Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 3, 231-243 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Waterfall: Salto Collazo. High-Level Design of Tokenomics

Sergii Grybniak[1], Yevhen Leonchyk[2], Igor Mazurok[2], Oleksandr Nashyvan[1], Alisa Vorokhta[*,2]

[1]*Institute of Computer Systems, Odesa Polytechnic State University, Shevchenko av. 1, Odesa, 65044, Ukraine*

[2]*Faculty of Mathematics, Physics and Information Technologies, Odesa I.I. Mechnikov National University, Dvoryans'ka St 2, 65082, Odesa, Ukraine*

ARTICLE INFO

Article history:
Received: 28 February, 2023
Accepted: 20 May, 2023
Online: 25 June, 2023

Keywords:
Tokenomics
Incentive System
Distributed Protocol
Transaction Fee
Directed Acyclic Graph
Blockchain

ABSTRACT

This article explains the fundamental principles of the economic policy that are integrated into the decentralized public platform Waterfall. The platform has a DAG (Directed Acyclic Graph) based system architecture and is designed to develop decentralized applications and financial services. The main goal of this work is to create a favorable environment that incentivizes positive behavior from each network participant and from the system as a whole. Economic leverages ensure general equilibrium to provide an optimal data replication ratio, attack protection, and affordable transaction fees. Although this model of tokenomic is designed explicitly for the current version of the Waterfall platform named Salto Collazo, the presented approaches possess the potential to be applied across a broad spectrum of decentralized public platforms, owing to their inherent transparency and a set of tuned parameters.

1. Introduction

1.1. Problem Statement

This paper is an extension of work originally presented in the proceedings of the IEEE International Conference on Blockchain, Smart Healthcare, and Emerging Technologies [1] and presents a high-level economic design of decentralized public networks such as blockchains, blockDAGs (Directed Acyclic Graphs consisting of linked blocks), etc.

The emergence of blockchain technology has transformed modern society and businesses, primarily thanks to the attributes of its transparency, tamper-proof safety of data, and logical consistency [2]-[4]. However, its subpar network performance and exorbitant commissions make it unsuitable for many enterprise-class applications. On the other hand, DAG technology is considered the next generation of blockchain due to its optimized validation mechanism, high scalability, efficient provenance, and multiparty involvement [5]-[7]. A DAG-based architecture can provide the necessary functions to develop a variety of decentralized finance (DeFi) services [8], [9], including payment systems, non-fungible tokens (NFTs), web3 gaming [10], new solutions in logistics [11] and real estate sector [12], identity documents [13], and e-voting services [14]. The success of this approach depends on the establishment of ad-hoc economics for a decentralized storage system that is both high-speed and scalable, while also ensuring low-cost transaction fees. The primary focus of this article is on the core economic principles embedded within the Waterfall DAG-based protocol [15] and its efficacy in fulfilling these specific requirements.

1.2. An Exposition of the Waterfall Platform: A Short Survey

Waterfall is a decentralized platform designed for developing a variety of decentralized applications (Dapps). The platform features high scalability and is built on DAG technology, a distributed ledger system that differs from traditional blockchain technology in that it does not rely on a single chain of blocks. Instead, DAG technology uses a graph-like structure, enabling the platform to process transactions in parallel, without the need for central authority.

Waterfall leverages a fast finality Proof-of-Stake (PoS) [16] consensus algorithm to ensure the integrity of its transactions. The platform is built to rely on Coordinating and Sharding networks, enabling a significant volume of transactions via parallelized block generation. The Coordinating network processes transactions and communicates with the Validator network to ensure consensus on the validity of each block. Meanwhile, the Sharding network

*Corresponding Author: Alisa Vorokhta, Dvoryans'ka St 2, 65082, Odesa, Ukraine, +380951641320 & alisa.vorokhta@stud.onu.edu.ua

divides the workload across multiple nodes, improving the platform's overall scalability.

Each node in the Waterfall network is composed of 2 components: a Coordinator and a Validator, representing their respective roles within the system. The Sharding network is responsible for processing incoming transactions and ensuring their validity. Transactions are combined into blocks that refer to other blocks to form a DAG. Information about the created blocks enters the Coordination Network for structure linearization and finalization based on consensus. The blockchain of the Coordinating network records data on the finalization of blocks in all shards.

Overall, the Waterfall platform is a highly-scalable smart contract platform. DAGs in decentralized technologies facilitate scalability, addressing one of the key challenges faced by such systems, and allow for the parallel processing of transactions, which can be verified and confirmed quickly and efficiently. This feature of the platform enables it to process a high volume of transactions per second, making it a viable option for decentralized applications.

The Waterfall consensus protocol Gozalandia [17] has established a time-based system to ensure efficient and secure block production. This timeline is composed of distinct time intervals, including slots, epochs, and eras. The Coordinating network assumes responsibility for registering Validators and assigns roles such as block producers, committee members, and leaders during the commencement of each epoch. In addition, the Coordinating network maintains information regarding the validated blocks generated on the Sharding network. The honest producer is required to include links to all the known tip-blocks of the DAG to its created block. Furthermore, the Coordinating network performs ordering and finalization of the distributed ledger, enhancing the synchronization and overall network security.

The Waterfall platform incorporates and refines the most advantageous properties of Ethereum 2.0 [18], augmenting its performance and extending its functionality. The platform's inherited coin serves as a primary digital asset within the network, facilitating the transfer of transactions and governance voting, executing smart contracts, and providing for the creation of auxiliary tokens, thereby creating an ecosystem with the potential for mutually beneficial interaction among all its components. Nonetheless, the structure of the DAG platform requires new approaches to tokenomics and economic incentives, as traditional mechanisms may be incompatible or insufficient to support the platform's decentralized nature and ensure its sustainable growth. Therefore, the Waterfall team must continually research and implement new solutions to empower its users and incentivize positive behavior, thereby promoting the longevity and stability of the system.

1.3. Tokenomics Strategies: Achieving Sustainable Development in Decentralized Systems

Tokenomics is a fundamental concept in decentralized systems that leverages economic incentives to encourage desired behaviors from participants, such as users, developers, and Validators [19]. The goal is to create a self-sustaining and self-regulating ecosystem that maximizes benefits for all stakeholders. Tokenomics involves the use of native tokens or coins that serve as the currency of the decentralized network and facilitate transactions and interactions within the system. A well-designed tokenomics model can incentivize positive actions, such as network participation, governance voting, and contribution to the development of the network. It can also disincentivize malicious behavior by imposing penalties for non-compliance with network rules and regulations. Additionally, tokenomics can facilitate the effective allocation and use of existing and new resources on the network, resulting in a variety of affordable services for users. Therefore, a robust and balanced tokenomics model is crucial for the successful operation and growth of public decentralized networks [20], [21].

