing blockchain infrastructure underpinning the tokenomics models, leveraging its capabilities for secure and immutable voting records. The criteria for accepting a new partner company are predefined and could include factors such as market reputation, customer base, alignment with the loyalty program's objectives, and potential synergies with existing partners. The decision to incorporate a new partner is based on a majority rule. The specific threshold for a majority can be predefined. Upon a successful vote, the new partner company is integrated into the MCLP. This involves setting up the necessary technical and operational frameworks to ensure seamless interaction with the existing tokenomics model and loyalty program structure.

### **Simple & Stable Model (Model 1):**

As mentioned before, the first model is based on a private blockchain like some already existing projects developed for different companies, such as Chanticleer, Hitachi-PointInfinity, Gege Points, UnionPay, Singapore Airlines, Rakuten and Royal Bank of Canada (Wang et. al., 2018). This model involves two parties: partners and customers. In this model, for each transaction at a partner company, consumers receive an amount of tokens, which have a stable conversion

rate. In turn, consumers can spend their loyalty points towards other existing partner companies within the ecosystem. Then, based on the gamification method, consumers are divided among themselves into distinct levels based on the total amount of money they spend on transactions with the partner companies. In practice, the more customers spend, the higher they get between tiers. In addition, if consumers are not able to cover, within a certain period, the number of purchases necessary to remain in the same tier, they descend. In this model, tokens' supply is dynamic and related to demand and transactions volume. In the model, we see how consumers can redeem their TKN for purchases at any partner company at a stable redemption rate, i.e.,  $1 \text{ TKN} = 0.5\text{€}$ ; moreover, the issuance rate is fixed but differs between the different tiers. Given the stable nature of this tokenomics model, exposure to the public market is not intended or feasible. However, to make participation in the multicompany loyalty program more attractive, consumers have the option of converting their TKN into a fiat currency through a smart repurchase agreement. By paying a predefined commission to partners, consumers can liquidate their TKN. The TKN is proportionally returned to the issuing companies and can then be put back into circulation. The amount accumulated with the fees should be distributed among the partner companies in proportion to the issuance of the liquidated portfolio. In conclusion, in order to maintain a fair and effective loyalty program, a balancing mechanism is essential. Consumers often spend loyalty points impulsively, which can disadvantage companies. To solve this problem, a smart contract solution can be implemented to reduce the redemption rate when consumers use points earned from one company at another one. This strategy encourages consumers to spend points where they were earned, ensuring a more balanced and mutually beneficial loyalty program. An algorithmic approach could be used to maintain a balance between issuance and redemption across partners.

At the implementation level, the first model is developed on a private layer-1 blockchain,

designed according to the principles of decentralisation and security. Layer-1 blockchain refers to the blockchain protocol that serves as the network's foundation. It is a distributed ledger technology (DLT) designed to securely record transactions on a private/public, immutable, and trustless ledger (Jie Xu et al., 2023). In this case, the network is private and managed by the partners participating in the loyalty programme. Each partner hosts one node of the network on its own server infrastructure, ensuring that nodes are distributed on independent servers. The process of validating transactions is entrusted to the algorithms of the smart contracts implemented on the blockchain. Smart contracts determine which node on the network will be responsible for the validation of each transaction (Neudecker & Hartenstein, 2018). Consumers participate in the loyalty programme via a mobile application (Android/iOS) or a web app. These platforms provide an intuitive interface for managing the consumer's token wallet. Through these apps, customers can view their wallet balance, monitor transactions, and participate in loyalty programme activities. Consumers can access their digital wallet to view their current token balance; this section provides details on the amount of tokens earned and spent, enabling transparent management of loyalty programme activities. A detailed transaction log is accessible to users, allowing them to track every token movement over time. This promotes transparency and trust in the system. Users can participate in special initiatives or promotions through the application. This could include registering for new partner services, participating in surveys, or other activities that provide consumers with the opportunity to earn additional tokens. Since the blockchain is private, consumer data and transactions are encrypted and only accessible to authorised actors. Security is built into every level of the system, from key management to encryption of data in transit. Blockchain maintenance and updates are managed collaboratively by partners. Smart contracts can be improved and adapted to meet the changing needs of the loyalty programme, ensuring the sustainability and evolution of the system over time. This Level 1 private blockchain implementation provides a robust technology

infrastructure to support the complex dynamics of the first model and the proposed loyalty programme.

### **Open & Speculative Model (Model 2):**

The second model to be evaluated is more publicly open and has speculative pricing. Unlike the others, the proposed model consists of volatile coin pricing according to the bonding curve and supply. A fixed amount of pre-mint tokens is issued before going live and locked up in a reserve. As the companies decide to join the program, they must acquire a minimum amount of tokens from the reserve at a fixed price. The amount of tokens unlocked from the reserve by the partner companies influences the program's initial token's value, determined by the position on the bonding curve at the supply of tokens in circulation. Partner companies have two management options for their token holdings. First, keep them in circulation for the token-economy, thus, for circulation. Adjustments to the staking balance can only be done in monthly intervals. Second stake a share of their tokens, thus, isolating them from circulation, and increasing their chances to earn rewards from the PoS validation mechanism, to be conducted exclusively by partner companies for all transactions involving token issuance or redemptions. For each block a predefined number of partner companies is selected as validators. The likelihood to be selected as validator node is dependent on a weighted metrics, including the absolute amount of token staked, and the relative amount of token staked. Throughout the program, the model follows an adjustable but predetermined issuance rate that is designed by an algorithm and various parameters (like the current token price and circulating supply). In order to preserve the steadiness of the coin value and create trust in the community, periodic adjustments (on a monthly basis) and open communication with the stakeholders are foreseen. Post-purchase, these tokens are held for reward distribution, with options for companies to replenish their holdings as needed or for staking and reserving for customers. In essence, partner

companies function as both the initial "buyers" and "distributors" of the token. They buy tokens as a stake in the system and then distribute them as rewards based on a customer's purchasing behaviour and the prevailing issuance rate. The adjustable issuance rate ensures that the rewards remain dynamic, attractive, and sustainable over time. When a customer makes a purchase at a partner company, the amount spent is multiplied by the current issuance rate (also dependent on the Tier membership) to determine the number of tokens the customer should receive as a reward from the company's holdings in their wallet. Tokens can be used for redemption in exchange for a good or reward in partner companies or trading. Upon redemption the model remains circular, as the token redeemed are injected into the partner companies' liquid wallet. As for gamification, model 2, integrates the common gamification features. Given the Model's incorporation of active staking mechanism it employs decentralized decision-making, where stakeholders, including partner companies and consumers, are given a say in the program's rules and directions. Voting is conducted through a token-based system, where each token represents a vote. Proposals subject to voting may include adjustments to the program's parameters, algorithmic quests and issuance rates, or decisions about including or excluding new partner companies. To facilitate this, partners and customers should have access to a voting portal, which allows them to view active proposals and request new ones.

At the implementation level, the model is developed on a public level 2 blockchain, designed according to the principles of decentralisation and security. A layer-2 blockchain refers to network protocols that overlap with a layer-1 solution. Layer 2 protocols use layer 1 blockchain for network infrastructure and security but are more flexible in their ability to scale transaction processing and overall network throughput (Sguanci et al., 2021). Potentially, the model could be developed as a layer 2 solution on the Ethereum, Polkadot, Cardano or Binance Smart Chain

blockchains, through respectively the Solidity<sup>5</sup>, Rust<sup>6</sup>, Haskell<sup>7</sup> and again Solidity<sup>8</sup> programming languages. For each case, a smart contract that regulates the pre-minting and the reserve have to be developed; the same smart contract will contain the bonding curve mechanism which will influence the token's price after the initial token distribution. The phase following development consists of compiling the smart contract using a special compiler, such as Truffle or Remix on Ethereum and Binance Smart Chain, cargo-contract on Polkadot and plutus-playground on Cardano. Once the smart contract has been compiled, the deployment can be conducted, which should first take place on a test network, so as to verify the correct functioning of the model, and then on the main network. Also, for the second model, consumers participate in the loyalty programme via a mobile application (Android/iOS) or web app. As in the first model, customers will be able to access their digital wallet to view their current token balance, the amount of tokens earned and spent, enabling transparent management of loyalty programme activities. A detailed transaction log is accessible to users, allowing them to track every token movement over time. This promotes transparency and trust in the system. The mobile and web apps should allow users to view active proposals, vote and propose changes to the programme, ensuring fair and transparent participation in the management of the ecosystem. Blockchain maintenance and updates are managed collaboratively by partners. Smart contracts can be improved and adapted to meet the changing needs of the loyalty programme, ensuring the sustainability and evolution of the system over time. This implementation of a public level 2 blockchain provides a robust technology infrastructure to support the complex dynamics of the second model and the proposed loyalty programme.

---

<sup>5</sup> <https://ethereum.org/en/developers/docs/>

<sup>6</sup> <https://polkadot.network/development/docs/>

<sup>7</sup> <https://docs.cardano.org/>

<sup>8</sup> <https://docs.bnbchain.org/>

### **Sidechain Model (Model 3):**

Model 3 employs a closed ecosystem with sidechain technology, an approach that empowers individual companies within the multi-brand loyalty program with their own dedicated coins. These coins are seamlessly connected to a central common coin which is managed by a third party such as Celfocus, facilitating the conversion of loyalty coins across partner businesses. In this model, the entrance of new partners in the ecosystem is based on the majority vote of existing partners and third party. Beforehand, participating companies collaboratively agree on conversion rates, which are then encoded into smart contracts. This streamlined process not only eases the integration of new partner companies but also ensures a harmonious flow of loyalty transactions.

One of the standout features of this model is its emphasis on user experience. Every consumer is granted a distinct avatar. By completing periodic tasks, they can earn badges, which are also apparent on their personal profile. These badges come with some specific features, such as discount coupons or higher conversion rates from purchases. With every purchase, clients will be rewarded with coins corresponding to the amount spent. In order to create a community around this ecosystem and encourage competition, consumers may see other interacted consumers points and badges on the leaderboard. By implementing personalization, it is aimed at sparking intrinsic motivation while transforming the mundane act of earning loyalty points into an engaging and interactive journey. Earned coins hold tangible value and can be utilized in two flexible ways: clients have the option to redeem them directly with the partner company, enjoying instant benefits, or they can convert these coins into the platform's common currency. The latter option offers unparalleled flexibility, allowing clients to store their converted coins until they find the perfect opportunity to utilize them with any of the participating partner companies. This freedom of choice not only enhances user satisfaction but also encourages long-term engagement with the loyalty program.

At the implementation level, choosing the sidechain on which to develop the model's smart contract requires an analysis of its ability to scale, be secure, have low transaction costs, be widely adopted, and have an adequate level of developer and community support. There are several sidechains based on different blockchains that exhibit these characteristics. Among them there is Polygon, a widely supported and popular Ethereum-based solution that provides a scalable infrastructure and low transaction costs. Either the Truffle suite or the OpenZeppelin suite can be used to develop and compile the smart contract, and these suites need to be configured in order to get a connection to the Polygon network. Without that connection the smart contract could not be deployed on it (Sutopo, 2023). As in the first and second models, consumers will participate in the loyalty programme via a mobile application (Android/iOS) or web app. In this case also, customers will be able to access their digital wallet to view their current token balance, the amount of tokens earned and spent, enabling transparent management of loyalty programme activities. A detailed transaction log is accessible to users, allowing them to track every token movement over time. This promotes transparency and trust in the system. The mobile and web apps should allow users to view active proposals, vote and propose changes to the programme, ensuring fair and transparent participation in the management of the ecosystem. Blockchain maintenance and updates are managed collaboratively by partners. Smart contracts can be improved and adapted to meet the changing needs of the loyalty programme, ensuring the sustainability and evolution of the system over time. This implementation of a sidechain provides a robust technology infrastructure to support the complex dynamics of the third model and the proposed loyalty programme.

In the appendix can be found the comparison table of the three models: appendix (see *Table 2*).

## **Vulnerabilities and mitigation strategies**

Some of the vulnerabilities that could arise with respect to the first model concern both technical aspects of cybersecurity and marketing aspects.

From a cybersecurity perspective, several types of risks can be identified due to different classes of cyber-attacks. These include risks related to smart contracts, as a poorly designed or insufficiently secure code could be exploited for attacks such as exploits, fraud or manipulation of transactions. Another type of risk concerns the security of consumers' private keys. A vulnerability in the handling of private keys could lead to unauthorised access and the compromise of funds and sensitive data associated with tokens (Hasanova et al., 2019). Finally, not to be overlooked are the reputational risks following a successful cyber-attack. Such an attack or the exploitation of a vulnerability could compromise the trust of consumers and partners in the loyalty programme. Reputation protection is essential for the sustainability of the model (Taylor et al., 2020).

From a marketing perspective, the risk of consumer withdrawal from the programme can be identified. This risk relates to the possibility that loyalty programme participants, especially those in higher tiers, may decide not to actively participate or even abandon the programme altogether. This scenario could occur if consumers do not perceive sufficient value in the benefits associated with higher tiers or if they feel that the fees charged are excessive.

The following countermeasures can be implemented to mitigate this risk: periodically updating the benefits offered by the higher tiers of the loyalty programme based on participant feedback and preferences; clearly communicating the benefits associated with the higher tiers on an ongoing basis; and explaining in detail the justification for the fees. Transparent communication can help eliminate doubts and reticence (Magatef & Tomalieh, 2015).



## Simulations

We translated each of the three proposed Tokenomics Models into a Simulation Model using Python. In addition, to the three Tokenomics Models we also programmed a Baseline Model. The Baseline Model mimics the purchasing dynamics in a market without any tokenomics-based purchasing incentives. We thus, use the Baseline Model as a benchmark for the status quo.

To obtain robust results, we define a fixed set of initial partner companies (see *Table 3*) with which we perform iterations across the different Simulation Models. Yet, to account for market ambiguity for each partner company we generate the metrics based on a random distribution. This induces more variation into the Simulation Models. Each Partner Company record is defined by a set of attributes, thus, allowing for performing Monte Carlo Analyses testing for diverse company sets and configurations.

*Table 3: Partner companies records*

| <i>Sample of Initial Partner Data</i> |                   |                   |          |                      |
|---------------------------------------|-------------------|-------------------|----------|----------------------|
| Partner Company                       | Sales Events/year | Avg. Basket Value | Industry | Avg. Purchases/month |
| Partner 1                             | 18245             | 157               | 1        | 0.5                  |
| Partner 2                             | 34002             | 75                | 4        | 3                    |
| Partner 3                             | 19003             | 31.57             | 2        | 9                    |
| Partner 4                             | 43664             | 564.19            | 3        | 0.002                |

Each of the Simulation Models is designed to model the theoretical features of its respective Tokenomics model. The specific features of each Model are preprogrammed as functions (Class methods) that interact within the dynamics and variables of the tokenomics system.

As explained in the Methodological Approach we define a set of parameters and functions that

model the *External Context*. Specifically, we programmatically model four factors impacting the model's dynamics.

- New partners

The ``generate_new_partner_data`` function simulates the creation of new partner data in the model. It generates random sales and average basket value figures within defined ranges and calculates a size factor based on these values. The size factor represents the partner's relative size in the network and is an input to recalculate the number of customers after a new partners entry. The function returns a dictionary with partner attributes, including sales events, average basket value, industry assignment, purchasing rate, and the computed size factor, contributing to introducing variability in new partner characteristics during the simulation.

- Customer incentive curve

We assume that customers' purchasing incentives are not constant, but dynamically respond to an agent's current state. Through the function ``incentive_curve_linear`` we model a linearly shaped incentive curve. This curve links an input variable 'x' to an incentive value, characterized by two key parameters: ``max_value`` representing the upper limit of the incentive and ``slope`` defining the lines steepness in transitions from lower to higher incentives. 'x' represents the aggregation of all factors we proxy to influence an agent's incentive.

- Network growth

The function ``calculate_customer_growth`` models the monthly growth of the customer network. It considers an initial customer count, a base growth rate, and random factors that simulate variability in growth rates. The initial customer count serves as the starting point, and the base growth rate defines the default monthly growth rate. Throughout the simulation, the function introduces random diminishing factors within predefined bounds, reflecting the inherent uncertainty and flattening in real-world growth scenarios. This approach provides a

method to analyse and project customer network growth over time while considering both deterministic and stochastic elements. Such modelling can be particularly useful in assessing the long-term dynamics and potential variations in customer acquisition within a network context, contributing valuable insights to strategic decision-making processes.

The growth rate is complemented by a function adjusting the customer base according to the size of new partners joining the network. It considers the sales contributions of both existing and new partners to determine the appropriate number of new customers to add. This ensures that the customer base scales in harmony with partner size, simulating network growth realistically.

- Competition effects

The ``calculate_competition_effect`` function quantifies competition effects among partners companies. It assesses how competition within industries impacts partner performance. The function counts partners in each industry, calculates the competition effect for each partner based on industry competition, and uses an adjustable factor to control the strength of this effect. It ensures that the competition effect remains non-negative. This function aids in modelling and analysing the influence of competition on partner outcomes within the simulated context.

As for the *Internal Context's Domain of Governance*, across all Models the following features shaping customer expectations are modelled:

- Customer Tiers

A system to classify customers based on their spending. Higher tiers offer greater earning rates for tokens, incentivizing increased spending. Customers can advance to a higher tier by surpassing specific spending thresholds and must maintain a minimum spending level to retain their tier status.

- Leaderboard

A competitive feature that ranks customers based on the tokens they have earned. The leaderboard position can influence the spending incentive, with higher-ranked customers receiving a greater probability to spend due to higher rank-based multipliers.

- Monthly Quests

Gamified challenges that provide customers with specific targets to meet within a month, involving spending a certain amount with a partner. Completing these quests rewards customers with additional tokens, further encouraging engagement and spending within the network.

- Quarterly Decentralized Voting

A democratic process occurring every three months where existing partners vote on the admission of new partner applications. Successful applicants are added to the network, potentially increasing the customer base depending on the size and influence of the new partners. This mechanism simulates the expansion and dynamism of the network's ecosystem.

Additionally, the three models present a spectrum of distinct complexities and functionalities within the Domain of Governance. Model 1 presents a stable and straightforward approach, ideal for private blockchain integration, where the token value remains constant, simplifying customer-partner transactions. Conversely, Model 2 introduces a dynamic landscape with its bonding curve mechanism, where token values fluctuate in response to supply and demand, presenting a more dynamic and speculative market behaviour. This model not only tracks token supply and circulation but also incorporates partner staking and market trends, offering a multifaceted view of token economics. Model 3 operates on a sidechain principle, hosting multiple token types. Each partner possesses unique tokens convertible to a central token, creating a diversified and decentralized token ecosystem. This model's complexity is heightened by variable conversion rates and the central token's fluctuating value, mirroring the

intricacies of a multi-token environment. Collectively, these models range from the simplicity and stability of a private chain (Model 1) to the dynamics of a volatile, market-driven system (Model 2), and to the diversity of a sidechain setup (Model 3).

We capture the *Internal Contexts Domain of Interaction*, specifically the agents' possibilities to act within the system by the following functionalities:

- Spend

In all models, customers have a probability of spending within the partner network, influenced by factors such as tier status, tokens held, and competition among partners. Spending events can earn tokens and contribute to tier advancement.

- Voting

A feature across all models where partners vote on accepting new partners into the network. This simulates the governance aspect, allowing the network to expand or maintain its size through collective decision-making.

- Initial Buy-In (Model 2)

A mechanism where new partners purchase a set amount of tokens upon joining the network. This buy-in is determined by sales events and market conditions, simulating an investment into the ecosystem.

- Staking (Model 2)

Partners in Model 2 can stake their tokens to earn higher "PoS rewards". Staking reflects long-term commitment to the system and reduces the amount of token in circulation, thus, putting deflationary pressure on the bonding curve.

- Token Replenishment (Model 2)

This process involves partners buying additional tokens to maintain their operational liquidity. It is driven by their sales events and market dynamics, ensuring they have enough tokens for customer redemptions and other expenses.

- Set Conversion Rates (Model 3)

This feature allows the adjustment of conversion rates between partner-specific tokens and a central token based on the central token's current value, ensuring fair and balanced token exchange within the network.

- Convert Partner Token (Model 3)

Customers can convert partner tokens to a central token, and vice-versa, facilitating liquidity and utility within the ecosystem, while incentivizing brand loyalty.

## **Results**

### **Comparative analysis of the tokenomics models**

We perform Monte Carlo Analysis with 10000 iterations on an initial customer base (n=500), over a time span of twelve months. The results below show on an aggregated level<sup>9</sup>, the development of key metrics (Total Sales, Number of Purchases, Number of Unique Customers, and Average Basket Value), monthly, compared across Models. In each of the iteration's randomness is induced, across all parameters within predefined probabilistic bounds. Each iteration initiates with a new random seed. However, to ensure comparability we keep the random seed equal across the models, thus initializing each iteration with the same set of four partner companies for each model. However, in each iteration the properties of the four initial

---

<sup>9</sup> To enhance comparability between the models we aggregate performance metrics of all partner companies by month.

Group part

partner companies are subjected to a degree of randomness to increase in-sample variance.

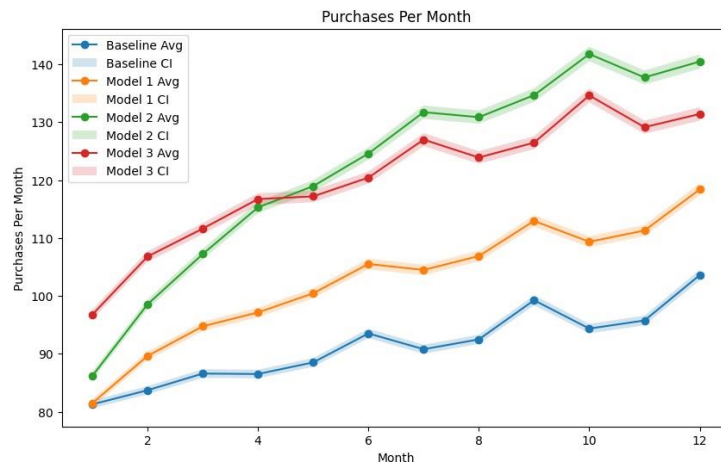


Figure 11: Purchases Per Month

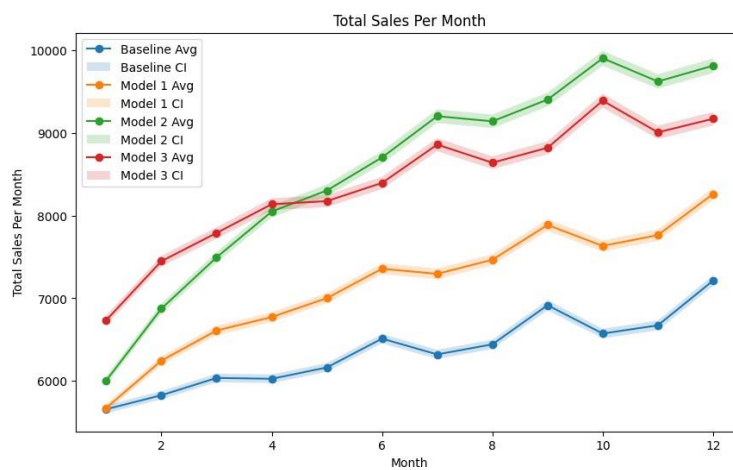


Figure 12: Total Sales Per Month

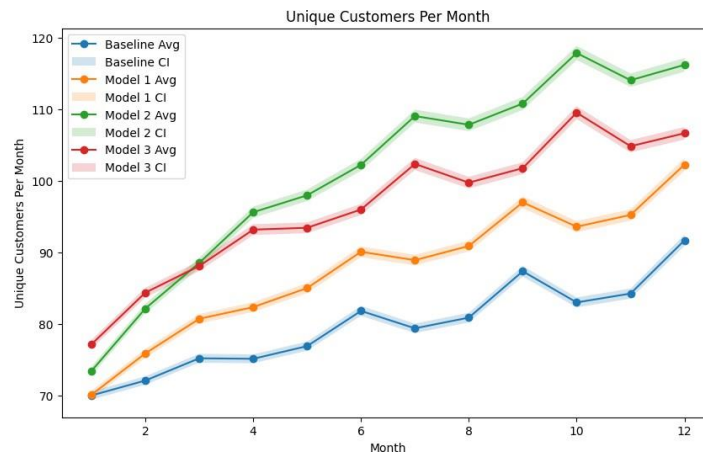


Figure 13: Unique customers Per Month

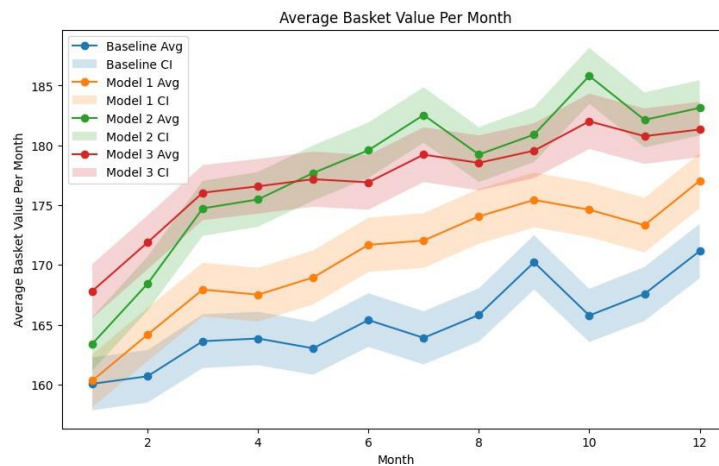


Figure 14: Average Basket Value Per Month

The graphs above provide an overview of the results of the four models developed, in terms of four overall performance metrics over a time horizon of twelve months: Purchases per month (Figure 11), Total Sales per month (Figure 12), Unique Customers per month (Figure 13) and the Average Basket value per month (Figure 14). For comparability, each metric is an aggregation of the monthly averages across partner companies, per model. All models are distinguished by a colour: The Baseline model, marked in blue, lacks a loyalty system, and hence offers no incentives; Model 1, shown in orange, features a stable and straightforward

tokenomics design; Model 2, depicted in green, incorporates a bonding curve; and Model 3, illustrated in red, utilizes a side chain mechanism. Every performance metric shows a growth trend across all models. Across all metrics all Models are upward sloping over a time span of 12 months. This in line with our expectation a growth factor is induced by modelling network effects, and the addition of new customers quasi-proportional to the size of new partner companies, entering through the decentralized vote-in mechanism.

Nevertheless, in all graphs we observe considerable variation across the models in terms of the slope, the curve behaviour, and the starting point of the metric ( $t=0$ ). Across all metrics Model 2 has by difference the highest slope, meaning that it leverages purchasing incentives most effectively. The growth curve of Model 2 exhibits characteristics of a root-function, with its metrics initiating at a similar position as the Baseline Model and Model 1. In contrast, the performance metrics for Model 3 begin higher at  $t=0$ . While Model 3 maintains performance gaps in relation to Model 1, Model 2 starts to outperform Model 3 across all metrics after four months.

Moreover, the graphs show that across all metrics all three tokenomics models as expected outperform the baseline model. For the Purchases per Month, Total Sales per Month, and the Unique Customers per Month we can conclude that at the end of one year, Model 1 and Model 3 outperform the baseline model by more than 10% with 95% confidence. After twelve months Model 2 outperforms the Baseline by more than 20% with 95% confidence in terms of the Purchases.

The Average Basket Value (Figure 14) does not convey the same performance gains in terms of magnitude. While the gaps between the Baseline and Model 1 remain equally high, Model 3 performs comparatively better after twelve months and holds a narrower gap to Model 2. Given a higher degree of variance across the Models in terms of the average basket value the confidence intervals are wider.

All the four graphs show that Model 1 performs better than the Baseline across all metrics, despite starting at the same point as the Baseline.

Model 2's performance-leadership and relatively steep growth are in line with the dynamic token value, in response to supply in circulation as algorithmically enforced by the root-shaped bonding curve. While initial purchasing incentives may not significantly differ from the Baseline, the entry of additional partners and customers, staking-decisions, and token replenishment purchases from existing partners, drive the token value, thus, speculation-based spending incentives upwards.

Model 3 starts higher. This observation could be explained by partner companies having the autonomy to define initial conversion rates for their individual tokens. This flexibility allows partners to leverage more favourable reward conditions since their inception, thus, making it more appealing for customers to start spending and earning rewards right away.

Overall, the results from the performance metrics are in line with expectation.

Within the iterations for each model, we generate and record data, to aid the computation of a set of multi-dimensional System-KPI as proposed in the Methodological Framework. The System-KPI comprise five dimensions. Firstly, we capture *General Performance Metrics* by the Sum of Sales, the Sum of Purchases, and the Sum of Unique Customers after one year across all partner companies. Next, we capture *Customer Retention* by calculating the average purchasing monthly frequency change and the average monthly spending change. Both represent good proxies for the development of a customer's engagement within the system. Third, we capture (relative) *Profitability* by computing the net present value (NPV). Applying a five percent discount rate, we compute each Model's returns as sales in excess of the Baseline. We further capture costs, as opportunity-costs by tracking the cumulative monetary equivalent of tokens redeemed. *System Equity* is another dimension captured by our System KPI. Through

System Equity we seek to make comparable uneven growth tendencies across partner companies per model. System Equity is innovatively measured by computing the total average mean absolute deviation from the average sales growth rate across all partner companies. This is achieved by summing up all monthly absolute growth deviations from the partner companies relative to the total average monthly growth rate. Lastly, we account for customer *Sustainability*, by computing the estimated customer lifetime value (CLTV) for the time horizon of the simulation, here one year.



Figure 15: Radar Chart comparing System KPI across Models

The simulation results highlight differences between the Models in terms of System-KPI (see. Figure 15). In relative terms Models 2 and 3 achieve the highest transactional volume as captured by Sales, Unique Customers, and the number of Purchases. The same observation applies to the CLTV and the NPV. Yet, Model 1's gap in terms of NPV is considerably lower

than for the ‘volume’ metrics and the CLTV. Figure 18 compares the model’s competitive positions across CLTV and NPV to obtain a more comprehensive view about each model’s value creation. The Baseline Model and Model 1 perform best in terms of System Equity, followed by Model 3 and lastly Model 2. Finally, both customer retention metrics draw a more ambiguous picture across models. While the Baseline and Model 2 outperform in terms of Spending Growth, Model 3 and Model 2 perform best in terms of Frequency growth. Competitive differentiation in terms of retention rates is further underscored by Figure 17.

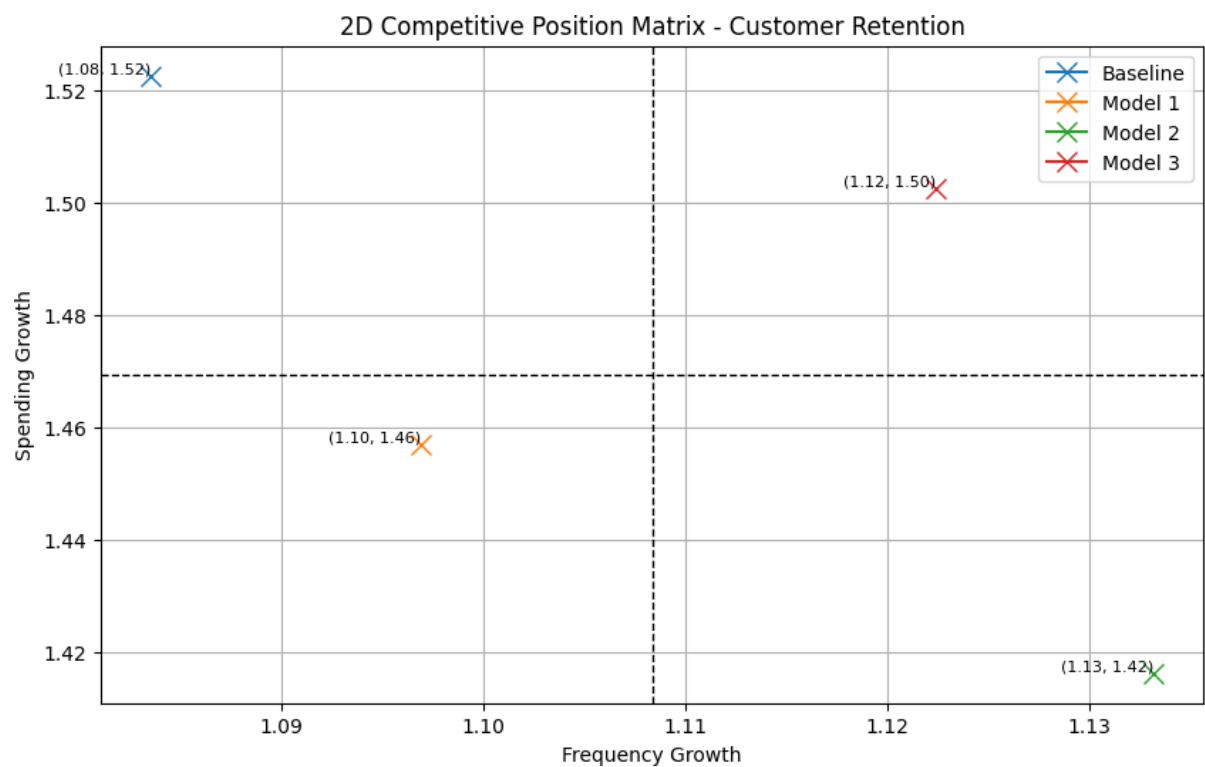


Figure 16: 2D Competitive Position Matrix comparing Models across Customer Retention KPIs

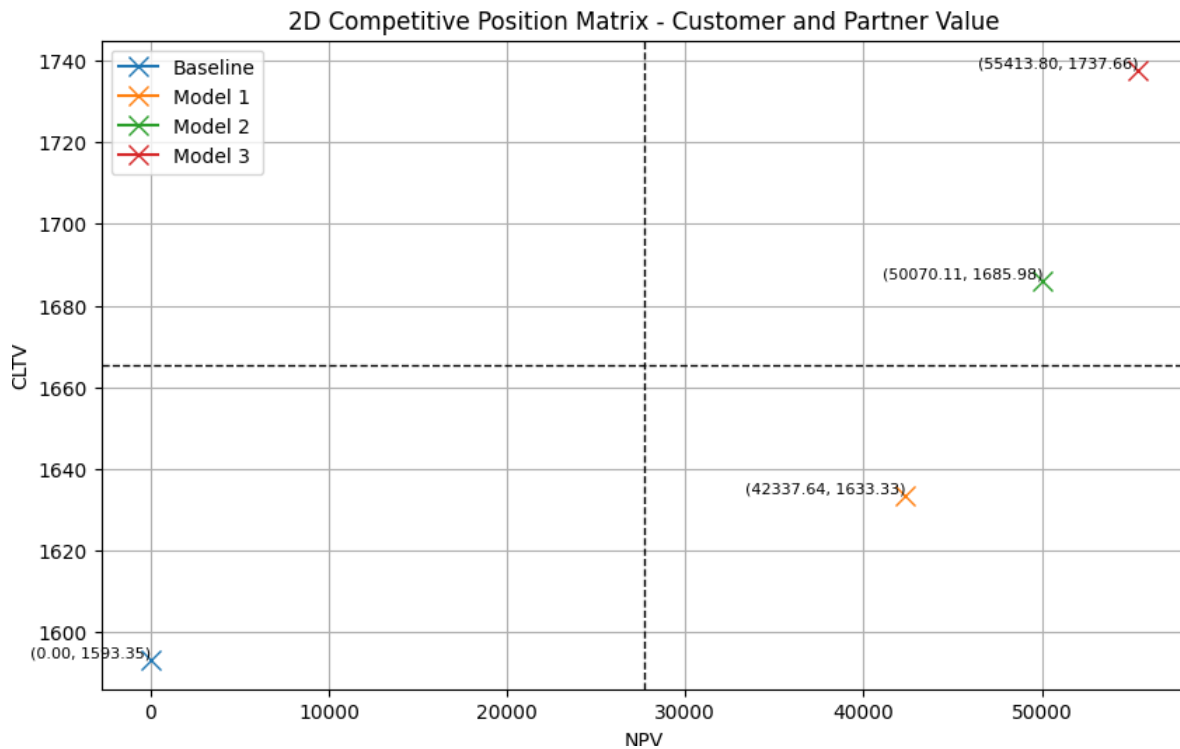


Figure 17: 2D Competitive Position Matrix comparing Models across NPV and CLTV

## Robustness

Given the ambiguity of real-world dynamics potentially altering the context of our tokenomics models, we need to account for such by validating our tokenomics models' performance under the influence of different scenarios, meaning deterministic combinations of specific parameters, and changes of critical controllable and non-controllable parameters, to estimate the Sensitivity. The results from both Scenario-, and Sensitivity Analysis will determine the tokenomics' models bounds of robustness and thus serve as a pivotal benchmark for deployment and configuration as to the client's needs.

### Scenario analysis

Scenario Analysis emerges as a pivotal component of the robustness evaluation. It involves evaluating the models under varying sets of external context parameters while maintaining their probabilistic nature (Hacura et al., 2011). The goal of Scenario Analysis is to amplify variability

and, consequently, the robustness of the models from three primary sources:

The input data for sales metrics, including the number of partner companies and the extent of competition for market share, is subjected to variation. We explore Scenarios based on three factors of variation. First, explore the impact of *different constellations of partner companies*, we hypothesize that an imbalance as we define by a high dispersion between partners, adversely impacts model performance. Second, we account for differences in competitive dynamics among initial partner companies. We expect higher industry concentration among the initial partner companies to negatively impact performance metrics. Partner companies competing in the same industry have a higher likelihood to fulfil the same customer needs and may thus loose a share of their sales to competitors. Third, we account for the scenario of an additional partner company initializing the MCLP system.

The models were evaluated under various scenarios. We compare the different treatment groups from the scenario analysis through parallel-line plots employing a normalized scale for each metric. Findings suggest that a “balanced” constellation of partners is the best conservative choice for the tokenomics models (Figure 18) While, the “balanced” constellation under- the “concentrated-high” constellation, across all value metrics, it presents more stability in terms of partner equity, thus, providing a more sustainable and stable outlook to potential new-joiners. The analysis emphasizes that disperse and highly concentrated models, may not be apt for the presented tokenomics systems to achieve best performance. Such configurations should thus be carefully evaluated. Moreover, the composition of these partners, whether from the same or different industry, also plays a significant role (Figure 20). Loyalty programs that include partners from the same sector tend to create less sales volume, as captured by the CLTV and total sales, while also reducing retention. Nevertheless, a greater industry concentration seems to be slightly positively associated with a higher NPV. As for the initialization with an additional partner company, results show a negative impact across all metrics. This may be

## Group part

indicative of cannibalization, yet the chosen properties of the additional partner company could have driven these effects. A more granular overview of the scenario analysis is presented in the Appendix (Figure 18).

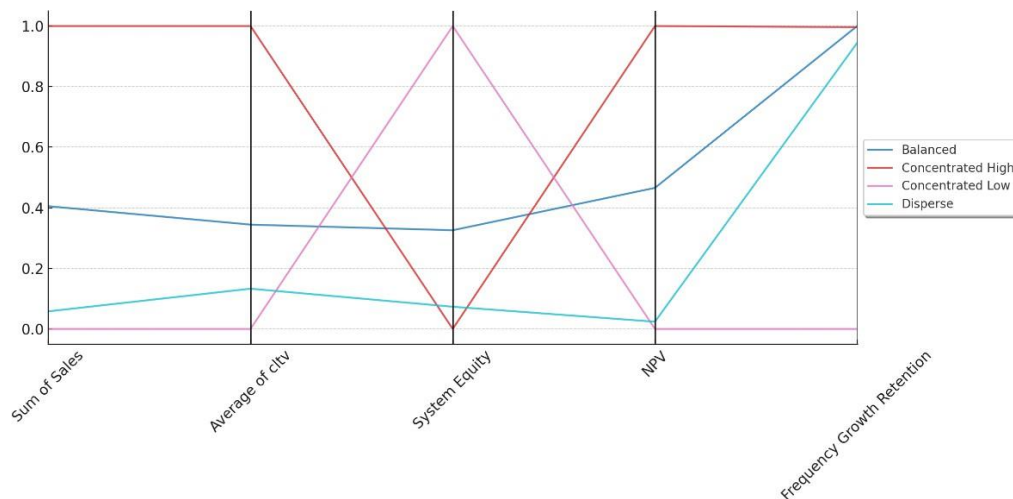


Figure 18: Parallel-line plot comparing KPI performance across different partner constellations on a normalized scale.