The concept of Waterfall tokenomics is a set of economic principles and mechanisms designed to support the growth and functionality of distributed networks, with a particular emphasis on DAG structures. Waterfall tokenomics has specific goals aimed at creating economic conditions that promote scalability, speed, security, and reliability.

One of the primary objectives of Waterfall tokenomics is to establish economic conditions that enable the network to expand to a size that provides an optimal data replication coefficient and a maximum speed of mempool synchronization. This objective is especially critical for networks that utilize edge networking, which entails a high volume of transactions that must be processed and propagated efficiently.

Another important goal of Waterfall tokenomics is to promote fast finality [22], which plays a pivotal role in facilitating payment systems and decentralized applications (Dapps). Fast finality ensures that transactions are secure and reliable by preventing any alteration or reversal once a transaction is confirmed.

It is worth noting that the DAG structure of the network presents unique challenges and vulnerabilities that differ from those of traditional blockchain architectures. Therefore, Waterfall tokenomics must provide proper protection and security in intimate collaboration with the technical network architecture.

In summary, the concept of Waterfall tokenomics is a vital economic framework for distributed networks, with an emphasis on DAG structures. Its goals are aimed at creating economic conditions that promote scalability, speed, security, and reliability, and it plays a crucial role in supporting payment systems and Dapps. Finally, it must work closely with the technical network design to ensure appropriate protection against possible attacks.

The vertices in bold are spine blocks in Figure 1. These blocks precede all other blocks in their slots after linearization. We used methods of statistical analysis and simulation to study the probability of successfully executed attacks (considered below) and the degree of damage caused by them. This allows us to evaluate the effectiveness of developed countermeasures and analyze the statistical properties of the acquired graph.

The set of rules and guidelines that govern the network economics is implemented through software that encompasses all the essential features required for its operation. These economic rules are autonomously enforced and transparently visible to the general public. This feature increases user confidence in the platform and makes it more resilient. Additionally, there must be mechanisms in place to adapt specific rules dynamically to changing situations. This approach ensures that the network's ability to sustain desirable behavior over its entire lifespan, fostering overall economic equilibrium and systematic development aligned with the network's objectives. Achieving this goal poses a considerable challenge within the scope of this endeavor.

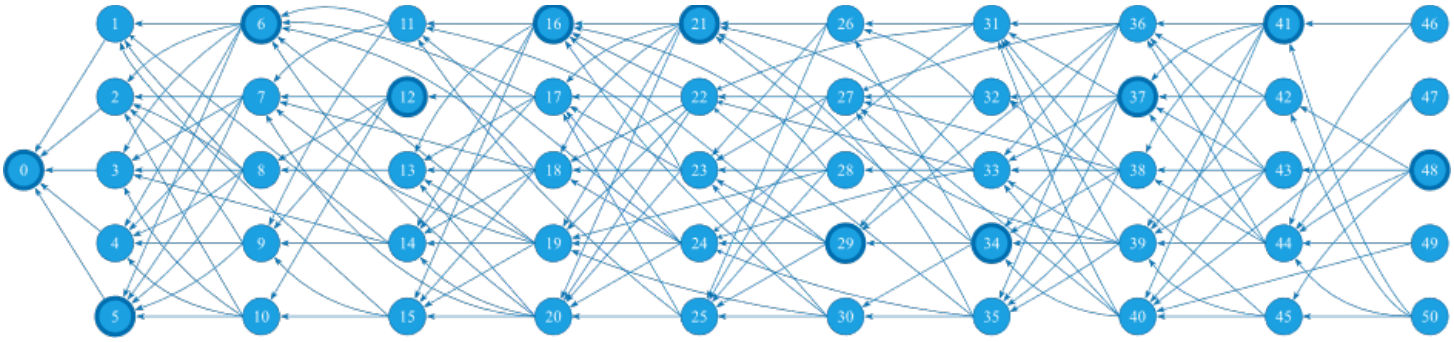

Figure 1: An example of a starting fragment of a DAG network created using simulation

2. Related Works

The evolution of economic blockchain models has been a subject of intense research in recent years. The choice of consensus protocol has important implications for the economic model of a blockchain network [23], [24]. For example, the development of Proof-of-Work (PoW) decentralized networks like Bitcoin and Ethereum 1.0 represents a significant milestone in the history of blockchain technology (as evidenced by numerous studies including [19], [25], [26]). In a PoW system, nodes compete to solve cryptographic puzzles, with the first node to solve the puzzle being rewarded with a new block and the corresponding amount of cryptocurrency. This creates an economic, incentivizing network node participation and contributes to the overall security of the system. This type of system is known for its simplicity but has also been criticized for its high energy consumption and vulnerability to 51% attacks. Early models were characterized by relatively simple economics compared to more modern PoS models, which have since emerged as a promising alternative that can potentially enhance network maintenance [27]. PoS systems use a different mechanism to achieve consensus, whereby nodes are selected to create new blocks based on their ownership of a certain amount of cryptocurrency. In such models, network participants are incentivized to hold a certain amount of cryptocurrency as collateral, and transactions are validated based on the stake they hold. Compared to PoW models, PoS models are less energy-intensive and less vulnerable to 51% attacks.

Overall, the development of economic blockchain models has been driven by the need to incentivize network participants to act in ways that contribute to the overall health and sustainability of the system. While early models like PoW and PoS have been successful in achieving this goal, research is continued on new consensus algorithms and economic models that can potentially offer even better performance and security. For example, there are also approaches to achieving consensus that have been proposed in the literature, such as the use of Byzantine Fault Tolerant (BFT) algorithms [28], DAGs [29], and Delegated Proof-of-Stake (DPoS) [30]. However, these approaches often require ad-hoc methods to incentivize network participants [31], which can make them more difficult to implement and manage.

Despite the differences among these models, they all share a common goal: incentivizing network participants to behave in a way that benefits the network as a whole. This challenge requires a deep understanding of game theory [32], [33] and the underlying properties of blockchain technology. By designing economic models that reward good behavior and penalize bad actors, these models aim to ensure the smooth and sustainable functioning of decentralized networks.