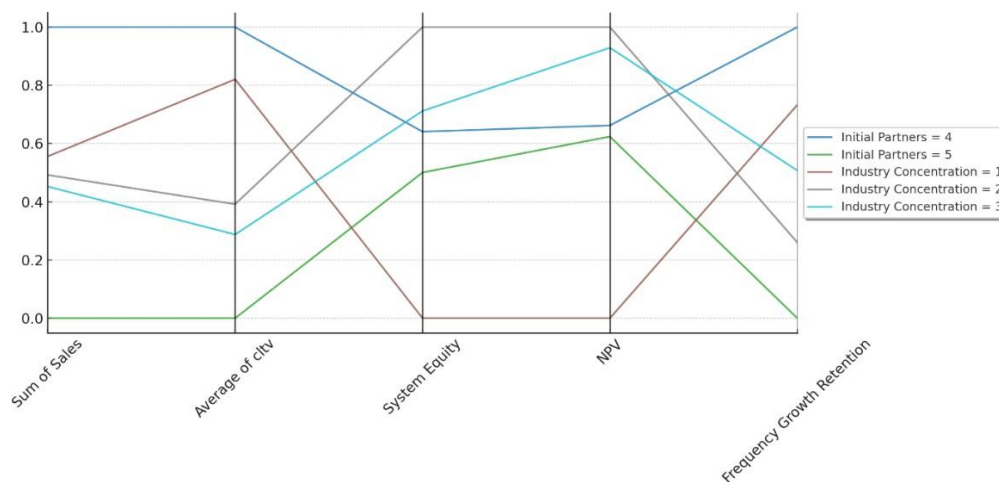


Figure 19: Parallel-line plot comparing KPI performance across different partner constellations on a normalized scale.

## Sensitivity Analysis

We further perform Sensitivity Analysis to assess the impact of specific parameter changes on the models` performance. For each parameter of interest, we define three steps, where each step

represents a different parameter value. Holding all other model-parameters constant we run 500 iterations for each step and compare the results across the four KPI that we consider most comprehensive for this exercise (see Fig. 19). Firstly, the mean of Total Sales after twelve months. Secondly, the mean NPV. Thirdly, the mean of System Equity. Finally, the mean CLTV. Within the Sensitivity Analysis we account for two types of parameters depending on their context within the Tokenomics Model:

- Variations in the Properties of the Tokenomics System (Internal Context): Most importantly, to understand the tokenomics systems' responses to changes in their rules and design an introspective sensitivity analysis is performed. Firstly, we test the sensitivity to varying Gamification parameters, such as Tier-Thresholds, - Rewards, and Leaderboard-reward groups. We also perform model-specific sensitivity analyses to account for variations in Bonding Curve properties and Proof of Stake reward rules for Model 2. Finally, we account test the Sensitivity of Model 3 to variations in the initial Central Token Value, which we expect to influence the customers' purchasing incentives.
- Ambiguity in the External Context: The probabilistic distributions related to purchasing incentives such as (Incremental)<sup>10</sup> Purchasing Incentive resulting from the agents' interaction with gamification, are tested for sensitivity in a range of marginal values. Equally, we investigate the sensitivity of the Network Growth Rate, Competition, and the Base Spend Probability by testing different parameter values within specified stepped ranges.

Figure 18 lists the ten parameters considered for Sensitivity Analysis and summarizes the

---

<sup>10</sup> Incentives modelled to respond incrementally to the obtained and expected rewards from Gamification.

absolute parameter changes per step relative to the baseline. The baseline represents all parameters as included in the default configuration for the Monte Carlo Simulation.

With regards to parametric changes of the Internal Context it is observable that higher Tier-Thresholds are associated with lower Customer Spending as proxied by a reduction in Total Sales and CLTV across all models. This is in line with expected model behaviour, as higher Tier thresholds make more favourable Tier status, thus reward conditions more difficult to attain. However, the NPV reacts differently. Across all models NPVs are lowest at the lowest Tier Threshold, while being highest, or level with step 3 at the baseline configuration. This observation can be explained by the fact that NPVs accrue the monetary value of token redeemed as a cost. NPVs will thus decrease as soon as cost of redemption increases relative to the value of sales. Model 2 exhibits by far the most sensitive NPV with regards to the adjustments in the Tier Thresholds. This is due to the effects of increased demand trickling down on the bonding curve raising the Token value, hence, increasing the cost of redemptions for partner companies. Overall, holding all else equal the default configuration of the Tier Thresholds is close to the optimum.

In terms of Sensitivities in Response to different Tier Rewards; implying token redemption rates per currency unit spent, the Sensitivities across Models and KPI are inconclusive. While the optimum for Model 2 is proximate to the baseline parameter, Model 1 indicates that NPV increase in either direction of the baseline value. Contrastingly, Model 3 hints at a positive effect of Tier Rewards on the NPV as seen by the upward sloping line across its three steps. As for the Tier Rewards this means, high Model-specific sensitivity.

The effect of enlarging the group of customers to receive leaderboard rewards by 5pp and 10pp, respectively as compared to the baseline (1% of highest spending customers) depends on the tokenomics model. Models 1 and 3 are closest to reach an optimum NPV if the 5% of the highest

spending customers receive leaderboard rewards. In contrast, Model 2 performs best, at the baseline configuration, thus, by rewarding fewer customers within the leaderboard.

As for the External Context, the base spend probability reflects a customer's probability to consider a purchase. Naturally, the Sensitivity of this parameter for all Models indicates a strong positive linear relationship between base spend probability and performance.

We granularly model purchasing a customer's purchasing incentive in each point in time through the parametrically defined linear incentive curve. The slope of this curve indicates how steeply a customer's incentives respond to the customers unique components of perception. We define components of perception as any variable uniquely visible to an agent, thus, shaping an agent's perceived benefits from making a purchase, affecting the agent's incentive. An example of such a component of perception is the number of tokens held in an agent's wallet, or the token value. It is observable that CLTVs and Total Sales respond positively to an increase in slope. However, as for the NPV Models 1 and 3 perform better moving in either direction from the baseline ( $a=0.5$ ). Model 2's NPV appears to increase consistently as the slope increases across the steps.

All Models show unexpected sensitivity in response to changes in competition effects. An increase in the effect of competition yields no notable pattern changes to the NPV, System Equity, or Total Sales. Yet, an inverse effect of higher competition effects on NPV is observable across all tokenomics models. Again, this may result from a favourable shift in the equilibrium between the change in spend and redemption.

With regards to the Network Growth Rate, we observe that Model 2's NPV behaves much more sensitively to any changes in the Network Growth Rate. This demonstrates that Models 2's bonding curve mechanism, ruling the relationship of price-demand, and supply, needs careful adjustments to expected Network Growth Rates. Higher Network Growth rates may cause faster

token value appreciations and make token redemptions unproportionally costly for partner companies. Conversely, Models 1 and 3 given their token stabilities are less sensitive and benefit from higher Network Growth Rates.

With regards to Model 2, the sensitivity tests conducted for the Rewards per Block and Bonding Curve Asymptote parameters underscore the need for precise adjustments. For instance, a decrease in Rewards per Block from the baseline might reduce the incentive for new participants to join the network, potentially slowing down the network's expansion and affecting the token's liquidity. Conversely, an increase could accelerate growth but might also lead to inflationary pressures on the token value.

Similarly, changes to the Bonding Curve Asymptote can significantly influence the token supply's responsiveness to price changes. A lower asymptote might make the token supply more elastic, thereby increasing the tokens in circulation for a given price change. This could help stabilize prices in the short term but might introduce long-term volatility if not managed correctly. On the other hand, a higher asymptote could decrease supply elasticity, which might stabilize token value but also risks reducing the responsiveness of the supply to demand shifts. Nevertheless, at the default configuration a higher asymptote or a lower token growth factor may be more beneficial.

Finally, vis-à-vis the 'Central Token Base Value' fluctuations, Model 3 demonstrates a heightened sensitivity, with minor deviations from the baseline affecting the NPV. This indicates that the model's reliance on the central token's stability is significant and that any strategic decisions related to the sidechains tokenomics must be made with consideration of their potential impact of the central token's valuation.

A detailed sample of the Sensitivity Analysis output is shown in *Tables 4-6* in the Appendix.

| <i>Summary of Parameter changes for Sensitivity Analysis</i> |                          |                            |
|--------------------------------------------------------------|--------------------------|----------------------------|
|                                                              | parameter                | step      parameter change |
| Internal Context                                             | Tier Threshold           | 1      -100                |
|                                                              |                          | 2      baseline = 300      |
|                                                              |                          | 3      +100                |
|                                                              | Tier Reward              | 1      -0.025              |
|                                                              |                          | 2      baseline = 0.15     |
|                                                              |                          | 3      +0.05               |
|                                                              | Leader Board Reward      | 1      baseline = 0.01     |
|                                                              |                          | 2      +0.04               |
|                                                              |                          | 3      +0.09               |
| External Context                                             | Spend Probability        | 1      -0.1                |
|                                                              |                          | 2      baseline = 0.25     |
|                                                              |                          | 3      +0.1                |
|                                                              | Incentive Curve Slope    | 1      -0.25               |
|                                                              |                          | 2      baseline = 0.5      |
|                                                              |                          | 3      +0.25               |
|                                                              | Competition Effect       | 1      -0.1                |
|                                                              |                          | 2      baseline = 0.15     |
|                                                              |                          | 3      +0.1                |
| Bonding Curve                                                | Network Growth Rate      | 1      -0.01               |
|                                                              |                          | 2      baseline = 0.03     |
|                                                              |                          | 3      +0.01               |
|                                                              | Reward per Block         | 1      -60                 |
|                                                              |                          | 2      baseline = 90       |
|                                                              |                          | 3      +60                 |
|                                                              | Bonding Curve Asymptote  | 1      -0.75 bn            |
|                                                              |                          | 2      -0.5 bn             |
|                                                              |                          | 3      baseline = 1 bn     |
| Sidechain                                                    | Central Token Base Value | 1      -0.25               |
|                                                              |                          | 2      baseline = 0.5      |
|                                                              |                          | 3      +0.25               |

*Fig. 20: Summary of Parameter-changes for Sensitivity Analysis*

The scenario and sensitivity outcomes inform the necessary adjustments to the tokenomics models, to ensure robust and adaptability to realistic market fluctuations and customer

Group part

behaviours. Overall, this analytical approach not only enhances the predictive power of the models but also aids in the strategic planning and risk management of the tokenomics system.

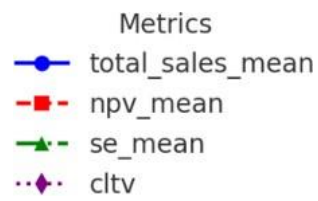


Figure 21: KPI Legend for Sensitivity Analysis

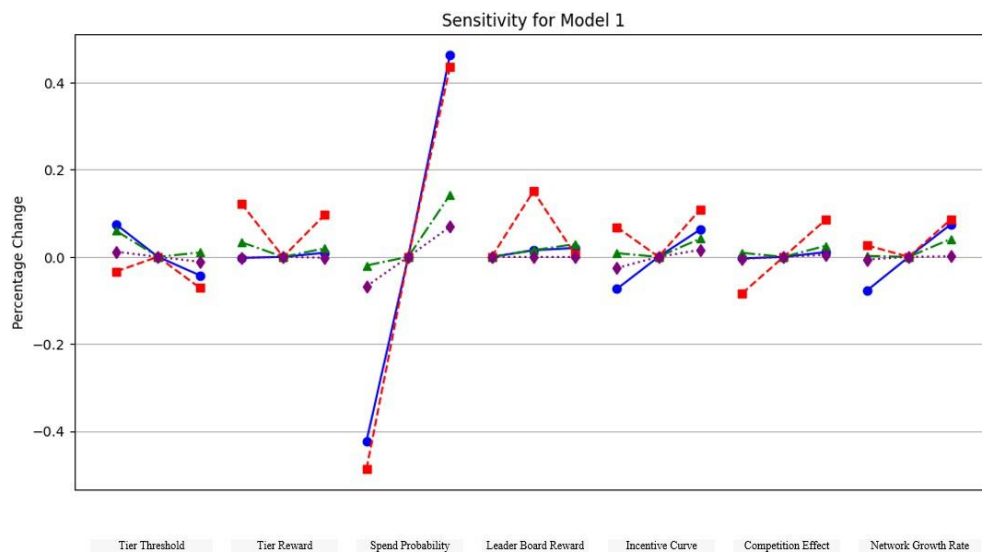


Figure 22: Sensitivities for Model 1

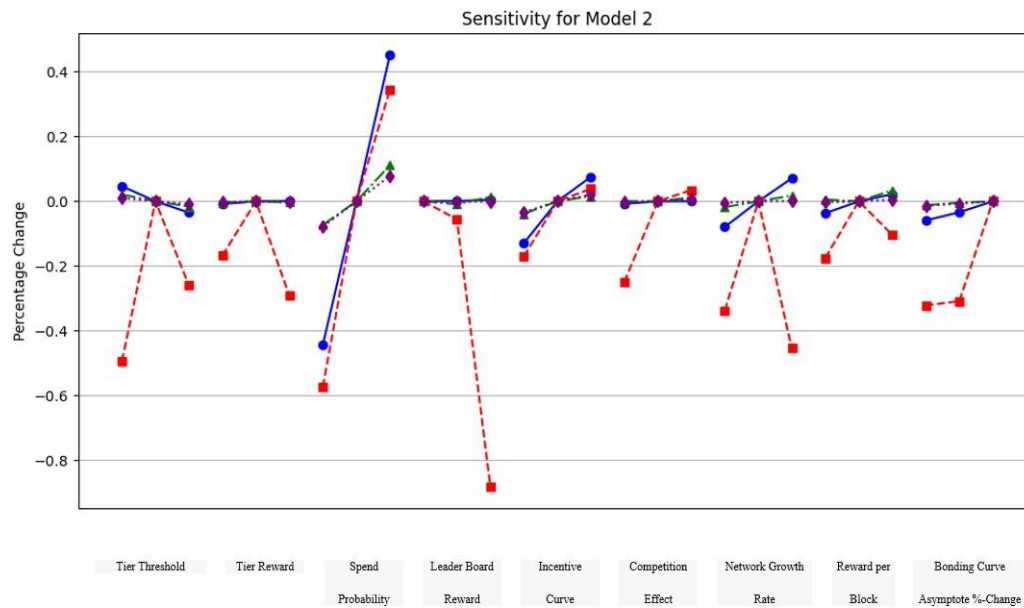


Figure 23: Sensitivities for Model 2

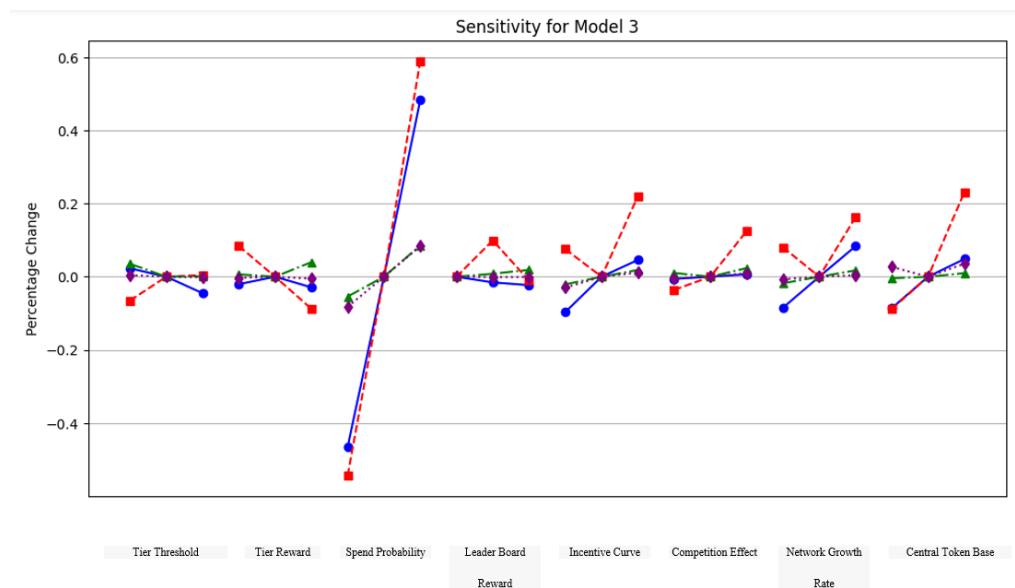


Figure 24: Sensitivities for Model 3

## Confidence intervals

In assessing the robustness of our tokenomics models, confidence intervals play a significant role. By running numerous iterations, we can observe the range of outcomes for each variable

and determine the probability that the true value of a parameter falls within a specific range. The confidence interval gives us a measure of the precision of our simulation results and the reliability of the model under various scenarios. Should the interval be too wide, it would indicate a prominent level of uncertainty and a potential need for parametric refinement. Incorporating confidence intervals into our robustness assessment ensures that findings are not only based on the most likely outcomes but also consider the variability and uncertainty inherent in the tokenomics environment. Apart from considering confidence intervals for assessing model stability, we also utilize them to facilitate strategic decision-making, as to determine the probability for a Model to reach a minimum benchmark. *Table 7* shows the 90% Confidence Intervals for the Customer Retention Metrics and the respective probabilities for achieving a positive retention rate.

*Table 7: Confidence Intervals for Retention Metrics across all Models in their default configurations.*

| <i>Confidence Intervals for Retention Metrics</i> |                           |          |         |         |         |
|---------------------------------------------------|---------------------------|----------|---------|---------|---------|
| Retention Metric                                  |                           | Baseline | Model 1 | Model 2 | Model 3 |
| Mean                                              | $\mu$                     | 0.0835   | 0.0969  | 0.1332  | 0.1224  |
| Purchasing                                        | 90% CI Lower Bound        | -0.0047  | 0.0036  | -0.0073 | 0.0196  |
| Frequency                                         | 90% CI Higher Bound       | 0.1717   | 0.1902  | 0.2737  | 0.2252  |
| Growth                                            | Probability ( $\mu > 0$ ) | 0.9452   | 0.9531  | 0.9453  | 0.9632  |
|                                                   |                           |          |         |         |         |
|                                                   | $\mu$                     | 0.5226   | 0.4569  | 0.4163  | 0.5025  |
| Mean Spend                                        | 90% CI Lower Bound        | 0.3404   | 0.3534  | 0.3173  | 0.3687  |
| Growth                                            | 90% CI Higher Bound       | 0.7047   | 0.5605  | 0.5154  | 0.6362  |
|                                                   | Probability ( $\mu > 0$ ) | 0.9930   | 0.9970  | 0.9967  | 0.9959  |

Discussion

The comprehensive analysis of the three tokenomics models within a multi-brand loyalty program has yielded insightful results. Each model demonstrated a distinct growth pattern,

underscoring the critical importance of model design in meeting specific business objectives. Model 2, with its innovative bonding curve mechanism, stood out for its exceptional performance in leveraging purchase incentives, reflected in its steep growth curves. This model effectively harnessed the speculative aspects of tokenomics, driving consumer engagement and investment. Conversely, Model 3, despite its promising start facilitated by sidechain technology, eventually lagged behind Model 2, highlighting the dynamic nature of market responses to different tokenomics structures. Model 1, with its modest yet consistent performance, illustrates the effectiveness of even basic tokenomics principles in loyalty programs.

Theoretically, this study significantly contributes to the burgeoning field of blockchain technology in loyalty programs. It extends the current understanding of how various tokenomics models can be strategically deployed to enhance customer engagement and loyalty. Practically, the findings offer valuable insights for businesses contemplating the integration of blockchain technology into their loyalty strategies. The distinct performances of the models serve as a guide for companies to design their loyalty programs in alignment with their specific goals and customer base.

The results highlight the potential of tokenomics to transform customer loyalty landscapes. Businesses can leverage these models to create more engaging, rewarding, and interactive loyalty programs. The success of Model 2, in particular, illustrates how innovative tokenomics designs can foster a more dynamic and engaging customer experience, potentially leading to increased customer retention and spending. The study also reveals the importance of balancing the initial attractiveness of loyalty programs with their long-term sustainability, as demonstrated by the varying performances of the models over the 12-month simulation period.

However, the study also reveals that performance gains come at the cost of complexity and increased sensitivity to the dynamics of the External Context. While Model 2 under default conditions has the highest likelihood to achieve the highest transactional volume and customer and growth, its bonding curve mechanism requires careful adjustment to expected agent specificities. Additionally, any parameter changes to the systems rule design should be reviewed for compatibility with the dynamics of Model 2.

Despite potentially higher returns users might favour to join a leaner system with more predictable mechanism. It is thus indispensable to mitigate the performance-complexity trade-off by providing a clear, consistent, and transparent communication strategy towards the systems participants. Wallet Information, Gamification, Rules, and Token Mechanisms must be conveyed in a concise, centralized, and engaging manner since the user's onboarding.

System Equity is key to attract a diverse range of partner companies to the MCLP. Results indicate that tokenomics models compared to the baseline generally reduce equity because a higher leverage of customer incentives on spending increases disparities. Generally, we observe that greater speculative components and more sophistication increase the disparity among partner companies. Nevertheless, the relative differences are marginal and could be offset by smart contracts enforcing algorithmic mechanisms to facilitate a fairer distribution of growth and returns among partner companies. Furthermore, our scenario analysis reveals that the criteria set for partner selection should sensibly set by Celfocus. Partner companies should be selected to form balanced constellations, in terms of industry representation, size, and purchasing frequencies. Especially high degrees of dispersity between the set of partner companies can significantly reduce system equity. High industry concentrations among the partner companies prove to have the same negative effect.

*Table 8* presents a scorecard comparing the identified characteristics of the models across four dimensions. Model 2 performs best in terms of bolstering transactional value for the partner companies.

Regarding customer value, Model 2 leads the way because of its leverage on purchasing incentives due to its volatile nature and its utility enriched by its open trading gateways. Enabling its users to exchange their partner token for central token and vice-versa Model 3 also offers significant customer utility by enabling users to exchange partner tokens for a central token and vice versa. To mitigate potential issues like arbitrage and the risk of partner-token run-offs, Model 3 employs smart-contract-enforced mechanisms. These mechanisms are designed to adjust the conversion rates between partner tokens and the central token. This adjustment ensures a stable value-to-value conversion, in scenarios where the value of the central token experiences fluctuations. While this stabilizing mechanism is beneficial for maintaining value consistency upon exchange, it does inherently reduce the incentives for speculation in Model 3 when compared to Model 2. This aspect of Model 3 ensures a more stable but potentially less speculative investment environment for users.

The dimension of resilience draws a different picture across the Models. Model 1 given its token stability, private deployment environment, and more limited features offers the greatest benefits in terms of resilience. On the other hand, Model 2 reacts most sensitively to fluctuations in the External Context, and changes in rule design. Ensuring Model 2's stability thus requires a bonding curve thoughtfully tailored to the most likely scenarios and chosen tokenomics configuration. Moreover, Model 2 calls for a strong monitoring capability to counter-act potential shocks. Nevertheless, with appropriate risk-management mechanisms put in place

Model 2 yields the highest gains and growth potential for participants.

Finally, the degree of Customization is a pivotal consideration for partner companies seeking to strategically leverage higher returns within the MCLP. With its customizable sidechain and partner-token issuance, Model 3 provides most space for customization. Model 2 follows up as it allows partner companies to tailor the amount of staked token, trading, and replenishment-decisions to their commercial strategies and desired commitment to the MCLP.

The choice and configuration of the tokenomics system depends on the Celfocus's strategic preferences and system design capabilities.

Overall, this study offers a foundational understanding of how different tokenomics models can be utilized in loyalty programs, paving the way for more innovative and effective customer engagement strategies in the digital era. The findings underscore the need for businesses to carefully consider their choice of tokenomics model, aligning it with their specific objectives and market dynamics to maximize the benefits of their loyalty programs.

Table 8: Multidimensional Scorecard of Tokenomics Models. (High = 3; Moderate = 2; Low = 1)

| Dimension      | Feature                               | Model 1  | Model 2  | Model 3  |
|----------------|---------------------------------------|----------|----------|----------|
| Partner Value  | Sales Impact                          | Moderate | High     | High     |
|                | Sales Growth Rate                     | Moderate | High     | Moderate |
|                | Scalability Potential                 | Moderate | High     | High     |
| Customer Value | Model-intrinsic Customer Incentives   | Low      | High     | Moderate |
|                | Customer Utility                      | Moderate | High     | Moderate |
|                | Speculative Component                 | Low      | High     | Moderate |
| Resilience     | Token Stability                       | High     | Low      | Moderate |
|                | Simplicity                            | High     | Low      | Moderate |
|                | System Stability                      | High     | Low      | Moderate |
| Customization  | Customizability for Partner Companies | Low      | Moderate | High     |
| Scorecard      | Partner Value                         | 6        | 9        | 8        |
|                | Customer Value                        | 4        | 9        | 6        |
|                | Resilience                            | 9        | 3        | 6        |
|                | Customization                         | 1        | 2        | 3        |
|                | Total                                 | 20       | 23       | 23       |

## **Future work**

This study, while primarily theoretical, has not delved into the nuances of price structures and customer behaviours prevalent in the market. Future research can aim to bridge this gap by conducting an in-depth market analysis. This analysis could focus on understanding the demographic distribution of potential customers, particularly emphasizing the factors they consider most crucial in their decision-making processes.

Another pivotal aspect that warrants further exploration is the perception of crypto assets among certain consumer segments. There is a noticeable apprehension towards crypto assets within a specific group of potential customers. Investigating the distribution and sentiments of this group within the larger customer base is crucial for a comprehensive understanding of market dynamics.

Moreover, the expectations of companies aiming to thrive in such an ecosystem merit attention. Future studies should investigate not just the customer perspective, but also the corporate viewpoint, particularly in the context of blockchain-based loyalty programs. Understanding the symbiotic relationships between companies and how they envision coexisting in this ecosystem is essential.

Lastly, our study has focused on the performance of loyalty programs from a tokenomics perspective. However, there remains a significant area of research to be explored regarding the practical implementation of these programs. When our developed model was applied to real-world scenarios with specific assumptions, some variables were not included. Future research could explore how seasonal variations impact the model's performance. Enhancing the model by incorporating additional parameters could potentially improve the precision of the outcomes.

Future researchers should delve into the specifics of how these loyalty programs can be effectively implemented in real-world scenarios, including the selection of appropriate platforms for their deployment.

## **Conclusions**

The in-depth analysis of the four tokenomics models has provided a detailed insight into their performance within a multi-brand loyalty program. Overall, all models have demonstrated a positive growth trend in key metrics over the simulated 12 months, compared to the baseline model. However, significant differences between the models highlight the importance of careful design to achieve specific objectives. Model 2, characterized by the presence of a bonding curve, exhibited the steepest growth curves, effectively leveraging purchase incentives. On the other hand, Model 3, utilizing sidechain technology, started with higher metrics but was surpassed by Model 2 after four months. As expected, the first model showed the most modest growth, but still performed better than the baseline model. These results can be attributed to the speculative component of the second model, which provides a greater incentive for consumers. Model 2 is structured to provide tangible incentives to partner businesses. Through the acquisition of a minimum quantity of tokens at a fixed price from the reserve, companies can participate in the program and benefit from various management options. These options include the ability to keep tokens in circulation or stake them to earn rewards through the PoS validation mechanism. PoS validation and validator selection based on weighted metrics ensure fair participation and give partner companies an active role in program governance. The ability to maintain an elevated level of engagement and consumer retention is emphasized by the incorporation of gamification elements in the models. The introduction of monthly quests and the creation of premium tier levels with significant discounts offer an engaging experience to consumers. Through the assignment of badges and the encouragement to complete periodic

activities, consumers are entertained and motivated to actively participate in the loyalty program. Regarding the provision of benefits to consumers, the models implement a flexible system for earning and using tokens. Consumers can earn tokens through purchases and completing quests, and subsequently use them to obtain discounts, rewards, or convert them into the common currency of the program. This flexibility gives consumers the freedom to choose how they want to enjoy the benefits of the loyalty program, thereby incentivizing their continued participation and loyalty.

In conclusion, every tokenomics model studied prove effective in creating a loyalty ecosystem that promotes a mutually beneficial collaboration between partner businesses and consumers. However, as it can be seen by the comparison of the second and the third model, the choice of the model should be guided by specific business objectives, carefully considering the trade-off between incentivizing purchases, and ensuring long-term sustainability.

## References

- a Literature Review of Empirical Studies on Gamification. 2014 47th Hawaii International Conference on System Sciences, 3025–3034. <https://doi.org/10.1109/hicss.2014.377>
- Akcin, O., Streit, R.P., Oommen, B., Vishawanath, S., Chinchali, S. (2022). A Control Theoretic Approach to Infrastructure-Centric Blockchain Tokenomics. Cornell University.
- Alsalamah, H. A., Nasser, S., Alsalamah, S., Almohana, A. I., Alanazi, A., & Alrrshaid, F. (2021). Wholesome Coin: A pHealth Solution to Reduce High Obesity Rates in Gulf Cooperation Council Countries Using Cryptocurrency. *Frontiers in Blockchain*, 4. <https://doi.org/10.3389/fbloc.2021.654539>
- Au, S., & Power, T. (2018). *Tokenomics: The crypto shift of blockchains, ICOs, and tokens*. Packt Publishing Ltd.
- Azhari, A. (2019). Gamification Framework: The Contribution of User Centered Design, Social Media Applications, Gaming and Psychology Concepts and Frameworks. *Lecture Notes in Computer Science*, 381–390. [https://doi.org/10.1007/978-3-030-22602-2\\_28](https://doi.org/10.1007/978-3-030-22602-2_28)
- Barreiro-Gomez, J., Tembine, H. (2016). Blockchain Token Economics: A Mean-Field-Type Game Perspective. *IEEE Access*.
- Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials*, 21(4), 3796-3838.



and the self-determination of behavior. *Psychological Inquiry*, 11(4), 227–268.

[https://doi.org/10.1207/S15327965PLI1104\\_01](https://doi.org/10.1207/S15327965PLI1104_01)

- Deci, E. L., Vallerand, R. J., Pelletier, L. G., & Ryan, R. M. (1991). Motivation and Education: The Self-Determination Perspective. *Educational Psychologist*, 26(3-4), 325–346.

<https://doi.org/10.1080/00461520.1991.9653137>

- DEL DATO, T. R. A. T. T. A. M. E. N. T. O. PROCESSI DECISIONALI E TRATTAMENTO DEI DATI.

- Delgado Fernandez, J., Barbereu, T., & Papagerogiou, O. (2022). Agent-based Model of Initial Token Allocations: Evaluating Wealth and Concentration in Fair Launches.

- Deterding, S., Dixon, D., Khaled, R., & Nacke, L. E. (2011). From game design elements to gamefulness. *From Game Design Elements to Gamefulness: Defining Gamification*.

<https://doi.org/10.1145/2181037.2181040>

-Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.

<https://bitcoin.org/bitcoin.pdf>

- Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, 19(5), 92-95.

- Dorotic, M., Bijmolt, T. H., & Verhoef, P. C. (2012). Loyalty programmes: Current knowledge and research directions. *International Journal of Management Reviews*, 14(3), 217-237.

- Dragulescu, A., Yakovenko, V.M. (2000).Statistical mechanics of money. *The European Physical Journal B – Condensed Matter and Complex Systems*, 17, 723-729.

- Dutta, R., Das, A., Dey, A., & Bhattacharya, S. (2020). Blockchain vs GDPR in collaborative data governance. In *Cooperative Design, Visualization, and Engineering: 17th International Conference, CDVE 2020, Bangkok, Thailand, October 25–28, 2020, Proceedings 17* (pp. 81-92). Springer International Publishing.

- Eyal, I., & Sirer, E. G. (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. *arXiv* (Cornell University). <https://doi.org/10.48550/arxiv.1311.0243>

- Freni, P., Ferro, E., & Moncada, R. (2022). Tokenomics and blockchain tokens: A design-oriented morphological framework. *Blockchain: Research and Applications*.

- Gabe Zichermann. (2011). *Gamification by Design*. O'reilly Media.

- Gamification Market Size US\$ 96.8 Billion by 2030. (n.d.). [www.precedenceresearch.com](http://www.precedenceresearch.com). <https://www.precedenceresearch.com/gamification-market/The-global-gamification-market-size>

- Giannopoulou, A. (2020, June). Data protection compliance challenges for self-sovereign

identity. In International Congress on Blockchain and Applications (pp. 91-100). Cham: Springer International Publishing.

- Gupta, S. S. (2017). Blockchain. IBM Onlone ([http://www. IBM. COM](http://www.ibm.com)).

- Gürcan, Ö. (2020). On using agent-based modeling and simulation for studying blockchain systems. Journées Francophones de la Modélisation et de la Simulation.

- Hacura, A., Jadamus-Hacura, M., & Kocot, A. (2011). Risk analysis in investment appraisal based on the Monte Carlo simulation technique. The European Physical Journal B

-Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does Gamification Work?

-Hammedi, W., Leclercq, T., & Poncin, I. (2019). Customer engagement: the role of gamification. Handbook of Research on Customer Engagement, 164–185.  
<https://doi.org/10.4337/9781788114899.00014>

- Hammersley, J., & Handscomb, D. C. (1964). Monte Carlo Methods. London: Chapman and Hall Ltd.

- Han, R., Yan, Z., Liang, X., & Yang, L. T. (2022). How Can Incentive Mechanisms and Blockchain Benefit with Each Other? A Survey. ACM Computing Surveys.  
<https://doi.org/10.1145/3539604>

- Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), e2060.

- Hofman-Kohlmeyer, M. (2016, September). Customer loyalty program as a tool of customer retention: literature review. In CBU International Conference Proceedings (Vol. 4, pp. 199-203).

- Huang, W.H.-Y. and Soman, D. (2013) Gamification of Education. Research Report Series: Behavioural Economics in Action. Rotman School of Management, University of Toronto.

-Catalini, Christian and Gans, Joshua S., Some Simple Economics of the Blockchain (April 20, 2019). Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16, Available at SSRN: <https://ssrn.com/abstract=2874598> or <http://dx.doi.org/10.2139/ssrn.2874598>

- Huotari, K., & Hamari, J. (2012). Defining Gamification: A Service Marketing Perspective. In Proceeding of the 16th International Academic MindTrek Conference (pp. 17-22). New York, NY: ACM.

- Hwang, Y.-S., & Choi, Y. K. (2019). Higher education service quality and student

satisfaction, institutional image, and behavioral intention. *Social Behavior and Personality: An International Journal*, 47(2), 1–12. <https://doi.org/10.2224/sbp.7622>

- Information Commissioner's Office, UK, (2022) The General Data Protection Regulation, Key Definitions, What is personal data?, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data-1-0.pdf>

- Information Commissioner's Office, UK, (2023) Right to data portability, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>.

- Introduction to gamification. (2014). Association For Project M.

- Jakobsson, M., & Juels, A. (1999, September). Proofs of work and bread pudding protocols. In *Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99)* September 20–21, 1999, Leuven, Belgium (pp. 258–272). Boston, MA: Springer US. Zetsche, D. A., Buckley, R. P., Arner, D. W., & Fohr, L. (2019). The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators. *Harv. Int'l LJ*, 60, 267.

- Jie Xu, Cong Wang, and Xiaohua Jia. 2023. A Survey of Blockchain Consensus Protocols. *ACM Comput. Surv.* 55, 13s, Article 278 (December 2023), 35 pages. <https://doi.org/10.1145/3579845>

- justice/article-29/documentation/opinion-recommendation/files/2014/wp216\_en.pdf

-Grand View Research. (2020, May). Video Game Market Size, Share | Industry Report, 2020-2027. [www.grandviewresearch.com](https://www.grandviewresearch.com/industry-analysis/video-game-market). <https://www.grandviewresearch.com/industry-analysis/video-game-market>

- Kampakis, S. (2018). Three Case Studies of Tokenomics. *The Journal of The British Blockchain Association*.

- Kampakis, S. (2022). Auditing Tokenomics: A Case Study and Lessons from Auditing a Stablecoin Project. *The Journal of The British Blockchain Association*.

- Kampakis, S., & Stankevicius, L. (2023). The Tokenomics Audit Checklist: Presentation and Examples from the Audit of a DeFi project, Terra/Luna and Ethereum 2.0. *The Journal of The British Blockchain Association*.

- Komiya, K., Nakajima, T. (2019). Increasing Motivation for Playing Blockchain Games Using Proof-of-Achievement Algorithm. In: Fang, X. (eds) *HCI in Games. HCII 2019. Lecture Notes in Computer Science()*, vol 11595. Springer, Cham. [https://doi.org/10.1007/978-3-030-22602-2\\_11](https://doi.org/10.1007/978-3-030-22602-2_11)

- Letychevskyi, O. (2022). Creation of a Self-Sustaining Token Economy. The Journal of The British Blockchain Association.
- Liu, Y., Tsyvinski, A. (2021). Risks and Returns of Cryptocurrency. The Review of Financial Studies 34, 1105-1155.
- Magatef, S. G., & Tomalieh, E. F. (2015). The impact of customer loyalty programs on customer retention. International Journal of Business and Social Science, 6(8), 78-93.
- Martins Bratuskins @Monetizr. (2018, April 19). Four ways game reward systems boost loyalty... and sales. Medium; Monetizr. <https://medium.com/monetizr/four-ways-game-reward-systems-boost-loyalty-and-sales-ec0362c986c7>
- McMillan, D. W., & Chavis, D. M. (1986). Sense of community: A definition and theory. Journal of community psychology, 14(1), 6-23.
- Meyer-Waarden, L., & Benavent, C. (2009). Grocery retail loyalty program effects: self-selection or purchase behavior change?. Journal of the Academy of Marketing Science, 37, 345-358.
- Meyer-Waarden, L., Benavent, C., & Castéran, H. (2013). The effects of purchase orientations on perceived loyalty programmes' benefits and loyalty. International Journal of Retail & Distribution Management, 41(3), 201–225.  
<https://doi.org/10.1108/09590551311306255>
- Mitchell, N., Danino, N., May, L.: Motivation and manipulation: a gamification approach to influencing undergraduate attitudes in computing. In: European Conference on Games Based Learning. Academic Conferences International Limited (2013)
- Molina, F., Betarte, G., & Luna, C. (2021, May). Design principles for constructing GDPR-compliant blockchain solutions. In 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) (pp. 1-8). IEEE.
- Montero, V., Bradlow, E., & Fader, P. (2012). Latent Redemption Thresholds in Linear Loyalty Programs. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.2142482>
- Mouna Denden, Abed, M., Holotescu, V., Tlili, A., Holotescu, C., & Grosseck, G. (2023). Down to the Rabbit Hole: How Gamification is Integrated in Blockchain Systems? A Systematic Literature Review. International Journal of Human-Computer Interaction, 1–15.  
<https://doi.org/10.1080/10447318.2023.2238973>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

- Neudecker, T., & Hartenstein, H. (2018). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials*, 21(1), 838-857.
- Palma, S., Tamburri, D., Pareschi, R., Cerrone, C., & van den Heuvel, W.-J. (2018). Business-Savvy Blockchains with Gamification: A Framework for Collaborative Problem Solving. *EAI Endorsed Transactions on Game-Based Learning*, 5(16), 155567.  
<https://doi.org/10.4108/eai.13-7-2018.155567>
- Paulavicius, R., Grigaitis, S., & Filatovas, E. (2021). A Systematic Review and Analysis of Blockchain Simulators. *IEEE*.
- Paulavicius, R., Grigaitis, S., & Filatovas. (2021). An Overview and Current Status of Blockchain Simulators. *European Union*.
- Pham, M. T., & Avnet, T. (2004). Ideals and oughts and the reliance on affect versus substance in persuasion. *Journal of consumer research*, 30(4), 503-518.
- Preneel, B. (1994). Cryptographic hash functions. *European Transactions on Telecommunications*, 5(4), 431-448.
- Robson, K., Plangger, K., Kietzmann, J. H., McCarthy, I., & Pitt, L. (2016). Game on: Engaging customers and employees through gamification. *Business Horizons*, 59(1), 29–36.  
<https://doi.org/10.1016/j.bushor.2015.08.002>
- Rosenbaum, M. S., Ostrom, A. L., & Kuntze, R. (2005). Loyalty programs and a sense of community. *Journal of Services Marketing*, 19(4), 222-233.
- Sadykhov, R., Goodell, G., De Montigny, D., Schoerning, M., Treleaven, P. (2023, November). Decentralized token economy theory (DeTEcT): token pricing, stability and governance for token economies. *Front. Blockchain* 6:1298330.
- Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of financial studies*, 34(3), 1156-1190.

- Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). Layer 2 blockchain scaling: A survey. arXiv preprint arXiv:2107.10881.
- sharpcorner.com/article/do-you-need-a-blockchain2/.
- Sheth, H., & Dattani, J. (2019). Overview of blockchain technology. Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146.
- Shugan, S. M. (2005). Brand Loyalty Programs: Are They Shams? Marketing Science, 24(2), 185–193. <https://doi.org/10.1287/mksc.1050.0124>
- Sim, W. L., Chua, H. N., & Tahir, M. (2019, November). Blockchain for identity management: The implications to personal data protection. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 30-35). IEEE.
- Smith, M. S. (2022, August 10). The Spectacular Collapse of Cryptokitties, the First Big Blockchain Game. IEEE Spectrum. <https://spectrum.ieee.org/cryptokitties>
- Somin, S., Gordon, G., Altshuler, Y. (2018). Network Anaysis of ERC20 Tokens Trading on Ethereum Blockchain. *International Conference on Complex Systems*, 439-450.
- Sutopo, A. H. (2023). Blockchain Programming Smart Contract on Polygon. Topazart.
- Hamari, J., & Lehdonvirta, V. (2010). Game Design as Marketing: How Game Mechanics Create Demand for Virtual Goods. INTERNATIONAL JOURNAL OF BUSINESS

SCIENCE AND APPLIED MANAGEMENT, 5(1), 14-29.

- Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 6(2), 147-156.

- Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy*, 42, 91-107.

- Wang, L., Luo, X. (Robert), & Lee, F. (2019). Unveiling the interplay between blockchain and loyalty program participation: A qualitative approach based on Bubichain. *International Journal of Information Management*, 49, 397–410.  
<https://doi.org/10.1016/j.ijinfomgt.2019.08.001>

- Wang, L., Luo, X. R., & Xue, B. (2018). Too good to be true? understanding how blockchain revolutionizes loyalty programs.

- Wang, Y., Han, J.H. and Beynon-Davies, P. (2019), "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda", *Supply Chain Management*, Vol. 24 No. 1, pp. 62-84. <https://doi.org/10.1108/SCM-03-2018-0148>

- Wright, S. A. (2023, March). Why Decentralize Deep Learning? In 2023 IEEE 15th International Symposium on Autonomous Decentralized System (ISADS) (pp. 1-6). IEEE.

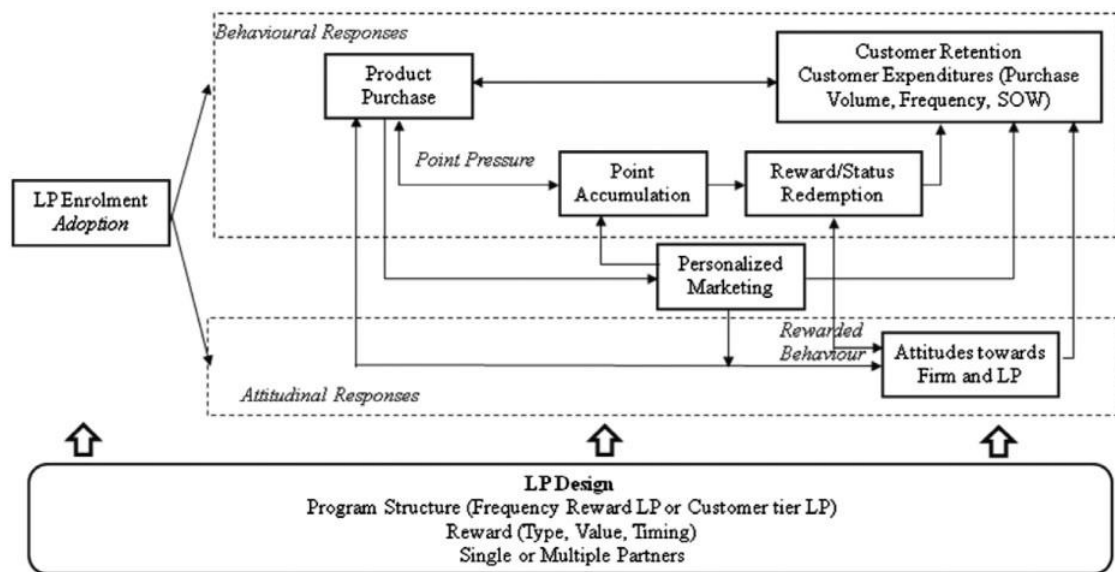
- Xu, F., Buhalis, D., & Weber, J. (2017). Serious games and the gamification of tourism. *Tourism Management*, 60, 244–256. <https://doi.org/10.1016/j.tourman.2016.11.020>

- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Panoramica della tecnologia Blockchain. arXiv preprint arXiv:1906.11078 .

- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, 11(10), e0163477.

- Zhang, X., Jian, Y., Li, X., Ma, L., Karanis, G., & Karanis, P. (2018). The first report of *Cryptosporidium* spp. in *Microtus fuscus* (Qinghai vole) and *Ochotona curzoniae* (wild plateau pika) in the Qinghai-Tibetan Plateau area, China. *Parasitology research*, 117, 1401-1407.

## Appendix



Source: (based on Blattberget al.2008)

Fig. 1: Loyalty Programmers: An Overview

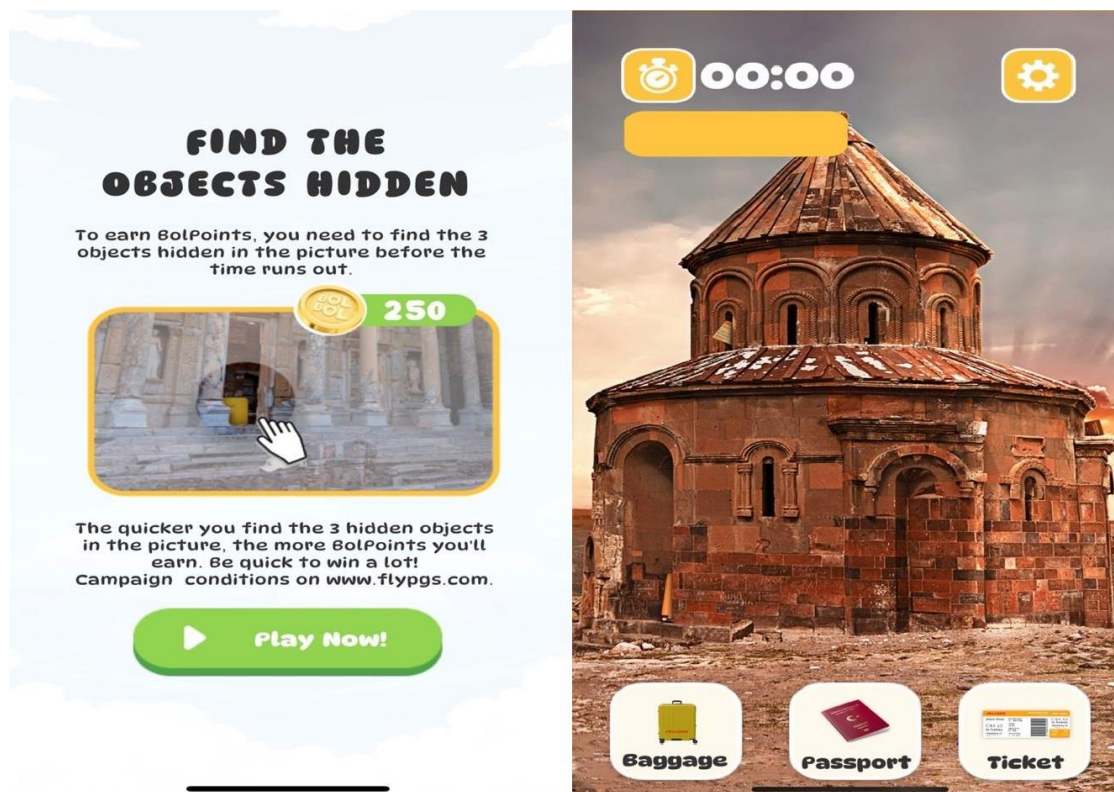


Fig. 2-3: Gamification Features on Pegasus Airlines Loyalty Program  
Screenshot of the Pegasus Airlines app showing the hidden object game.  
Source: Pegasus Airlines app 2023.



Fig. 4-5: Screenshot of the Pingo Doce App showing the game designed only for Christmas.  
Source: O Meu Pingo Doce App 2023

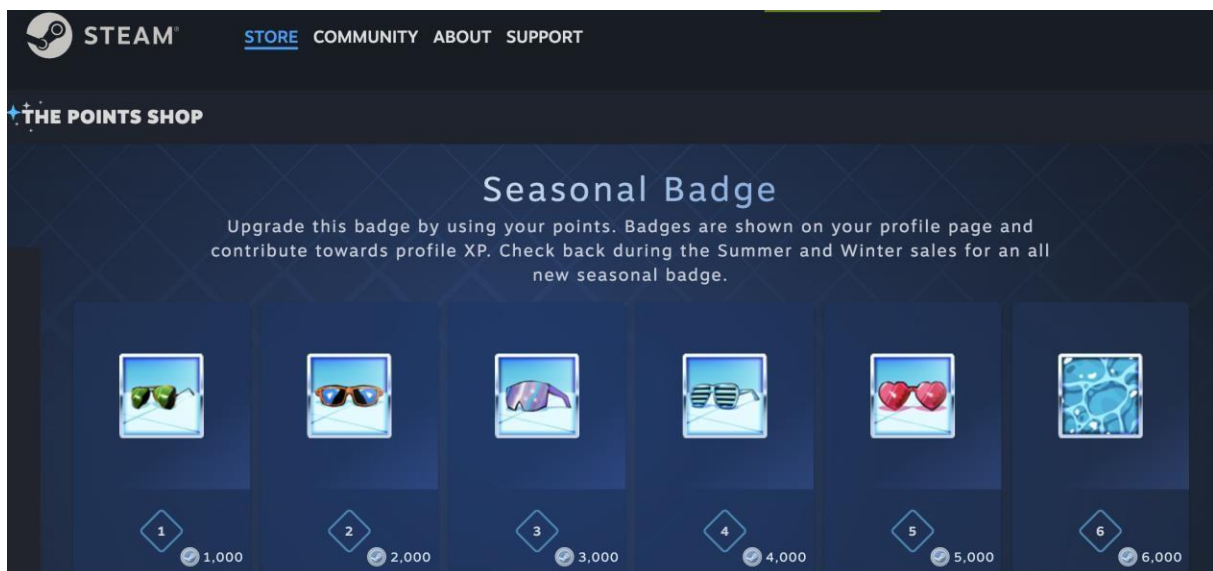


Fig 6: Badge and Point System on Steam Points Shop  
Source: <https://store.steampowered.com/points/shop/c/games>

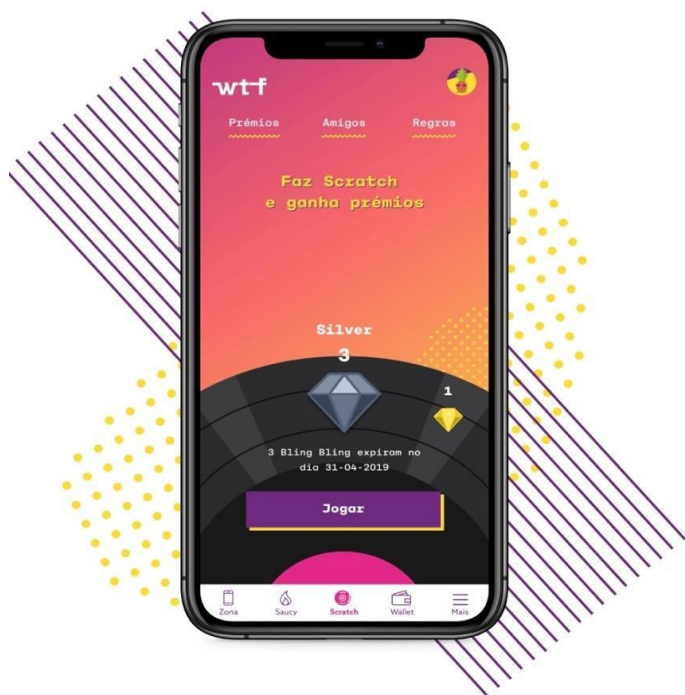


Fig. 7: Screenshot from WTF Reward Game “Scratch”  
Source: WTF app 2023

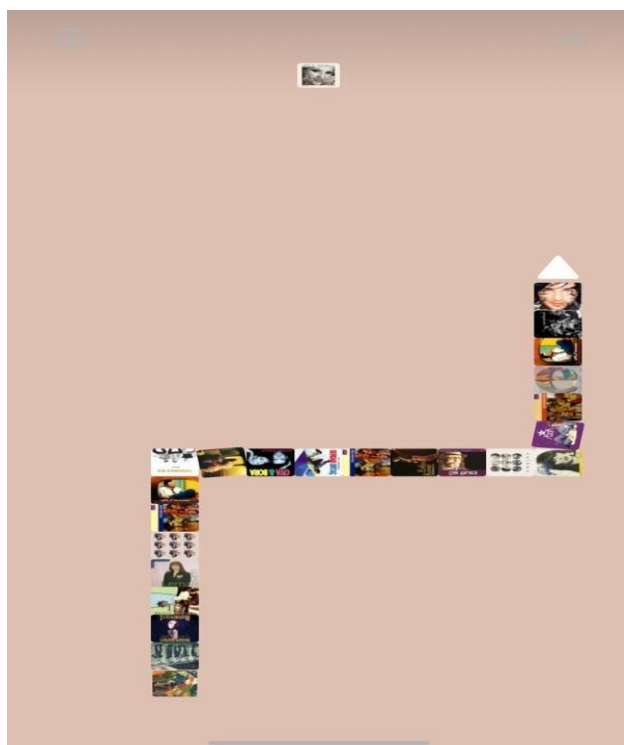


Fig. 8: Screenshot showing the Snake Game on Spotify  
Source: Spotify app

|                                     | Simple & Stable (Model 1)                                                                                                                                                                                                                                   | Open & Speculative (Model 2)                                                                                                                                                                                                                                                                                               | Sidechain Model (Model 3)                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Supply</b>                       | <ul style="list-style-type: none"> <li>Unlimited &amp; Dynamic Supply according to the demand and volume of transactions. A tokens circulation end upon redemption.</li> </ul>                                                                              | <ul style="list-style-type: none"> <li>Limited pre-minted supply; smart contract. Only the circulating supply determines token value through the bonding curve. Token flow from customer to partner wallet upon redemption.</li> </ul>                                                                                     | <ul style="list-style-type: none"> <li>Unlimited supply for both sidechain and ledger coins</li> <li>Hybrid Blockchain</li> </ul>                                                                                                                                                                                                                                         |
| <b>Incentive &amp; Gamification</b> | <ul style="list-style-type: none"> <li>Tiers: Higher conversion rates for high-rank tiers.</li> <li>Leader board rewards</li> <li>Monthly Spending Quest: Earn token reward upon completion</li> </ul>                                                      | <ul style="list-style-type: none"> <li>Tiers: Higher conversion rates for high-rank tiers.</li> <li>Monthly Spending Quest: Earn token reward upon completion</li> <li>Leader board rewards</li> <li>Speculation on token appreciation</li> </ul>                                                                          | <ul style="list-style-type: none"> <li>Tiers: Higher conversion rates for high-rank tiers.</li> <li>Monthly Spending Quest: Earn token reward upon completion</li> <li>Incentive to be loyal to issuing partner companies, due to more favourable conversion rates compared to the Central token</li> <li>Speculation on the appreciation of the Central token</li> </ul> |
| <b>Token value</b>                  | <ul style="list-style-type: none"> <li>Stable – Constant Value</li> </ul>                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>Controlled-Volatile root-shaped Bonding curve.</li> </ul>                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>Constant Value determined beforehand among partners</li> </ul>                                                                                                                                                                                                                                                                     |
| <b>Validation System</b>            | <ul style="list-style-type: none"> <li>Validation carried out by regulator</li> </ul>                                                                                                                                                                       | <ul style="list-style-type: none"> <li>Pos validation carried out by partners</li> <li>Composite KPI determines chances for validator selection</li> </ul>                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Ourboros PoS validation</li> <li>SPV(Simplified Payment Verification) system</li> </ul>                                                                                                                                                                                                                                            |
| <b>Token Issuance</b>               | <ul style="list-style-type: none"> <li>Tier dependent Issuance rate</li> </ul>                                                                                                                                                                              | <ul style="list-style-type: none"> <li>Tier dependent Issuance rate, adapting dynamically to the current token value to maintain a stable value-to-value (utility) rate.</li> </ul>                                                                                                                                        | <ul style="list-style-type: none"> <li>Companies are responsible for issuing their own coins.</li> </ul>                                                                                                                                                                                                                                                                  |
| <b>Conversion Rate</b>              | <ul style="list-style-type: none"> <li>Conversion rate is different among tiers</li> </ul>                                                                                                                                                                  | <ul style="list-style-type: none"> <li>Token Conversion Rate is volatile, based on demand &amp; supply, determined by the bonding curve</li> </ul>                                                                                                                                                                         | <ul style="list-style-type: none"> <li>Conversion rate is fixed among companies by smart contracts.</li> </ul>                                                                                                                                                                                                                                                            |
| <b>Redemption &amp; Cash Out</b>    | <ul style="list-style-type: none"> <li>Redemption at partner companies at the fixed conversion rate.</li> <li>Upon redemption, tokens flow from the customer wallet into the company wallet</li> <li>Enable cash-out only by paying a commission</li> </ul> | <ul style="list-style-type: none"> <li>Redemption at partner companies at the current conversion rate.</li> <li>Upon redemption token flow from the customer wallet into the company wallet</li> <li>Enables customers to cash-out through trading</li> <li>Partner companies can further sell back their token</li> </ul> | <ul style="list-style-type: none"> <li>Partner token can only be redeemed at issuing partner company</li> <li>Redemption at partner companies at the fixed conversion rate.</li> </ul>                                                                                                                                                                                    |
| <b>Entry</b>                        | <ul style="list-style-type: none"> <li>Approval through decentralized majority voting</li> </ul>                                                                                                                                                            | <ul style="list-style-type: none"> <li>Approval through decentralized majority voting</li> <li>Buy-in</li> </ul>                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>Approval through decentralized majority voting</li> <li>Agree on partner token conversion rates</li> </ul>                                                                                                                                                                                                                         |
| <b>Partner Cost-Benefit</b>         | <ul style="list-style-type: none"> <li><b>Sales Impact</b></li> <li><b>Transaction Fees</b></li> </ul>                                                                                                                                                      | <ul style="list-style-type: none"> <li>Hold Token as means of investment</li> <li>Pos Rewards</li> <li><b>Sales Impact</b></li> <li>Buy-in for participation (staking)</li> <li><b>Transaction Fees</b></li> </ul>                                                                                                         | <ul style="list-style-type: none"> <li>Compares store customer data internally and protect themselves against malicious attacks.</li> <li><b>Sales Impact</b></li> <li><b>Increased Brand Loyalty</b></li> <li><b>Transaction Fees</b></li> </ul>                                                                                                                         |