In response to modern demands, various economic models have been developed to support PoS-based systems ([34], [35], [36]). These models aim to address the challenges faced by decentralized systems, such as decreasing transaction costs, increasing transaction frequency, and reducing finalization time. Additionally, a few approaches have been proposed by incorporating economic principles into BFT-like consensus mechanisms, these systems aim to achieve a balanced internal economy that aligns with specific objectives ([37], [38], [39]).

After analyzing related works, it has been revealed that one of the primary challenges facing decentralized systems is the need to decrease transaction costs, increase transaction frequency, and reduce finalization time. This is particularly important for the mass adoption of Distributed Ledger Technology (DLT) in real-world applications. In Messari's report for 2023 [8], one can find a comprehensive examination of current prospects and significant trends in the development of tokenomics.

Therefore, our aim is to develop a tokenomics model that addresses these challenges, with a focus on limiting the increase in transaction fees while maintaining the Worker's economic viability, which includes blockchain Validators and block producers. To achieve this, we propose a flexible and transparent architecture that can be easily modified with a set of adjustable parameters. This is especially important for emerging public platforms, as they must be able to successfully meet formation requirements.

However, important to highlight that most of the already existing economic models are developed for established systems such as Ethereum 2.0 [18]. As such, there is a need for new and innovative models that take into account the specific requirements and limitations of emerging decentralized systems.

The Waterfall model incorporates and enhances the most favorable aspects of Ethereum tokenomics. Furthermore, it presents notable benefits owing to its novel consensus protocol [17] and horizontal scaling, with subnetworks necessitating economic incentives [40]:

- **Dynamic adjustment.** A mechanism for dynamic adaptation of system parameters is in place to ensure optimal network behavior, particularly by automatically adjusting the optimal number of Workers. This approach enables the system to attain self-sufficiency throughout its complete lifespan.
- **Low transaction fees.** In various scenarios, the architecture and tokenomics of the system are structured to maintain low transaction fees. The protocol scales dynamically with the increasing network load, which leads to the simultaneous publication of more blocks within the same slot and

consequently reduced transaction fees as the system expands. Thus, transaction processing during peak times remains efficient, while the number of pending transactions in the transaction pool remains low.

- **Supporting high transaction throughput.** The Waterfall platform achieves high transaction throughput via the use of system-scalable DAG-based block structures. These structures allow multiple blocks to be published simultaneously, forming a DAG that provides finality for all transactions, as long as the blocks do not conflict with each other. In recent intermediary lab tests, our protocol demonstrated the ability to process up to 3,600 transactions per second. The tokenomics model effectively supports this architecture.

In the world of public blockchain networks, the presence of corrupt and malicious nodes leads to an environment of complete distrust. To address this issue, a reputation system could be implemented to enhance the security of interactions. Several approaches have been proposed for building a reputation system based on blockchain data, as discussed in existing literature (e.g. [41], [42]).

In [43], a detailed discussion is presented on the reward distribution scheme among honest Workers for their role in block production and validation, as well as on the determination of penalties for faulty Workers, with particular attention paid to the consensus achievement mechanism of the Waterfall platform. The key principles underlying the proposed scheme are that Workers should be rewarded in proportion to the significance of their contributions, and that the penalties imposed on them should outweigh the potential benefits of any malicious actions. The tokenomics of the system is analyzed at a macro level, without delving into the specific functional roles of individual nodes. As such, the proposed approach is independent of any particular PoS-based consensus algorithm that opens up the possibility of its adaptation to a broad range of platforms for macroeconomic design, owing to a multi-parameter configuration.

3. Macroeconomic Design

This section delves into the analysis of the decentralized Waterfall platform from an economic standpoint, using a holistic approach that avoids focusing on the specific behaviors or contributions of individual participants. It covers the platform's governance framework, which includes core principles of network economic policy that shape the interactions of community groups and affect various economic indicators such as cryptocurrency rates, inflation, and deflation. The system architecture and coin circulation are visually represented in Figure 2 and are discussed in-depth later in this section.

3.1. Pre-mining Strategy

In the early stages of a network, the initial coin distribution is a critical element for ensuring system security. As such, a recommended approach is to create a set of N_{opt} Workers at the beginning, each with a fixed stake divided into nodes that share a ledger and IP address. The stake amount is denoted by s coins per Worker, and any increase in the total amount of the stake is achieved solely through the addition of new Workers. This strategy helps to ensure a secure and stable system during the network's initial phase.

Typically, the entire token supply is not immediately available at the outset. Assume α represents the proportion of the current supply (C) to the total staked amount $S_{opt} = s \cdot N_{opt}$. The value of N_{opt} should be determined as the present optimal number of Workers necessary to ensure a secure and efficient network. A restricted number of Workers in a network raises the risk of a majority holding attack. Conversely, a larger total stake results in a decrease in free funds in circulation, which can impede effective network operations. To maintain the desired level of available funds and the optimal number of Workers, it is crucial to uphold the ratio α. In other words if the current supply C is lower than the total stake multiplied by $\alpha(1 - \varepsilon_1)$, a proportional amount of coins is released. Conversely, if the current supply C exceeds the total stake multiplied by $\alpha(1 + \varepsilon_2)$, an appropriate number of Workers is added using the Foundation's funds. ε_1 and ε_2 are relative values, expressed as fractions of the base value α, which define the lower and upper limits of the range respectively. In the first scenario mentioned in the text, the Foundation has the ability to revoke its Workers if they were created using a specific protocol. This means that instead of releasing additional coins into circulation, the Foundation can choose to remove Workers from the system. To ensure that this condition is met and that the system remains in balance, a smart contract is used. This smart contract monitors the balance between the current coin supply and the number of Workers in the system. This balance is adjusted periodically to ensure that it remains within acceptable limits. Determining the optimal values of $\alpha \geq 2$, $\varepsilon_1 > 0$, and $\varepsilon_2 > 0$ to achieve effective and secure network functioning is an unresolved matter that relies on various factors. These factors include the total and current supplies, required available funds, security level, and network operating goals. We consider the initial values of parameters: $\alpha = 2.5$ and $\varepsilon_1 = \varepsilon_2 = 0.25$ as a starting point for the Waterfall case. During the initial stage of the Waterfall platform, it is expected that the foundation will control approximately 2/3 of the total number of tokens in circulation. With the current value of the parameter α, a network capture attack, also known as a majority attack [44], would inflict losses on both the attackers and the attacked parties, making such an attack economically infeasible. As the platform continues to grow and the number of nodes increases, the value of α will decrease accordingly, while maintaining a sufficiently high level to guarantee the platform's security.