Table 2: Comparison table of the three models

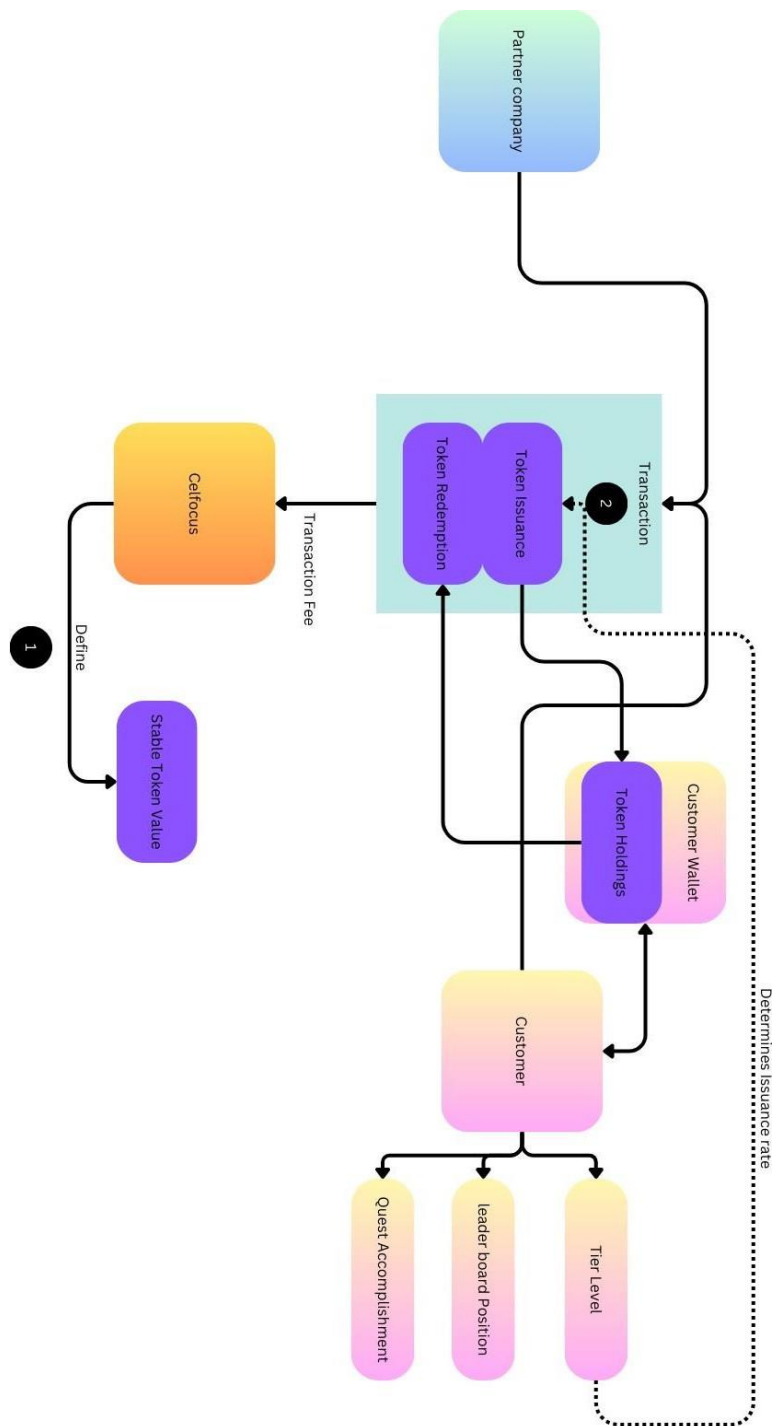


Fig. 25: Stakeholder-Interaction Map for Tokenomics Model 1

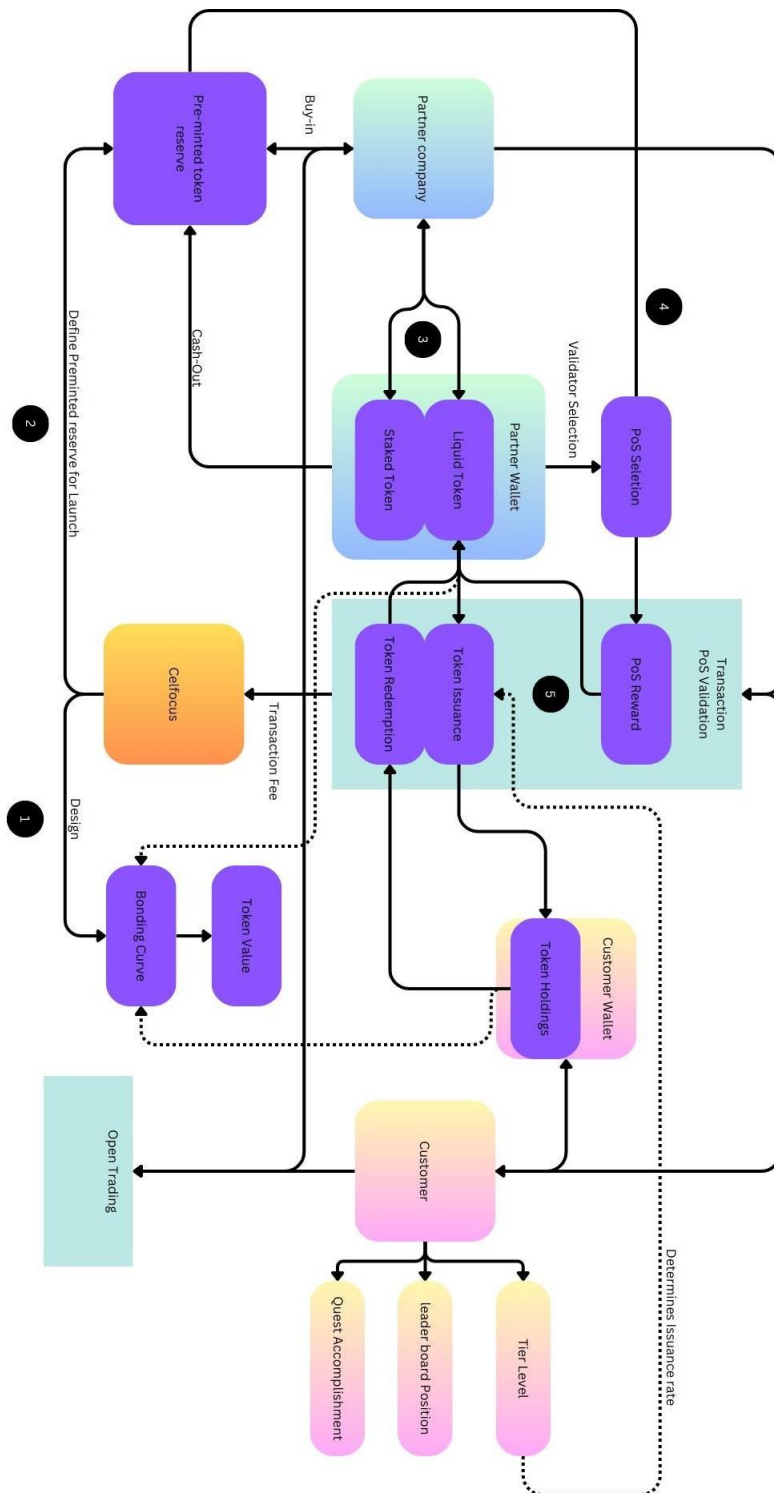


Fig. 26: Stakeholder-Interaction Map for Tokenomics Model 2

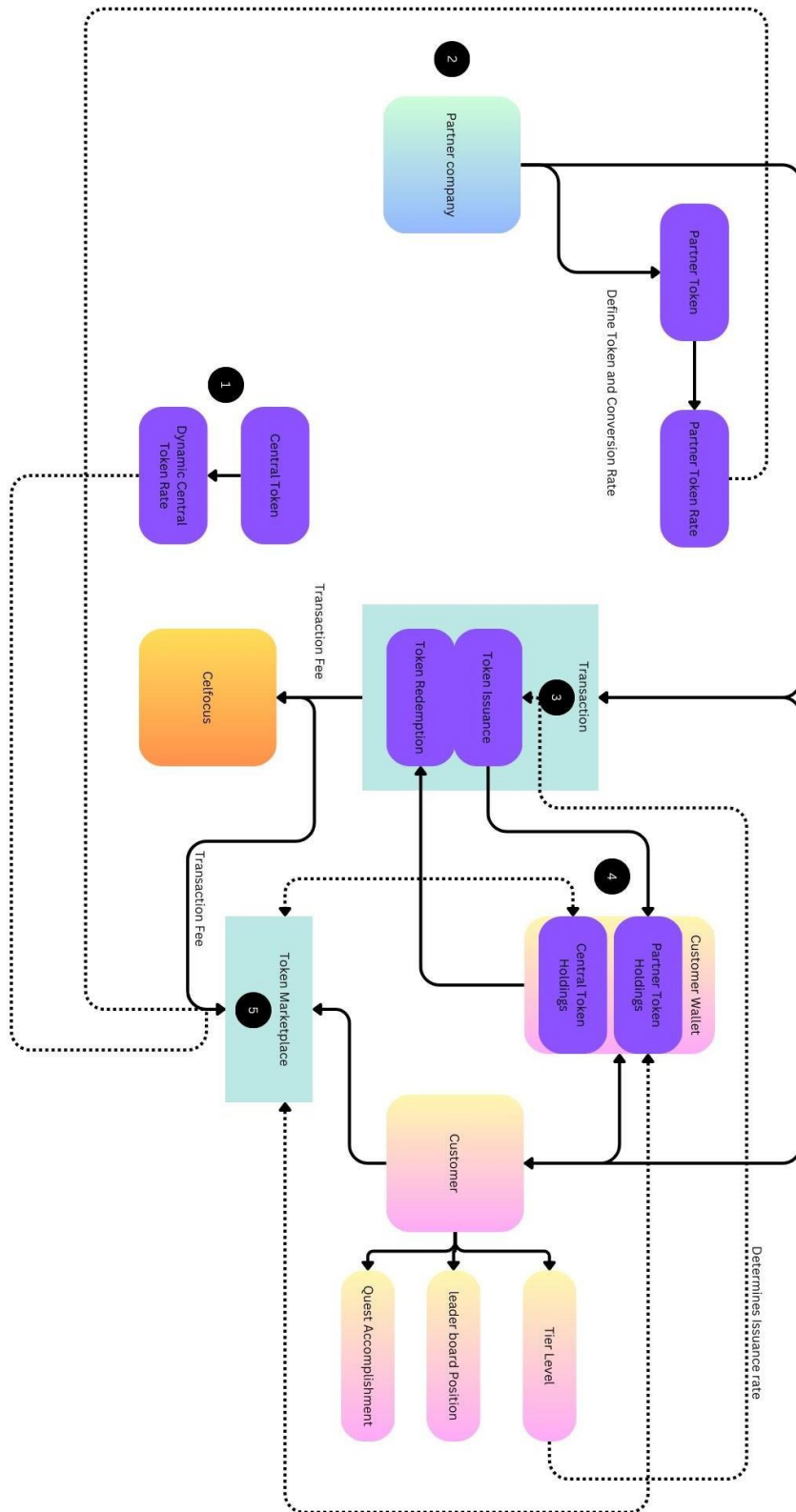


Fig. 27: Stakeholder-Interaction Map for Tokenomics Model 3

### Heatmap of KPI across Scenarios

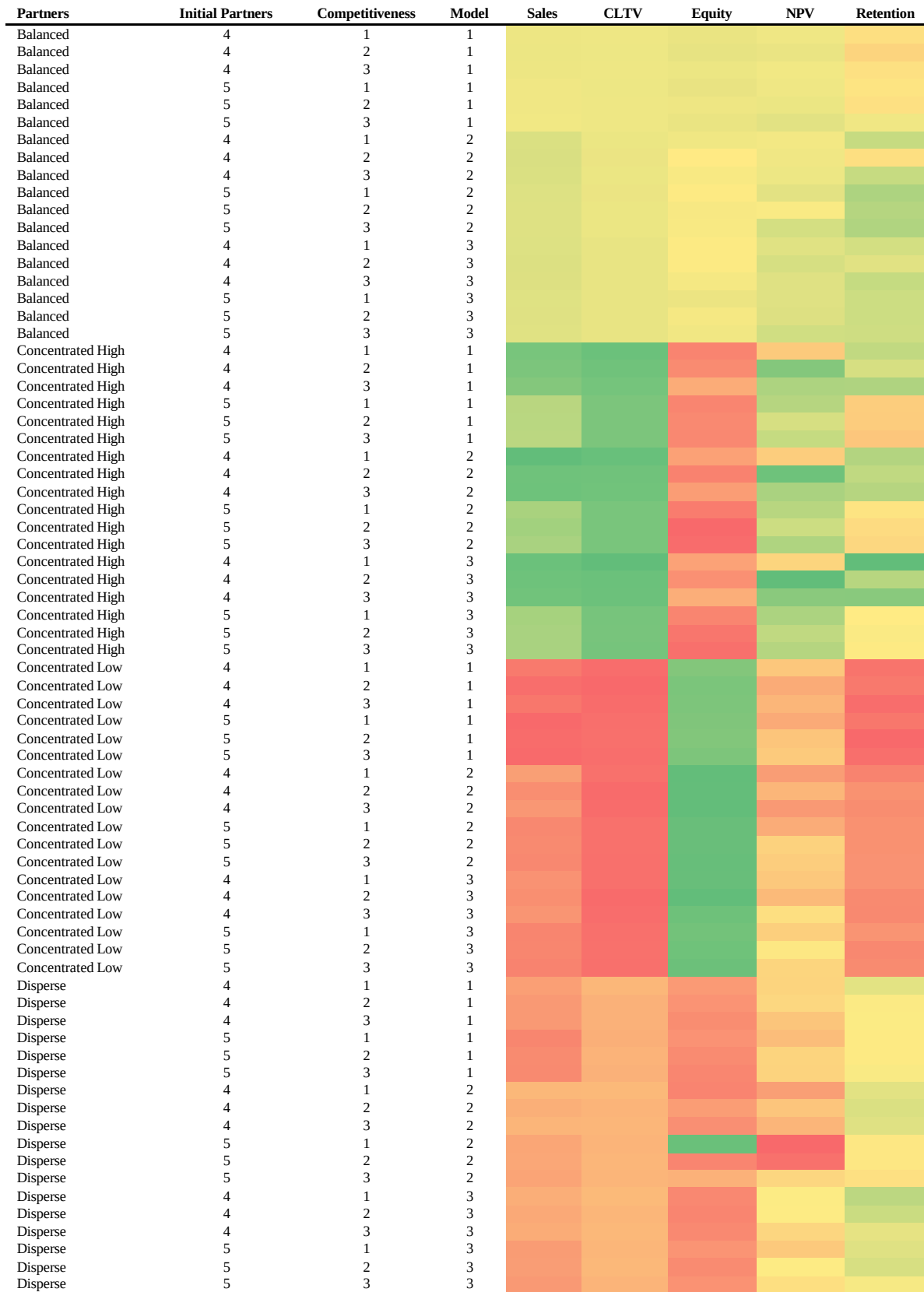


Fig. 28: Heatmap comparing the Scenarios across KPI metrics. Note: The colour-scale is applied per metric, where red represents least favourable and green most favourable.

| parameter      | parameter_change | model   | sales | purchases | unique_customers | frequency_change | spending_change | npv   | equity | cltv  |
|----------------|------------------|---------|-------|-----------|------------------|------------------|-----------------|-------|--------|-------|
| Tier Threshold | Tier - 100       | Model 1 | 0.07  | 0.08      | 0.06             | 6.93             | -0.05           | -0.03 | 0.06   | 0.01  |
| Tier Threshold | Tier - 100       | Model 2 | 0.05  | 0.05      | 0.04             | 0.39             | 0.12            | -0.49 | 0.02   | 0.01  |
| Tier Threshold | Tier - 100       | Model 3 | 0.02  | 0.02      | 0.02             | 1.68             | -0.34           | -0.07 | 0.04   | 0.00  |
| Tier Threshold | Tier 0           | Model 1 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00  | 0.00   | 0.00  |
| Tier Threshold | Tier 0           | Model 2 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00  | 0.00   | 0.00  |
| Tier Threshold | Tier 0           | Model 3 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00  | 0.00   | 0.00  |
| Tier Threshold | Tier +100        | Model 1 | -0.04 | -0.04     | -0.03            | -2.13            | -0.34           | -0.07 | 0.01   | -0.01 |
| Tier Threshold | Tier +100        | Model 2 | -0.04 | -0.03     | -0.03            | -0.13            | -0.16           | -0.26 | -0.02  | -0.01 |
| Tier Threshold | Tier +100        | Model 3 | -0.04 | -0.05     | -0.04            | -0.16            | -0.04           | 0.00  | 0.00   | 0.00  |

*Table 4: Sample Output from the Sensitivity Analysis on the Tier Thresholds*

| parameter              | parameter_change | model   | sales | purchases | unique_customers | frequency_change | spending_change | npv       | equity | cltv |
|------------------------|------------------|---------|-------|-----------|------------------|------------------|-----------------|-----------|--------|------|
| Leader Board<br>Reward | LB               | Model 1 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00      | 0.00   | 0.00 |
| Leader Board<br>Reward | LB               | Model 2 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00      | 0.00   | 0.00 |
| Leader Board<br>Reward | LB               | Model 3 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00      | 0.00   | 0.00 |
| Leader Board<br>Reward | LB +0.05         | Model 1 | 0.02  | 0.02      | 0.02             | 2.51             | 0.11            | 0.15      | 0.02   | 0.00 |
| Leader Board<br>Reward | LB +0.05         | Model 2 | 0.00  | 0.00      | 0.00             | 0.01             | 0.10            | -<br>0.06 | -0.01  | 0.00 |
| Leader Board<br>Reward | LB +0.05         | Model 3 | -0.02 | -0.02     | -0.01            | 2.06             | 0.89            | 0.10      | 0.01   | 0.00 |
| Leader Board<br>Reward | LB +0.1          | Model 1 | 0.02  | 0.02      | 0.02             | 1.80             | -0.06           | 0.01      | 0.03   | 0.00 |
| Leader Board<br>Reward | LB +0.1          | Model 2 | 0.00  | 0.00      | 0.00             | 0.08             | -0.02           | -<br>0.88 | 0.01   | 0.00 |
| Leader Board<br>Reward | LB +0.1          | Model 3 | -0.02 | -0.03     | -0.02            | 2.11             | -0.16           | -<br>0.01 | 0.02   | 0.00 |

Table 5: Sample Output from the Sensitivity Analysis on the Leaderboard Rewards

| parameter   | parameter_change | model   | sales | purchases | unique_customers | frequency_change | spending_change | npv  | equity | cltv |
|-------------|------------------|---------|-------|-----------|------------------|------------------|-----------------|------|--------|------|
| Spend       |                  |         |       |           |                  |                  |                 | -    |        | -    |
| Probability | Base Spend - 0.1 | Model 1 | -0.42 | -0.42     | -0.38            | 1.72             | 0.74            | 0.49 | -0.02  | 0.07 |
| Spend       |                  |         |       |           |                  |                  |                 | -    |        | -    |
| Probability | Base Spend - 0.1 | Model 2 | -0.44 | -0.44     | -0.39            | -0.41            | 0.24            | 0.57 | -0.07  | 0.08 |
| Spend       |                  |         |       |           |                  |                  |                 | -    |        | -    |
| Probability | Base Spend - 0.1 | Model 3 | -0.47 | -0.47     | -0.42            | 1.65             | 2.41            | 0.54 | -0.05  | 0.08 |
| Spend       |                  |         |       |           |                  |                  |                 |      |        |      |
| Probability | Base Spend 0     | Model 1 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00 | 0.00   | 0.00 |
| Spend       |                  |         |       |           |                  |                  |                 |      |        |      |
| Probability | Base Spend 0     | Model 2 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00 | 0.00   | 0.00 |
| Spend       |                  |         |       |           |                  |                  |                 |      |        |      |
| Probability | Base Spend 0     | Model 3 | 0.00  | 0.00      | 0.00             | 0.00             | 0.00            | 0.00 | 0.00   | 0.00 |
| Spend       |                  |         |       |           |                  |                  |                 |      |        |      |
| Probability | Base Spend + 0.1 | Model 1 | 0.46  | 0.47      | 0.37             | 6.52             | 0.03            | 0.44 | 0.14   | 0.07 |
| Spend       |                  |         |       |           |                  |                  |                 |      |        |      |
| Probability | Base Spend + 0.1 | Model 2 | 0.45  | 0.46      | 0.35             | 0.65             | 0.19            | 0.34 | 0.11   | 0.08 |
| Spend       |                  |         |       |           |                  |                  |                 |      |        |      |
| Probability | Base Spend + 0.1 | Model 3 | 0.48  | 0.48      | 0.37             | -0.09            | -0.92           | 0.59 | 0.08   | 0.08 |

Table 6: Sample Output from the Sensitivity Analysis on the Base Spend probability

A Work Project, presented as part of the requirements for the Award of a Master Degree  
in Business Analytics from the NOVA – School of Business and Economics.