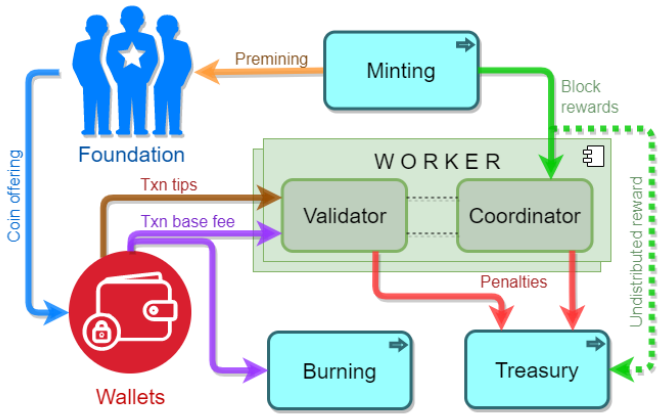

Figure 2: The circulation of coins on the platform

3.2. Understanding the Technical Aspects of Coin Mining and Its Challenges

The proposed tokenomics model incentivizes block production by offering minted rewards for every finalized block in the Coordinating network. This means that new coins will be issued to

compensate Coordinators for ensuring the required security guarantees, which is referred to as "Minimum Necessary Issuance". Earned coins are accrued to Workers every epoch. The annualized minted amount (V) is influenced by the total amount of staked coins (S):

$$V = k \cdot \sqrt{S},$$

where a coefficient k will be subsequently defined. As a result, the maximum annualized return rate (R) is determined as follows:

$$R = V / S = k / \sqrt{S}.$$

This non-linear relationship proposed in [18] implies that a decrease in the amount of staked coins leads to increased incentivization, and vice versa. This balance between the volume of minted coins and network security ensures that all initial stakes, which are initially uniform (although some may be reduced due to penalties), remain proportional, and

$$S = s \cdot N,$$

the coefficient k can be obtained through the desired value of R_{opt} at a certain total stake (S_{opt}) as well as at a certain optimal number of Workers (N_{opt}). In our case, the coefficient k is derived from a condition that the maximum annualized return rate equals R_{opt} with N_{opt} Workers:

$$k = R_{opt} \cdot \sqrt{S_{opt}} = R_{opt} \cdot \sqrt{s \cdot N_{opt}}.$$

Therefore, considering any given number of Workers, we obtain:

$$V = R_{opt} \cdot s \cdot \sqrt{N_{opt} \cdot N},$$

$$R = R_{opt} \cdot \sqrt{\frac{N_{opt}}{N}}.$$

During the initial stages of coin release, the current supply C experiences a rapid surge, necessitating the expansion of the optimal number of Workers to ensure network security. Consequently, the value of N_{opt} should also be substantially increased:

$$N_{opt} = \frac{C}{\alpha \cdot s}.$$

The coefficient k and the annual minted amount V are crucial factors that need to be adjusted to ensure the proper release of all coins. Recalibration is necessary to keep the system efficient and engaging for new Workers by increasing the rewards available for minting. However, if the number of Workers in the network exceeds a certain threshold, the platform may overpay for security, leading to inflation that could have detrimental effects on the tokenomics of the system. To prevent this, the value of α, which represents the percentage of total minted coins allocated for the development fund, should not be too low. It is important to note that the number of coins yet to be released can be approximated by subtracting the current amount in the releasing account (C) from the total coin supply. This approximation provides valuable insights into the state of the system and informs decisions about adjusting the minting process to optimize its performance. The overall rate of return (R), may be reduced due to the occurrence of faults or malicious behavior by certain Coordinators. Despite this, honest Workers who make investments at the outset can expect to receive rewards of approximately R_{opt} per year. This represents the minimum return rate that can be achieved by honest Workers. To illustrate this concept, we present Figure 3, which depicts the maximum annualized return rate that stakeholders can earn as block rewards under varying conditions of the number of Workers and different values of R_{opt} and N_{opt}. With the expansion of the Worker count, the return rate diminishes; however, the rewards could potentially be augmented by tips resulting from heightened network activity.

When evaluating the reward for a produced block in a blockchain network, it is crucial to consider various factors that contribute to the overall value of the reward. Two critical elements to consider are the annualized minted amount and the slot times. The annualized minted amount refers to the total number of tokens that will be minted during the year, assuming the network continues to operate at its current capacity. This value is essential because it determines the overall supply of tokens, and therefore impacts their value in the market. Additionally, the annualized minted amount can affect the incentive structure for network participants, such as block producers, who may receive a portion of the newly minted tokens as a reward. The slot times, on the other hand, refer to the time it takes to produce each block in the network. In most blockchain networks, a new block is produced at regular intervals, which are determined by the slot times. The shorter the slot time, the more blocks can be produced within a given timeframe, and the higher the potential rewards for block producers. To evaluate the reward for a produced block, these two factors must be taken into account. By multiplying the annualized minted amount by the slot times, we can calculate the value of each block produced in the network. This information is essential for understanding the incentives and rewards available to network participants and can inform decisions regarding the network's governance and economic policies. Overall, the evaluation of block rewards is a critical aspect of blockchain network design and operation. By considering various factors such as the annualized minted amount and slot times, we can ensure that the network is functioning efficiently and providing appropriate incentives to all participants. To determine the minted reward for a generated block, one can consider the values of the annualized minted amount and slot times. Let i represent the slot number within the Coordinating network. Then the annualized number of blocks:

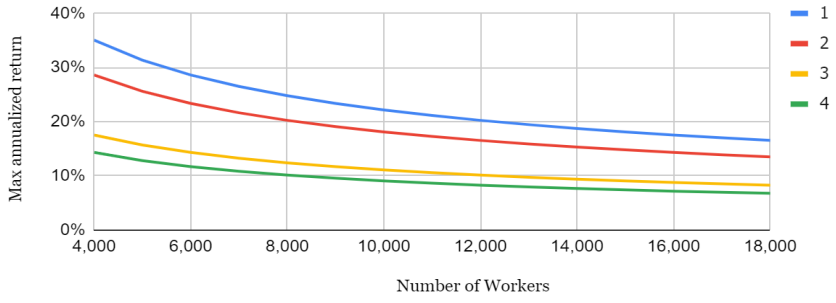

Figure 3: The maximum annual return rate of Workers (case 1 with R_{opt} = 0.20 and N_{opt} = 12,288; case 2 with R_{opt} = 0.20 and N_{opt} = 8,192; case 3 with R_{opt} = 0.10 and N_{opt} = 12,288; case 4 with R_{opt} = 0.10 and N_{opt} = 8,192)

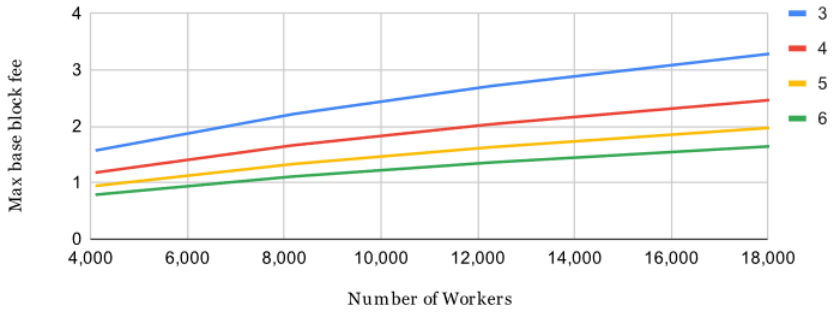

Figure 4: The maximum base block fee (W_i^s) with N_{opt} = 8,192 Workers, R_{opt} = 0.20, s = 32,000 coins, p = 1, t_i^s = 4 sec, and b_i = 3...6 blocks per slot

$$B_i^c = \frac{T}{t_i^c},$$

where t_i^c is its time in seconds, and constant $T = 60 \cdot 60 \cdot 24 \cdot 365.25$ represents the number of seconds per year.

Consequently, the reward that is minted per block in the i-th slot in the Coordinating network is:

$$W_i^c = \frac{V}{B_i^c}.$$

It is important to note that the total sum over all slots of the Coordinating network per year (Y) is equivalent to:

$$\sum_{\forall i \in Y} W_i^c = V \cdot \sum_{\forall i \in Y} \frac{t_i^c}{T} = V.$$

Further, the amount W_i^c is divided among the Committee leader and members who have created i-th block in the Coordinating network.

3.3. Understanding Base Transaction Fees

In the context of DLT, any transaction included in a block requires the payment of a base transaction fee. This fee is determined based on a mechanism similar to that used for obtaining a minted reward and depends on the annualized minted amount. Let i be the slot number of the Sharding network. Then the annualized number of blocks:

$$B_i^s = \frac{T \cdot b_i}{t_i^s}, \quad W_i^s = \frac{V}{B_i^s}.$$

where the number of blocks per slot in the Sharding network $b_i > 1$ and t_i^s is its time in seconds.

It is worth noting that if the block number and time slot remain constant throughout the year, the annual number of blocks B^s can be obtained by a simple calculation. By summing up the values of slots and blocks across the Sharding network for the entire year, we arrive at the following expression:

$$\sum_{\forall i \in Y} \sum_{j=1}^{b_i} W_i^s = V \cdot \sum_{\forall i \in Y} \frac{t_i^s}{T} = V.$$

And then, a base transaction fee in i-th slot is defined as:

$$f = \frac{G}{G_{max}} \cdot W_i^s \cdot p,$$

where G represents the required gas amount to process the transaction, G_{max} denotes the maximum permissible gas amount per block, and $p > 0$ is a price multiplier. The cumulative sum of all base transaction fees across the j-th block of the i-th slot:

$$F_{ij} = \sum_{txns} f \leq W_i^s \cdot p.$$

In the case of a regular transaction, the proportion:

$$\frac{G}{G_{max}} = \frac{1}{10{,}000}$$

ensures quite low base fees, even for quite high values of the multiplier p.

Clearly, the value of W_i^s depends on the current number of Workers as well (see Figure 4).

3.4. Coin Burning Procedure

The act of permanently removing a certain number of coins from circulation to reduce the current supply is commonly referred to as "coin burning." This process is often carried out by sending tokens to an account that can receive them but cannot withdraw them, rendering the coins useless and irretrievable. In the context of Ethereum, the Ethereum Improvement Proposal EIP-1559 has introduced a mechanism whereby base transaction fees are burned [45], effectively improving the tokenomics of the platform. However, Validators are permitted to retain the tips from transactions, providing an additional incentive for their participation. An alternative approach to coin burning involves deducting a fixed percentage of each transaction fee and sending it to an inaccessible account, thereby reducing the total supply of tokens over time. This method has been adopted by several blockchain platforms as a means of managing their token supply and improving their tokenomics [46]. Our economic model follows a similar approach, wherein the base transaction fee is divided into two portions using a burning multiplier denoted as $l \in [0; 1]$:

$$f = l \cdot f + (1 - l) \cdot f.$$

The first component is burned but the second one is left for a Validator. It is clear that l not equal to 1 increases the total Workers' rewards and reduces the burned coin amount. The value of l can be the same for all blocks and changed only by the network voting, or it depends on a particular block or the reputation of a block producer to incentivize it.

One of the possible approaches is discussed in [47]:

$$l = l_0 + (1 - l_0)(1 - q(b))$$

for each block b, where $q(b) \in [0; 1]$ is a measure of its referential structure "quality" (here 1 means the best quality), and the parameter l_0 not less than 0 signifies the minimum proportion of the transaction fees that are subjected to burning. To make this happen, the DAG topology created by honest Validators was examined and their typical behavior was described in [43]. Therefore, the function *q(b)* could be built on the basis of comparing the existing referential structure of block *b* with its theoretical reference (ideal) version. Incentivizing the encouragement of the establishment of a well-structured system of references can be highly beneficial in preserving the accuracy and safeguarding the confidentiality of data within the Sharding network. This practice serves as a means of incentivization, motivating users to adopt and adhere to a standardized method of referencing information, which in turn promotes better organization and security throughout the network.