TOKENOMICS MODELS FOR A MULTI COMPANY LOYALTY  
PROGRAMS: A MONTE CARLO METHOD APPROACH - REGULATORY  
IMPLICATIONS IN THE EU

MARTINA CROCE

A Project carried out on the Master in Business Analytics, under the supervision of:  
Advisor: Leid Zejnilovic  
Co-Advisor: Lénia Mestrinho

February 25th, 2024

## **Abstract**

The research aims to provide Celfocus with a comprehensive comparative analysis of tokenomics models for multi-company loyalty programs, highlighting their strengths and weaknesses to aid informed decision-making. This involves an in-depth analysis of current loyalty schemes, assessing the impact of tokenization in the digital economy, and exploring how blockchain and gamification can transform customer loyalty experiences. The study includes the development of three unique token-based loyalty programs, designed to optimize benefits for both partner companies and customers. It also addresses challenges and regulatory considerations, with a particular focus on GDPR compliance. The effectiveness of these models was validated through a Monte Carlo analysis, which involved simulating various scenarios to identify critical elements and evaluating key performance indicators for a more profound understanding.

**Keywords:** Loyalty program, Gamification, Blockchain, Tokenomics, Monte Carlo simulation, Technology, Marketing,

## List of abbreviations

|      |                              |
|------|------------------------------|
| LP   | Loyalty Program              |
| MCLP | Multicompany loyalty program |
| TKN  | Token                        |
| PoS  | Proof of Stake               |
| PoW  | Proof of Work                |
| KPI  | Key Performance Indicator    |

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

## **Regulations in a Loyalty Program**

More than ever, businesses of all stripes exploit personal data for a wide range of objectives. In the digital age in which we live, privacy and personal data management have become issues of paramount importance (Ginammi, 2023). The collection of personal data is a phenomenon that is becoming increasingly common for companies in all sectors involved in the development of digital and non-digital products. It is collected from a variety of sources in order to better profile individuals to whom personalised commercial offers can be provided. (Alizadeh et al., 2019). Privacy can be defined as the ability of individuals to control the terms under which their personal information is acquired and used. Personal information is information that identifies or can be used to identify an individual. (Westin, 1968). From a business perspective, protecting privacy means making consumers comfortable with disclosing personal information necessary for marketing. This involves simultaneously communicating to the consumer the benefits of disclosure and providing assurances that the disclosure of personal information is a low-risk proposition (Culnan, 2000). It follows that, fair information practices represent good public policy for both consumers and businesses. However, the collection and processing of personal data can pose significant risks to the privacy of individuals. For instance, data may be subject to unauthorised access, loss, or misuse. Furthermore, the interconnection of multiple services and platforms can create a highly detailed profile of users, which can be used for undesirable purposes such as discrimination or manipulation of individuals' choices (Ginammi, 2023). According to the definition contained in the GDPR, 'personal data is any information relating to an identified or identifiable living person. Various pieces of information which, when collected together, can lead to the identification of a particular person also constitute personal data' (GDPR). Organisations, both public and private, collect and process this data for various purposes, such as providing personalised services, improving targeted advertising, or conducting market research (Culnan, 2000). Nowadays, predictive models make the

management of copious amounts of data more convenient. They summarise their information and amplify its significance in relation to their business objectives, with the aim of designing customised market strategies (Pellicelli, 2008). The results can provide companies with a clearer view of customer profiles. Some of the main benefits of applying predictive analytics for the enterprise include:

- Loyalisation through optimisation of customer acquisition and research strategies, adopting appropriate tactics to improve the path to conversion to loyalty programs, based on the history of actions taken
- Focusing activities on real customer needs enables optimisation of cross-selling and up-selling<sup>2</sup> activities, resulting in increased revenue
- Development of marketing strategies customised on real-time user behaviour
- Improved planning of digital campaigns, choosing the most relevant channels in relation to current market trends
- Identifying the most profitable customers and their areas of interest

Looking at the consumer, however, there are benefits from the implementation of these models (Nasti, 2015):

- Functional, linked to the utility of the product itself
- Affective, linked to the emotional sphere. As, in a condition of mutual satisfaction, a lasting relationship is generated between the two subjects.

Today, most individuals are aware that surfing the Internet involves the installation on their device of a series of cookies by each website browsed. These cookies can be considered as real traces of the activities conducted on that site, useful for establishing browsing patterns. Personal data such as, for example, navigation data, purchase preferences or the topics sought are

---

<sup>2</sup> Johnson, J. S., & Friend, S. B. (2015). Contingent cross-selling and up-selling relationships with performance and job satisfaction: an MOA-theoretic examination. *Journal of Personal Selling & Sales Management*, 35(1), 51-71.

collected through the latter. The data are stored in dedicated databases on which predictive analyses are performed. (Sgobbi, 2022). Through to this process, marketers can nowadays record exactly what an individual consumer buys, when they buy it, how much they buy and how often. In a loyalty programme, the marketer pursues two main objectives: (i) to encourage the consumer to make more purchases in the future (repeat customer); (ii) to enable the marketer to profile the consumer in order to conduct market research and segmenting (profiled customer) (Justicia & Ferrer, 2016). The use of the collected data combined with retailer-sponsored loyalty programs (e.g., grocery shop discount cards) and shop credit cards (e.g. the Sears credit card) allows retailers to record, use and even sell information on the purchasing patterns of individual consumers. (Graeff & Harmon, 2002). Loyalty programs are a common way for companies to obtain and use personal information for commercial purposes. In addition to providing rewards and discounts for consumers, loyalty programmes benefit companies by fostering a higher level of customer loyalty. (Alizadeh et al., 2019). From what has been discussed so far, therefore, it can be observed that companies are increasingly using loyalty programs to manage their interactions with consumers. In order to encourage customers not only to return but also to reveal more about their profile, the retailer needs to offer additional rewards to consumers. Thus, sellers, the advantages offered, repay consumers for their private information. On the other hand, they become aware of how much their personal data are worth to sellers and can decide to what extent they are willing to disclose that data in exchange for those benefits. (Justicia & Ferrer, 2016). These initiatives help companies determine which customers are most valuable, foster greater loyalty with them and increase the effectiveness of marketing communications. Customers. often benefit from these programmes because they can access tailored products and services, relevant promotions, and more personalised and productive communications with the company. There is a positive feedback loop between the increased availability and analysis of 'big data' and the expansion of companies. Big data helps companies

leverage LPs more efficiently, as LPs are a great way to collect information on purchases and other transactions, which can increase profitability and improve other marketing initiatives. (Stourm et al., 2020). Factors such as, for example, who are the eligible customers for these programmes, what is the ideal length of stay in the promotion, or even what concept the company promoting the programme should adopt to attract and retain its customers, are particularly important aspects to consider when it comes to loyalty programmes. As shown in the article by Išoraitė (2016), one of the main problems highlighted in the surveys conducted are the rules of participation in loyalty programmes, which might influence the participants' intention to enter and stay in such programmes. For example, consumers are aware that loyalty programmes are also used to retrieve consumers' personal data that can then be sold to third parties.

## **The role of the GDPR**

The responsible management of personal data has become a key priority for organisations and regulators. For example, the General Data Protection Regulation (GDPR) seeks to provide customers with greater control over data collection and processing to curb this problem and thus, in other words, empower customers to review and manage their personal data (Alizadeh et al., 2019). Nowadays, personal information is widely exchanged online and is becoming increasingly relevant. Users benefit from the use of modern technologies and online communication services, often without incurring direct costs. However, personal privacy is often sacrificed in the process (Ginammi, 2023). In a context of increasing digitisation, where huge data sets are generated and stored, many of which include personal data, it is essential that individuals understand their rights and the implications of sharing their data. User awareness is key to making informed decisions about sharing personal data and trusting the organisations that process it (Thobani, 2019). The personal data obtained is often extremely sensitive and can

be misused or subject to data theft. The primary safeguarding objective of the General Data Protection Regulation is achieved by restricting data controllers to process personal and contact information only with the explicit and reversible consent of the individual. It is crucial that data controllers make explicit the purposes for which they use the information and the methods by which it is stored and protected (Tahal & Formanek, 2020). As a result, it was deemed necessary for individuals to be able to exercise some form of control over their personal data. That is, individual control, particularly over one's own person, has been described as reflecting fundamental values such as autonomy, privacy, and human dignity (Solove, 2007). Looking at the legal bases of the regulation, consent is one of them. With consent, the data subject approves of his or her data being used for one or more specific purposes, which are also referred to as subjective rights or control rights. It follows that, the right to information is closely linked to consent, since the latter is only valid if informed, e.g., if the data subject receives all the information necessary to approve or disapprove of the data processing (Lynskey, 2015).

The GDPR does not specify how data controllers should fulfil their notification obligation or, in other words, how the right to information should be guaranteed. In the context of Web 2.0, information is usually provided in the general terms and conditions of the web service or in the privacy policy of providers' websites (Kosta, 2013). Compared to what was discussed in the previous section, often, due to the length and complexity of privacy policies, data subjects rarely read or understand them and, if they do, they are not able to follow all the changes that frequently occur. The problem is compounded on mobile sites where reading lengthy policies is not practical (Edwards & Abel, 2014). One possible response to this failure of privacy policies could be visualisation using icons (standardised images). These could improve control for two reasons: firstly, they simplify the understanding of information. Secondly, they save readers' time. The idea has been made explicit in Article 12(7) of the GDPR, which contains the possibility of using standardised icons stating that:

“... information [...] may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing (L 119/40).” Recital 58 adds that such visualisation should be used “where appropriate” (L 119/11).

Picking up, then, on what was discussed earlier in this section, the use of personal data and advances in technology have made loyalty programmes more widespread and comprehensive. Since rewards are often determined using transaction data, loyalty programmes encourage customers to self-identify when making a purchase. Furthermore, the collection of data through LPs can lead to a complete 360-degree view of the customer. Although societal concerns would persist in the absence of LPs, they have the potential to ameliorate some problems. Examples could be inequality (the ability of LPs and big data to accurately target consumers) and sustainability, which is affected by the power of the LP/big data partnership because fees depend on demand. (Stourm et al., 2020). In this regard, Lacey & Sneath's (2006) equity theory can give us a distinct perspective on the topic. The two authors state that, the equity theory can be used to assess whether consumer loyalty programs are fair or discriminatory. This viewpoint holds that equity is anything that is worthy, just, or fair. Contrary to equality, which demands that every consumer receive the same value proposition regardless of individual contributions, equity does not imply equality. Equity theory states that consumers develop opinions about the inputs such as cash, time, effort, and opportunity costs and outputs such as tangible and intangible benefits that engage in a transaction. In this section, distributive equity, procedural equity, and interactional equity three well-established components of this theoretical base are used to evaluate the fairness of value proposition discrimination techniques that are frequently seen in customer loyalty programs. In *Table 1*, there is a summary of customer perceptions and potential sources of discrimination that are presented (Lacey & Sneath, 2006).

Table 1: Assessing fairness of value proposition discrimination in customer loyalty programs

| Form of equity       | Customer perceptions of equity                                                                             | Sources of perceived inequity                                                                                                                                                                 |
|----------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Distributive equity  | Customers perceive there is fairness in the rewards they receive in return for their input                 | Needs and desires of different market segments<br>Usage rate often linked to rewards<br>Observing how other customers are treated<br>Rising expectations and demands for greater rewards      |
| Procedural equity    | Customers perceive there is fairness in the process or means by which reward allocation decisions are made | Nonstandardization of loyalty programs<br>Changing rules<br>Nonportability of programs<br>Inaccurate and/or inadequate consumer information<br>Variability in response to individual requests |
| Interactional equity | Customers perceive there is fairness in the exchange of information and communication of outcomes          | Treatment of customers<br>Delivery of the value proposition<br>Inconsistency across interactions<br>Communication of mechanics and program criteria                                           |

## Tensions between blockchain systems and the General Data

### Protection Regulation (GDPR)

In this section, we have analysed some of the most discussed tensions between blockchain technology and the GDPR in the existing literature produced by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS)<sup>3</sup> and other academic authors. For most of the text, reference will be made to public blockchains, as the compliance of private blockchains is easier to achieve, given their centralised nature.

### Personal Data Saved on the Blockchain

Before analysing what tensions exist between blockchain and the GDPR, we need to analyse what personal data are stored within the blocks of a public blockchain or within off-chain<sup>4</sup> storage systems. To evaluate the legitimacy of processing personal data on public blockchain systems, it is mandatory to analyse the various data types saved on a blockchain and their

<sup>3</sup> [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS\\_STU\(2019\)634445\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

<sup>4</sup> Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, 58(3), 102535.

essential components. In particular, two types of data can be identified in this context: transactional data and metadata.

### **Transactional data**

The content of a transaction on a public blockchain includes personal data like personal identifiers, financial data or medical information relating directly or indirectly to data subjects, which could be memorised either as plain, encrypted, or hashed data on-chain. (Belen-Saglam et al., 2023). According to the National Institute of Standards and Technology (NIST), a hash function is defined as "[...] an algorithm that accepts an input of arbitrary length and produces an output of fixed length. The hash function is designed in such a way that it is difficult to find two different inputs that produce the same output." According to the international standard ISO/IEC 15408, encrypted data is instead defined as: "data that has been rendered unintelligible to anyone without the decryption key". The question that needs to be asked at this point is whether saving encrypted or hashed personal data on a chain makes it pseudonymised with respect to the GDPR. The GDPR defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information." As Duarte (2019) claims, it is fundamental to define what additional information in the blockchain context is sufficient to reveal the original data. In the case of encrypted data, the private key (decryption key) is the additional information useful to reveal the original data. On the contrary, given the nature of a hashed data, it might seem that there is no way to actually trace the original data, however there is a linkability risk when data is stored in a hashed form: the possibility to link a particular piece of data and a hash value can still be found (Erbguth, 2019). There would seem to exist a general consensus among researchers that transactional data pseudonymised by hash algorithms or encryption should be treated anyway as personal data (Schmelz et al., 2018).

However, the GDPR defines pseudonymisation and anonymisation of data as different concepts even though the distinction is not truly clear. As stated in Recital 26 of the GDPR, data becomes anonymous if it is “reasonably likely” that no identification of the data subject can be derived (European Parliament, Regulation 2016/679 (EU)). This issue has caused scholars and national data protection authorities to have divergent understandings of the matter.

A more definitive approach to hash functions is provided by the Spanish Data Protection Act (AEPD, Agencia Española de Protección de Datos), which states that hashed data should be considered either anonymised or pseudonymised depending on a range of factors, including the entities involved and the type of data at hand (Giannopoulou, 2020).

However, according to the UK's Information Commissioner's Office, pseudonymisation is really only a security precaution. In the document “The General Data Protection Regulation, Key Definitions, what is personal data?,” (2023), of the same institution it is stated that pseudonymisation has no effect on the data's status as personal data.

A similar view was expressed by Article 29 of the Data Protection Working Party in relation to the GDPR's previous data protection law, the EU Data Protection Directive, 1995. This working party acknowledged that while pseudonymisation lessens the linkability to the original identity, it does not completely eliminate the risk of the data subject being identified. An example is represented by a brute-force attack that decrypts a piece of encrypted data without the decryption key (Article 29 Data Protection Working Party, 2014).

Erbguth pointed out that it is questionable whether the GDPR is intended to shield the data subject from the risk of decrypting the data itself when the data subject is the only one with the key and no one else can obtain it (Erbguth, 2019). Giordano (2020) brought up the same point and emphasised that neither a central body nor an intermediary is aware of the connection between the key and its user because the key typically remains in the exclusive possession of the user. Rampone (2018) distinguished between the two roles and suggested that only the

owner of the list of correspondence connecting the codes to the identities of the data subjects and those who can lawfully obtain possession of it, would consider key-coded data to be personal data. She did not, however, view key-coded data as confidential for individuals who are not in possession of the correspondence list or are prohibited from accessing it. More surprisingly, Stan and Miclea (2019) argued that sensitive GDPR health data could be stored as a hash on a block without violating the GDPR because the data cannot be returned to its original state and is thus sufficiently anonymous. In the same context, Eichler et al. (2023) mentioned off-chain storage options and said that hashed data should once again be deemed sufficiently anonymous if the information connecting it to a data subject was stored off-chain and subsequently deleted. It is frequently emphasised in the literature that, while state-of-the-art methods are unlikely to link encrypted personal data back to the data subject at the moment, this cannot be guaranteed in the future due to the rapid advancement of technology (Wirth & Kolain, 2018). Advances in quantum computing, for example, have been mentioned as a threat to public-key cryptography, as available quantum computers may soon be powerful enough to derive the private keys used to encrypt personal data today (Shahaab et al., 2020).

### **Metadata**

Another type of data that can be considered personal data is metadata, which is stored in blockchains. Blockchain technologies are based on public-key cryptography, which verifies transactions using public keys. According to Politou et al. (2019), the keys are crucial components of the metadata and must be made publicly accessible on the blockchain in order for transactions to be validated.

Public keys, which are frequently used to determine the origin of transactions and which, when combined with other information, constitute personal data, are the kind of identifiers mentioned in Recital 30 of the GDPR, according to a consensus in the literature that we have observed (Wirth & Kolain, 2018). Real-world identities hidden behind public keys may be revealed by

extra data that is collected in compliance with legal requirements, such as when cryptocurrency asset exchanges conduct "Know Your Customer" (KYC) and during "Anti-Money Laundering" (AML) tasks (Duarte, 2019). It has been suggested that if a natural person uses the same public key across multiple transactions, patterns could appear that could be used to identify them again (Schmelz et al., 2018). In summary, public keys are a major obstacle to creating a blockchain system that complies with the GDPR since they are an integral part of the technology and cannot be moved to be off chain like other data. Nonetheless, the literature offers methods for anonymising public keys, including ring signatures and zero-knowledge proofs (ZKPs), which will be discussed below.

## **Role and responsibilities**

Regarding GDPR compliance for public blockchain systems, one of the most frequently discussed topics in the literature regards identifying data controllers and processors. A data controller is defined by the GDPR as an organisation that, either alone or in concert, chooses the means and purposes for processing personal data (Koscina et al., 2021). An organisation that manages personal data on behalf of a controller is known as a processor. There is little consensus among researchers on which subject should be identified as a possible data controller of a public blockchain system. The literature points out as data controllers either lightweight nodes, full nodes, miners, all nodes as joint controllers, designers/developers, or even users. On the other hand, users and blockchain network nodes are both agreed as data processors in public blockchain systems among researchers. (Belen-Saglam et al., 2023). Moreover, most of the articles cited below operate under the premise that individuals who provide personal data to the blockchain do so as network participants. Only Moerel (2018), on the other hand, considered the situation in which a user of an application based on a blockchain shares personal data to the blockchain as a data subject.

### **Lightweight nodes**

Un lightweight node is a node that plays a reduced role compared to a full node, as it does not store the entire blockchain, but only a part of it, or does not store transaction data, but only their hashes (Mellia et al., 2023).

According to Buocz et al. (2019), lightweight nodes' ability to request transaction creation would be an excessive interpretation of the term "controller" because they only define "what" (the transactions) but not "why" and "how" of the processing, as a true controller should do.

### **Full nodes and miners**

Full nodes and miners are subjects responsible for storing the entire blockchain ledger, verifying transactions, and maintaining the consensus protocol. Full nodes are essential for the security and integrity of blockchain systems (Khan et al., 2022). Buocz et al. (2019) recognized full nodes' critical contributions to the operation of the blockchain network; however, because they cannot change the protocol or choose a different protocol within the respective software, they were not considered controllers. According to Jaccard and Tharin (2018), when a number of full nodes form more than 50% of total mining power, they should be considered joint controllers. They also asserted that every full node and possibly every miner would be considered data processors under the GDPR because their operations are comparable to those of Internet hosts. Some researchers found the miners' responsibilities as controllers insufficient due to their lack of power in determining the purposes or means of processing. Other researchers have also acknowledged that, under certain conditions, nodes and miners could establish their own goals and methods, such as altering the regulations of blockchain-based platforms by forking the chain or gaining access to the public database stored on the blockchain to gather personal data for commercial purposes. It is possible to argue that in these situations, miners and nodes would work together as joint controllers (Duarte, 2019).

### **Designers/developers**

There is even greater diversity in the discussions about the roles that designers and developers should play. Buocz et al. (2019) began their examination of the developer responsibilities by posing the following question: who governs the infrastructure or in other words who decides what goes into the code? Since it outlines the obligations of the data controller(s) in a blockchain system, this question is crucial. The authors emphasised the dynamic nature of open-source project teams, in which a dynamic group makes proposals and provides inputs to improve the code. They also stated that in spite of this dynamic nature, the code is developed and maintained by a small group of core developers who are heavily involved in the platform's architecture. According to Schellekens (2020), although the core developers decide the protocol proposal's content, they do not have the authority to determine whether or not this will be the actual method by which data is processed within a blockchain network. Other subjects considered data processors in the literature are smart contract developers, who process personal data for data controllers (Ramos & Silva, 2019). According to Dutta et al. (2020), data processors might include both the creators of smart contracts and the smart contracts themselves.