Furthermore, in this system, all penalties incurred are effectively removed from circulation. A Worker who holds less than 50% of his/her initial stake forfeits the privilege to validate and produce blocks in the future, irrespective of any rewards he/she may have received. Any violation of the system's rules or any misbehavior on the part of a Coordinator or a Validator attracts an automatic penalty, which includes the following scenarios: (1) a Coordinator, acting as a committee member, deliberately omits a series of votes; (2) a Coordinator, acting as a committee member, issues conflicting messages or double votes; (3) a Coordinator, acting as a block producer, fails to create a block in the Coordinating network; (4) a Coordinator, acting as a block producer, generates more than 1 block within the same slot of the Coordinating network; (5) a Validator produces more than 1 block in the same slot of the Sharding network, and these blocks are subsequently confirmed in the Coordinating network; (6) a Coordinator submits an invalid proof of any of the aforementioned offenses. Penalties accumulate; for example, if three blocks are produced instead of one, the penalty doubles.

All Coordinators collectively make decisions based solely on the information provided by the coordinating ledger, without requiring any additional network consensus. If a whistleblower identifies an offense, they record proof of it in a block when it is their turn to produce one. Therefore, there is no need for an extra consensus mechanism. For instance, in case 4, a whistleblower, who detects two blocks generated in the same slot receives 50% of the penalty amount as a reward. In case 6, another Coordinator can report malicious activity by providing a reference to such a block, doubling the penalty imposed on such a leader in comparison to their potential benefits.

3.5. Treasury

In the blockchain ecosystem, a treasury refers to a reserved pool of digital assets that serve a specific purpose (e.g. [48], [49], [50]). This allows stakeholders to make decisions, usually through a decentralized governance process, on how to allocate funds. The blockchain treasury can be used for a wide range of purposes, e.g. to finance the development of new features or improvements in network protocols, to cover the costs associated with operational expenses, to fund marketing initiatives aimed at increasing awareness and mass adoption of decentralized services, to acquire other projects, for charitable activities, etc. Replenishment of the treasury can be carried out through various means. The most common methods include coin issuance and the accrual of a portion of transaction fees. Additionally, penalties and donations in the form of cryptocurrency can also be used to fund treasuries.

In the Waterfall platform, if committee members fail to vote in the *i*-th slot, they will not receive their share of the minted reward $W_i^{c,}$ and a slot leader will not receive the reward for including such missed votes in the block. Any undistributed funds are accumulated every epoch in keeping with the overall system design and can be used to replenish the treasury. In addition, a whistleblower that reports misconduct is rewarded with 50% of the penalty amount, with the other half being transferred to the treasury. If a Validator is unable to synchronize before producing their block and relies on outdated blocks, their reward may be diminished, and the resulting losses are also added to the treasury account.

The main advantage of this approach is that financing the treasury at the expense of undistributed funds and penalties does not create any additional inflationary pressure on the system. Under the consensus protocol assumptions [17], the percentage of faulty Workers does not exceed one-third of their total number. Therefore, the number of funds transferred to the treasury cannot exceed one-third of all minted coins, since at least two-thirds of Workers are well-behaved and fully rewarded. This design ensures a balanced and stable system, promoting fairness and transparency for all participants.

4. Examining Attacks on Tokenomics

Waterfall is a public decentralized and open-source peer-to-peer platform, which means that any individual or group can participate in the network, regardless of their motivations or intentions. Unfortunately, this open nature also makes the network vulnerable to bad actors who may choose to deviate from network protocols or even commit malicious acts against other platform participants.

To better understand these threats, we must first define what we mean by an "attack". In this context, an attack refers to any set of actions that results in a violation of the correct operation of the entire system or its components, leading to a deterioration in technical and economic indicators. However, not all attacks are created equally. Some may cause minor disruptions or receive insignificant benefits for a particular network participant, while others can result in irreversible violations and a complete disruption of the platform. In the case of Waterfall, we are particularly interested in attacks that are aimed at the economy of the platform and/or carried out with the help of economic leverage. These types of attacks leverage the financial incentives and structures of the platform to achieve malicious goals. They can take many forms, including, but not limited to, double-spending, Sybil, majority attacks, and other types of manipulation or exploitation.

Given the importance of economic incentives and structures in the functioning of tokenomics networks like Waterfall, it is very important to categorize these attacks based on the amount of damage or potential damage they can cause. Doing so can help us better understand the risks associated with different types of attacks and inform strategies for mitigating those risks. Ultimately, the goal is for the platform to remain secure, stable, and reliable for all involved.

Our next step is to classify attacks according to the extent of damage or potential harm they can inflict. This ranges from minor gains made by certain network participants at the expense of others, to severe violations that may lead to the complete disruption of the platform and irreversible consequences.

4.1. Typology of Node and User Behavior

In the context of the platform, users can be classified into three distinct groups based on their behavioral patterns. The first group comprises users who always abide by the network protocols without exception. The second group consists of users who seek opportunities to increase their income or decrease their expenses by flouting the rules, such as by altering the software. The third group is composed of users who engage in activities that harm the network as a whole or the other users, ultimately leading to financial losses for those involved.

Both the second and third groups of users can act either individually or collectively, forming homogeneous or mixed subgroups. For instance, users from the third group might bribe members of the second group to carry out an attack. While users who inadvertently violate the protocols due to hardware or software failures do not intentionally collude, they may still act synchronously for various reasons. Such users will also be classified under the third group, as they are not seeking to gain any benefit by violating the rules.

4.2. Reputation System

One promising indicator of reliable Worker performance is the number of earned tokens, which can be easily tracked using data from the blockchain ledger. This approach avoids the need for complex calculations that could overburden the network. Notably, we focus only on a "positive" reputation system, as a negative reputation system could be circumvented by a misbehaving Worker who could create a new account and start afresh (known as "zeroing").

It is worth highlighting that, in our scenario, each Worker starts with an equal stake. Consequently, those Workers who are more productive, particularly in block production, earn a higher income. However, the current approach can lead to an advantage for those Workers who joined the network earlier. Moreover, a Worker's productivity and efficiency may fluctuate over time. To address these concerns and ensure that node reputations are continuously updated, a depreciation mechanism can be implemented, such as a weighted moving average of rewards over several eras. This approach considers only tokens earned within a recent timeframe, ensuring that the most up-to-date information is used to determine a Worker's reputation.

The reputation system we propose can have broader applications beyond tracking Worker performance. For example, it could be utilized in peer-to-peer node interactions to prioritize communication with established nodes with a strong reputation. Moreover, we envision offering additional incentives and benefits to Workers with exceptional reputations as a means of motivating and rewarding their high level of performance.

4.3. Principles for Countering Economic Attacks

The principles for countering economic attacks on a network must be carefully considered to ensure maximum economic benefit to all users who comply with network rules. A unique Nash equilibrium [51] should be established in which it is most beneficial for all users to follow network protocols honestly and refrain from attacking the system. To achieve this, a thorough analysis of the system's functioning must be undertaken, taking into account the best rational behavior of malicious users. The behavior of users in the second group, who seek to increase their income by breaking the rules, must be rendered ineffectual in the absence of external funding for attacks.

It is also essential to estimate the cost of possible attacks by representatives of the third group, which actively disrupt the network to the detriment of individual users' economic interests. Network protocols should be designed to offset any damages caused by network disruptions with the necessary amount of funds. It should be noted that it is impossible to prevent attacks entirely in the operation of any public platform. The very concept of PoS assumes that by investing a certain amount of funds, a group of people gains control over a decentralized platform (a majority attack) [45].

To mitigate the impact of attacks on the network, protocols should be established to detect and promptly respond to any malicious activity. A mechanism for punishing attackers should also be implemented, which could involve the confiscation of tokens or other economic sanctions. Additionally, the use of staking mechanisms could provide incentives for network participants to act honestly, as they would possess a personal interest in the prosperity of the network. In summary, it is essential to build a network that is resistant to economic attacks and promotes honest behavior by all participants.

4.4. Economic Attack Vector

The Waterfall consensus protocol [17] plays a crucial role in countering attacks, including economic attacks. A consensus protocol has to have the following two features [52]:

- **Liveness:** once a valid block becomes available to network nodes, it will be appended to the distributed ledger, and all valid transactions will be accepted after a certain period of time;
- **Safety:** the consensus decision is consistent among all honest nodes.

In other words, the consensus protocol coordinates the current state of the distributed ledger to provide the necessary economic information to all network participants. Then, the directions of typical attacks and possible prevention mechanisms within the framework of high-level design are considered.

Double-spending is an attack where a certain number of coins is used multiple times [53]. A situation may arise where a transaction for spending the same amount is published in different blocks of the DAG network. To enhance security, a new PoS-oriented blockDAG linearization algorithm was presented in [17]. Here, security means that if an honest Worker proposes an order of a blockDAG part in its turn, all other honest Workers will also

approve the same block order to be further finalized. Therefore, after running the linearization and finalization procedure, only the first transaction is considered correct, and later conflicting transactions are ignored.

A common argument against PoS is that it favors the rich over time and reduces the rewards for those who start with fewer coins, the so-called **Rich-Get-Richer** problem [54]. To a greater extent, this is inherent in systems with a high financial entry threshold. Rich stakeholders receiving more income have the opportunity to increase their presence in the network by creating new nodes.

On the Waterfall platform, the number of Workers is given preference, setting a low financial entry threshold. Therefore, having earned even a relatively small amount, a new Worker can be created, thereby increasing future earnings. Additionally, there is an opportunity to generate income without staking by providing processing power for the operational platform. One can create a network node and, e.g., for a monthly fee, deploy Workers at the request of other users.

Nothing-at-stake is a security issue in PoS-based systems where nodes have no financial risks to support or generate mutually exclusive proposals (e.g. voting for different blockchain forks, producing a certain amount of blocks per slot) to gain extra benefits [55]. Such malicious behavior can disrupt the consensus, reducing system performance.

With Waterfall, as with most other public platforms, there are penalties for the misbehavior of Workers, and simultaneous validation/production of conflicting blocks/messages leads to the loss of locked coins [43]. Based on data recorded in the ledger, these penalties are levied automatically. Since data in the ledger is always the same and available, all honest Workers can make judgments based exclusively on that information without overloading the network or reducing its performance.

Maximal Extractable Value (MEV) attacks can occur on cryptocurrency platforms when a block producer is able to incorporate its own transactions and reorder users' transactions in the block to maximize its profit.

In traditional financial systems, this type of attack is only available to a narrow circle of people who have privileged/priority access to confidential information of financial institutions, since any algorithmically predictable behavior in finance is a vulnerability that can be exploited, for example, to conduct arbitrage [56]. However, in public platforms, such information is available to all users, primarily due to the openness and variety of smart contracts that implement financial instruments. Thus, there are ample opportunities for block producers to implement MEV. Strictly speaking, these attacks are not carried out directly on decentralized platforms but are seen in DeFi services deployed on their basis [9].

By definition, MEV provides a way to counteract this type of threat directly, eliminating or significantly reducing the possibility of block producers' influence on the order of transactions written to the ledger. Here, DAG-based protocols have certain advantages over blockchain-based systems [57]. In the future, we plan to implement additional MEV-resistant features into our consensus protocol.

5. Modeling Tokenomics

5.1. Inflation and Deflation

In traditional economics, the monitoring of currency issuances enables transparency in overseeing different financial aspects. Within tokenomics, an expansion and contraction in the circulation of coin supply are referred to as inflation and deflation, respectively. The distinction between minted and burned coin quantities is a significant network economic attribute, which can automatically be calculated in real-time. Therefore, the predetermined algorithm of the coin issuance should be carefully examined and simulated, considering specific transaction workloads that impact burned coin quantities as base transaction fees. We have examined several scenarios to gain a more comprehensive understanding of the economic dynamics within the Waterfall platform. Therefore, we were able to optimize and protect it.

Consider a value represented by the occupancy of j-th block of i-th slot in the Sharding network (see subsection 3.3):

$$r_{ij} = \frac{F_{ij}}{W_i^s \cdot p} \in (0; 1].$$

If $r_{ij} = r$ remains constant over a year, then the amount of burned coins (U) over a year can be calculated as follows:

$$U = \sum_{\forall i \in Y} \sum_{j=1}^{b_i} F_{ij} l \; = \sum_{\forall i \in Y} \sum_{j=1}^{b_i} r_{ij} W_i^s p \; l = rVpl.$$

If the slot time and the number of blocks are constant throughout the year, then the number of burned coins can be calculated using the following formula:

$$U = \sum_{\forall i \in Y} \sum_{j=1}^{b_i} r_{ij} \frac{V}{B^s} pl = r_0 Vpl,$$

where r_0 is the average value of r_{ij} across all blocks per year. The annualized burned amount U with a price multiplier $p = 1$ never surpasses the emitted amount V anyway, since $r_{ij} \leq 1$. It is possible to modify the value of p through network voting in the future.