According to some researchers, data on a blockchain network is pseudonymised and should be considered personal data only by participants who have access to extra information that enables the data to be linked to a specific data subject. In off-chain storage solutions, controllers are limited to participants who have the additional information (decryption keys, for example) needed for attribution; the party in control of the off-chain storage could be considered a data controller (Guggenmos et al., 2020).

## **Users**

Since users choose what information is included in a transaction and so determine the specifics of processing, some researchers have also argued that users should be considered data controllers. (Ramos & Silva, 2019). This interpretation raises the intriguing point that individual users can be both a data controller and a data subject, rendering many data processing

requirements superfluous. Buocz et al. (2019) made the exact opposite argument: while a user can choose to connect to and disconnect from the blockchain at any time, they do not appear to have the authority to decide the method or end goal of the processing. As a result, they cannot be considered data controllers in public blockchain systems.

### **Perspective of application domains**

Another use case involves data subjects using an application that provides a blockchain system as a service. Moerel claims that service and application providers who choose the method and goal of processing personal data have to be considered data controllers (Moerel, 2018).

### **Concerns**

While blockchain technology inherently incorporates certain security and privacy mechanisms, it has concurrently introduced novel concerns in these domains: Right to Be Forgotten, Right to rectification, Right of access, Right to object, Right to data portability, Right to restrict processing, Territorial scope (Belen-Saglam et al., 2023). Each concern will be briefly overviewed below.

#### **Right to be forgotten**

A significant area of contention regarding the interplay between blockchains, particularly public blockchain systems, and the General Data Protection Regulation (GDPR) centres on the immutable nature of blockchains. This inherent characteristic renders the deletion of personal information virtually impossible, thereby impeding the enforcement of the GDPR's Right to Be Forgotten, as delineated by Belen-Saglam et al. (2023). Public blockchain systems uphold a high standard of data integrity due to their immutable nature. However, as previously noted, this feature directly contradicts the GDPR's right to be forgotten for data subjects (Mannan et al., 2019). According to certain researchers, if a blockchain-based system complies with a data erasure request, it will do so at the expense of blockchain consistency, which could potentially

undermine dependability and trust (Tatar et al., 2020). According to the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS) different national authorities have given distinct interpretations to the concept of erasure, in order to include techniques that do not require the destruction of data. As the same research states, further light needs to be shed on the interpretation of the concept of erasure, with the aim to harmonize it for every member state. Meanwhile, the interpretation of erasure given by the French Authority (CNIL) could represent a possible resolution of the conflict which exists between GDPR and DLT systems. The destruction of the private key with which data was encrypted is interpreted as erasure of the data.

### **Right to restrict processing**

According to the GDPR, it is required to have a valid lawful basis in order to process personal data. Obtaining explicit consent from the data subject for the processing of any personal data is one of the most commonly used bases for lawful processing (European Parliament, Regulation (EU) (2016) 2016/679). The latest research conducted by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS), highlighted technical obstacles to the ability of blockchain solutions to comply with the Regulation. From the technical point of view, it seems hardly possible to restrict processing on a blockchain because of the automated processing that characterize this technology. In fact, intervening in the data processing of a blockchain is by design made extremely difficult, in order to increase trust and data integrity towards the network. Poelman and Iqbal (2021) suggest that smart contracts which limit the use of data only, when necessary, could be used to conduct the right to restrict processing. Daudén-Esmel et al. (2021) produced a solution in which the consent smart contract handled the restriction and could restrict the amount of personal data that could be gathered.

### **Right to rectification**

Article 16 of the GDPR states that the data subject has the right to obtain from the data controller the rectification of inaccurate personal data. As stated by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS), the applicability of the right differs depending on the type of blockchain involved. For private or permissionless blockchains, a rectification request could take the form of altering records by re-hashing consecutive blocks. This is not due to any technical difficulties, as each node has a local copy of the ledger that it could alter, but to organisational difficulties. Rectifying data on such a blockchain would require forking the network for each request, involving thousands of nodes. According to Al-Abdullah et al. (2020), this right might be given by presenting a supplementary statement that clarifies that a transaction can be changed by publishing a new transaction containing the updated or accurate data without having to entirely erase previous data. Dejanovic et al. (2019) created a procedure that erases and renders inaccessible the encrypted key for a previous data block as soon as the hash value of a new data block is added to the blockchain.

### **Right of access**

Article 15 of the GDPR states that the data subject has the right to obtain confirmation by the data controller regarding the processing of his or her personal data and to access those personal data. As suggested by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS) there are not particular problems with the applicability of Article 15 in the blockchain context. However, Al-Abdullah et al. (2020) contended that in order to uphold this right, policies and user agreements that detail the technical specifics of the network's operation should be given to data subjects. This is because the controllers in a blockchain system only handles encrypted or hashed versions of the data, not the actual form of it. The EU Blockchain Observatory and Forum have noted that it is difficult to enforce the right of access in public blockchain systems because data subjects are not given a contact person to inquire about whether and for what purpose their data is being processed, among other things.

## **Right to object**

Article 21 of the GDPR gives the data subject the right to object to any processing of personal data directly or indirectly related to them. The data controller must stop every processing activity when the data subject exercises the right. The applicability of this right to the blockchain context runs into two problems. As suggested by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS), the data controller's interest in maintaining the integrity of records on the blockchain could be interpreted as a 'legitimate interest', de facto preventing the data subject from exercising the right to object. In the same study conducted by STOA, the development of regulations providing legal certainty in this regard is suggested to the European Parliament. The other issue was highlighted by the authors Poelman & Iqbal (2021) and concerns the difficulties in identifying the data controller of a blockchain. In fact, according to their study, without knowing who the blockchain controller is, it may be challenging to exercise the right. However, Daudén-Esmel et al. (2021) asserted in their proposed study that smart contracts could be put in place in order to exercise the right to object by revoking consent.

## **Right to data portability**

Article 20 of the GDPR states that the data subject who after releasing his personal data to the data controller you have the right to receive them in a structured and in a machine-readable format. One of the goals of the GDPR is to provide individuals with greater control over their data by enabling them to access and utilise their personal information for independent uses across various services (Information Commissioner's Office, UK, Right to data portability, 2023). According to the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service (EPRS) interoperability between blockchains should be encouraged, in order to comply with Article 20 of the GDPR. However, opposing viewpoints have been expressed. For example, according to some researchers, this right necessitates interoperability between

various blockchains, which is currently non-existent in practice because blockchain systems are not standardised (Kusber et al., 2020). According to Giordanengo (2019), transferring data between providers would necessitate the removal of data stored by the previous provider, which is not achievable on public blockchains.

### **Territorial scope**

Another aspect which poses tensions to the GDPR is data sharing outside of the EU/EEA/UK: for a public blockchain system, it is normally the case that every node holds a full copy of all data, no matter where the node is physically located or even unknown (Belen-Saglam et al., 2023). Public blockchains are distributed, meaning that anybody can become a node and initiate transactions on the network. As a result, its network has no physical boundaries, which could cause problems with localization and the application of the law (Zemler & Westner, 2019).

In order to address the issue, Al-Abdullah et al. (2020) recommended that a comprehensive data security and protection agreement be prepared among network participants, adhering to mechanisms such as the standard contractual clauses permitted by the European Commission. In other research, smart contract-based technical solutions were offered that managed the nation of each actor receiving personal data; if that nation is outside of the EU, EEA, or UK, the algorithm sets the GDPR compliance to false (Barati & Rana, 2020)

### **Technical solutions for protection of personal data in public blockchain systems**

Personal data is not always stored in blockchain systems; however, the possibility of personal data being stored in a blockchain system cannot be ruled out. The literature below analyses possible technical solutions to the concerns discussed above.

#### **Anonymisation**

According to Karasek-Wojciechowicz (2021), any controller would not be able to link data on a public blockchain with a data subject if the data is anonymised without using additional information that the data subject possesses. She believed that finding the user who possesses the extra information required to identify the data subject was nearly impossible for data controllers.

The absence of legal guarantees and untraceable financial transactions that go against KYC and AML regulations are additional issues with anonymised data (Schmelz et al., 2018).

### **Hashing out**

The most talked-about method for processing personal data in blockchain in a GDPR-compliant manner with the intention of putting the Right To Be Forgotten into practice is hashing out or off-chain storage. Hashing out is a technique that resolves a number of issues brought up by the distributed nature of public blockchains by storing data hashes on-chain and keeping the actual data off-chain through the use of a local database. In this manner, personal data stored in an off-chain repository can be erased upon a data subject's request for its deletion (Sarier, 2021). Because hashes are much smaller than actual data, this also enables the blockchain to store more data (Belen-Saglam et al., 2023). Some researchers suggested using the hashing-out technique in conjunction with encryption to implement the Right To Be Forgotten. To encrypt the hashed value, a private key is thus sent to the data subject; removing the key is said to constitute erasure for GDPR purposes (Zieglmeier & Daiqui, 2021). Conversely, according to Karasek-Wojciechowicz (2021), this process could not be deemed erasure under the GDPR if, following key destruction, the controller is still able to link the data stored on the ledger with the natural person. This could be done by analysing the content of public ledgers and external data that the controller could access. For example, hashed data can reveal sensitive personal information when combined with other information and can be the target of dictionary attacks (Politou et al., 2019). In contrast to those views, Stan, and Miclea (2019) contended that hashes

do not violate the GDPR if all information about a data item is only stored as a hash on-chain because they are sufficiently anonymous.

### **Zero-knowledge proof**

Zero-knowledge proof (ZKP) is a technique that enables the entire blockchain network to agree on the validity of a transaction without revealing the transaction's content, and it has been recognized by several researchers as an effective privacy-enhancing technology that can reduce the risk of liability for GDPR violations (Damian et al., 2019). This method was also considered a way to adhere to the Right to Be Forgotten (Iqbal and Poelman, 2021). Despite being a well-known solution with numerous applications, its primary flaw was noted to be the heavy computational burden (Schwerin, 2018).

### **Merkle trees**

According to Schellinger et al. (2022), ZKPs and Merkle trees can be used to create a blockchain-based, privacy-preserving record of data that is exempt from GDPR regulations.

### **Ring signatures**

Ring signatures are digital signatures performed by a group of people, each of whom has a private key to sign a specific transaction. It is not possible to identify which member started the signing, even though it is known that one of those members did so. Consequently, this offers robust protection for personal information. Al-Abdullah et al. (2020) reported that certain researchers have either adopted or recommended the use of ring signatures for GDPR compliance. However, Giannopoulou (2021) pointed out that neither the developer communities nor any official standardisation bodies have yet to standardise ring signatures. Furthermore, it is still unclear if they meet the GDPR's anonymization requirements.

### **Secure multi-party computation**

By enabling multiple parties to conduct computations over encrypted data without disclosing their input to one another, secure multi-party computation seeks to protect privacy (Jaccard &

Tharin 2018). However, because this technique requires a significant amount of system resources, such as ZKPs and ring signatures, it does not appear to be feasible to implement at scale (Politou, et al., 2019).

## References

- A Survey on Full Nodes in Blockchain Khan, M. A. Khan, S. A. Qureshi, N. I. Aslam, M.A. Khan 2022
- Al-Abdullah, M., Alsmadi, I., AlAbdullah, R., & Farkas, B. (2020). Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. *Digital Policy, Regulation and Governance*, 22(5/6), 389-411.
- Albanese Ginammi, M. (2023). Privacy e gestione dei dati personali nella compravendita online.
- Alizadeh, F., Jakobi, T., Boden, A., Stevens, G., & Boldt, J. (2020, September). GDPR reality check-claiming and investigating personally identifiable data from companies. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 120-129). IEEE.
- Alizadeh, F., Jakobi, T., Boldt, J., & Stevens, G. (2019). GDPR-reality check on the right to access data: claiming and investigating personally identifiable data from companies. In *Proceedings of Mensch und Computer 2019* (pp. 811-814).
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, Official Opinion, European Commission, 2014. <https://ec.europa.eu/>
- Barati, M., & Rana, O. (2020). Enhancing user privacy in IoT: Integration of GDPR and blockchain. In *Blockchain and Trustworthy Systems: First International Conference, BlockSys 2019, Guangzhou, China, December 7–8, 2019, Proceedings 1* (pp. 322-335). Springer Singapore.
- Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, 100129.
- Blanco-Justicia, A., & Domingo-Ferrer, J. (2016). Privacy-aware loyalty programs. *Computer Communications*, 82, 83-94.
- Buocz, T., Ehrke-Rabel, T., Hödl, E., & Eisenberger, I. (2019). Bitcoin and the GDPR: Allocating responsibility in distributed networks. *Computer Law & Security Review*, 35(2), 182-198.
- Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working?. *Journal of Public Policy & Marketing*, 19(1), 20-26.
- Damian, C., Lazăr, I., Vişoiu, D. G., Romanescu, Ş., & Alboaie, L. (2019, October). Applying blockchain technologies in funding of electrical engineering industry applications. In *2019 International Conference on Electromechanical and Energy Systems (SIELMEN)* (pp. 1-5). IEEE.
- Daudén-Esmel, C., Castellà-Roca, J., Viejo, A., & Domingo-Ferrer, J. (2021, January). Lightweight blockchain-based platform for gdpr-compliant personal data management. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)* (pp. 68-73). IEEE.

-Dejanovic, S., Marjanovic, J., Lendak, I., & Erdeljan, A. (2019). Using blockchain to decentralize and protect user privacy in compliance with GDPR. ICIST 2019 Proceedings, Information Society of Serbia, 171-173.

-Duarte, D. (2019). An introduction to Blockchain technology from a legal perspective and its tensions with the GDPR. Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law-CIJIC.

-Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law and Technology Review*, 16(1), 1– 65.

-Jaccard, G. (2018). GDPR & Blockchain: the Swiss take. *Jusletter IT*, 4.

-Giannopoulou, A. (2021). Putting data protection by design on the blockchain. *Eur. Data Prot. L. Rev.*, 7, 388.

-Giordanengo, A. (2019). Possible usages of smart contracts (blockchain) in healthcare and why no one is using them. In *MEDINFO 2019: Health and Wellbeing e-Networks for All* (pp. 596-600). IOS Press.

Giordano, M. T. (2020). Blockchain and the GDPR: new challenges for privacy and security. In *Blockchain, Law and Governance* (pp. 275-286). Cham: Springer International Publishing.

-Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of consumer marketing*, 19(4), 302-318.

-Guggenmos, F., Lockl, J., Rieger, A., Wenninger, A., & Fridgen, G. (2020). How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the German asylum procedure.

-İşoraitè, M. (2016). Customer loyalty theoretical aspects. *Ecoforum Journal*, 5(2).

-J. Erbguth, Five ways to GDPR-compliant use of blockchains, *Eur. Data Protect. Law Rev.* 5 (3) (2019) 427–433, <https://doi.org/10.21552/edpl/2019/3/19>.

-Karasek-Wojciechowicz, I. (2021). Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. *Journal of Cybersecurity*, 7(1), tyab004.

-Koscina, M., Lombard-Platet, M., & Negri-Ribalta, C. (2021, March). A blockchain-based marketplace platform for circular economy. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (pp. 1746-1749).

-Kosta, E. (2013). *Consent in European data protection law* (Vol. 3). Martinus Nijhoff Publishers.

-Kusber, T., Schwalm, S., Shamburger, K., & Korte, U. (2020). Criteria for trustworthy digital transactions-Blockchain/DLT between eI-DAS, GDPR, Data and Evidence Preservation. *Open Identity Summit 2020*.

- Lacey, R., & Sneath, J. Z. (2006). Customer loyalty programs: are they fair to consumers?. *Journal of consumer marketing*, 23(7), 458-464.
- Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.
- M. Mellia, S. Romano, S. Ceri, P. Bellavista (2023) "Lightweight Nodes for Blockchain Systems: A Survey". In *IEEE Communications Surveys & Tutorials*
- Mannan, R., Sethuram, R., & Younge, L. (2019). Practitioner's Corner: GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review*, 5(3), 421-426.
- Moerel, L. (2018). Blockchain & data protection... and why they are not on a collision course. *European review of private law*, 26(6).
- Nasti, L. (2015). *Dal marketing tradizionale al web marketing*.
- Pellicelli, A. C. (2008). *Le strategie di posizionamento nell'economia digitale* (pp. 1-259). G. GIAPPICHELLI EDITORE.
- Poelman, M., & Iqbal, S. (2021, January). Investigating the compliance of the gdpr: Processing personal data on a blockchain. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)* (pp. 38-44). IEEE.
- Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 9(4), 1972-1986.
- Ramos, L. F. M., & Silva, J. M. C. (2019, April). Privacy and data protection concerns regarding the use of blockchains in smart cities. In *Proceedings of the 12th international conference on theory and practice of electronic governance* (pp. 342-347).
- Rampone, F. (2018). Data Protection in the Blockchain Environment: GDPR is not a Hurdle to Permissionless DLT Solutions. *Cyberspazio e diritto*, 19(61), 457-20.
- Sarier, N. D. (2021). Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management. *Computers & Security*, 105, 102243.
- Schellekens, M. (2020). Conceptualizations of the controller in permissionless blockchains. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 11, 215.
- Schellinger, B., Urbach, N., Volter, F., & Sedlmeir, J. (2022). Yes, I do: Marrying blockchain applications with GDPR. *e-government*, 19, 22.
- Schmelz, D., Fischer, G., Niemeier, P., Zhu, L., & Grechenig, T. (2018, August). Towards using public blockchain in information-centric networks: Challenges imposed by the european union's general data protection regulation. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)* (pp. 223-228). IEEE.
- Schwerin, S. (2018). Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): a delphi study. *The Journal of the British Blockchain Association*, 1(1).

-SGOBBI, M. IL TRATTAMENTO DEI DATI PERSONALI E GLI STRUMENTI DI RACCOLTA DEI DATI ONLINE: COOKIES E BIG DATA.

-Shahaab, A., Maude, R., Hewage, C., & Khan, I. (2020). Managing gender change information on immutable blockchain in context of GDPR. *The Journal of The British Blockchain Association*, 1-8.

-Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. Yale University Press.

-Stan, O. P., & Miclea, L. (2019). New era for technology in healthcare powered by GDPR and blockchain. In *6th International Conference on Advancements of Medicine and Health Care through Technology*; 17–20 October 2018, Cluj-Napoca, Romania: MEDITECH 2018 (pp. 311-317). Springer Singapore.

-Stourm, V., & Bradlow, E. T. (2023). Cross-reward effects in a coalition loyalty program: The impact of a point currency devaluation. *International Journal of Research in Marketing*, 40(2), 276-293.

-Stourm, V., Bradlow, E. T., & Fader, P. S. (2015). Stockpiling Points in Linear Loyalty Programs. *Journal of Marketing Research*, 52(2), 253-267. <https://doi.org/10.1509/jmr.12.0354>

-Stourm, V., Neslin, S. A., Bradlow, E. T., Breugelmans, E., Chun, S. Y., Gardete, P., ... & Venkatesan, R. (2020). Refocusing loyalty programs in the era of big data: a societal lens paradigm. *Marketing Letters*, 31, 405-418.

-Tahal, R., & Formánek, T. (2020). Reflection of GDPR by the Czech Population. *Management & Marketing. Challenges for the Knowledge Society*, 15(1), 78-94.

-Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*, 38, 105454.

-Thobani, S. (2019). Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente. *MEDIA LAWS*, 131-147.

-Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166.

-Wirth, C., & Kolain, M. (2018). Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data.

-Zemler, F., & Westner, M. (2019, August). Blockchain and GDPR: Application scenarios and compliance requirements. In *2019 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 1-8). IEEE.

-Zieglmeier, V., & Loyola Daiqui, G. (2021). GDPR-compliant use of blockchain for secure usage logs. In *Evaluation and Assessment in Software Engineering* (pp. 313-320).

-Zou, W., Huang, S., Xie, J., Dai, X., & Chen, J. (2019). A reinforced generation of adversarial examples for neural machine translation. *arXiv preprint arXiv:1911.03677*.