The calculation of the annual inflation rate involves determining the ratio between the difference between the total coin supply and the burned coins ($V - U$) and the current coin supply, which is approximately equal to the constant α multiplied by the total coin supply $\alpha \cdot S$. Figure 5 illustrates several potential scenarios with varying degrees of block occupancy and number of Workers, all of which are based on the assumption of a constant $\alpha = 2.5$, a price multiplier $p = 1$, and a burning multiplier $l = 1$.

As more transactions take place, more coins are burned as transaction fees, which can help offset the inflationary effects resulting from the creation of new coins. Obviously, there is no inflation when $r_0 \cdot p \cdot l = 1$, and the deflation process can be observed when $r_0 \cdot p \cdot l > 1$. Thus, the parameters p and l can be used to select the scenario of the economic dynamics. For example, when $l = 1$ and $p = 2$, at the level of 50% average block occupancy, the inflation rate equals zero (Figure 6). However, with a higher block occupancy corresponding to more transactions per second), a deflationary trend can occur.

The economic model can exhibit both inflationary and deflationary tendencies, as the number of coins burned in the Sharding network depends on its workload, and is closely tied to the number of coins minted in the Coordinating network. To identify the optimal configuration of parameters for a given set of

Figure 5: The relationship of the upper limit of the inflation rate per year from the block occupancy r_0 with $p = 1$ and $l = 1$

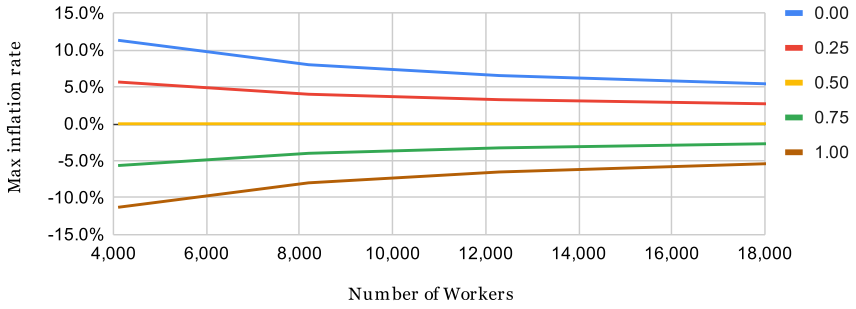

Figure 6: The relationship of the upper limit of the inflation rate per year from the block occupancy r_0 with $p = 2$ and $l = 1$

network specifications, it is possible to leverage both structural and mathematical modeling techniques, with a defined objective function tailored to the specific strategy pursued in platform development. By carefully fine-tuning the values of key parameters, it may be possible to achieve a balanced economic system that supports sustainable growth and stability over time. Ultimately, the ability to achieve the desired economic outcomes will depend on a range of factors, including the prevailing market conditions, the actions of network participants, and the overall level of demand for the platform's services.

5.2. Faulty Work Simulating

In [43], the theoretical underpinnings of the Waterfall incentive system were elaborated in detail, including the distribution of rewards and the imposition of penalties, all designed to achieve a state of general economic equilibrium. The key principle governing the calculation of penalties is that they should be significantly higher than any potential gains that could be realized through a potential attack on the system. To achieve this, a multiplier of $\lambda \geq 1$ is used to amplify the scale of the penalties. One of the core objectives of the simulation was to determine an optimal value λ that would be suitable for different scenarios of Worker misconduct. The overarching goal of this process is to ensure that faulty or idle Workers are eventually excluded from the consensus, thus preventing the accumulation of a critical mass of defective nodes that could hinder consensus. At the same time, temporary equipment failures or inadvertent shutdowns of Workers should not result in a permanent ban from the system.

The following scenarios for Worker failures were considered:

1. h_{online} hours working reliably and $h_{offline}$ hours off;
2. the shutdown duration distributed according to the normal law with mean t_{mean} and standard deviation t_{std};
3. the probability of failure when performing one or another action is $P \in (0; 1)$.

During the experiments, a fixed time interval was used, and different values were assigned to the various parameters mentioned above. After this interval, Workers were removed from participation in the work, and the topology of the resulting DAG was analyzed. Based on the findings, it was determined that a relatively high value of $\lambda = 100$ should be set for penalty rates. For instance, failing to produce two consecutive blocks or submitting conflicting messages during the voting process incurs a penalty 100 times greater than the corresponding reward. In addition to the penalty, the Worker's participation in the network is temporarily suspended for the current and next eras so that the necessary equipment settings can be made. This helps to preserve the value of the Worker's stake, as subsequent failures would cause the stake to fall below the 50% threshold, leading to permanent exclusion from the network. While the Worker is suspended, they do not take part in committee work or block production, which in turn reduces the percentage of faulty nodes in the network.

6. Implementation and Experimental Study of the Waterfall System

The development of the Waterfall system required a comprehensive approach, starting with the experimental study of its functioning. Initially, we focused on a small but increasing number of nodes, where we studied the system's behavior using simulation tools. As we gained more insights, we moved on to conduct full-scale tests in a test network with a smaller number of nodes.

Currently, we have implemented the main initial elements of our protocol and are conducting load experiments using t3.small and t3.medium AWS Servers with a 2-core CPU and 2 or 4 GB RAM respectively [58]. These tests are being conducted to evaluate the tokenomics model's ability to serve the Waterfall

Table 1: Network load test results

Number of				Loading							
				Idling		1st day			3rd day		
Servers	Nodes	Workers	Total	CPU	RAM	CPU	RAM	Spending	CPU	RAM	Spending
t3.medium	32	32	1024	1.91	0.59	2.51	1.3		2.2	1.8	
	32	16	512	2.32	0.69	2.32	1.3	3.44 USD	0.56	2.2	1.25 USD
	8	32	256	1.91	0.59	2.51	1.3				
	8	16	128	2.32	0.71	2.32	1.3		0.53	2.66	2.33 USD
	8	8	64	2.32	0.51	2.32	1.3				
t3.small	8	8	64	1.91	0.51	2.21	1.3				

platform with high transaction throughput. We are optimistic about the system's performance since it has demonstrated the desired behavior.

However, to ensure optimal performance, we continuously check the values of the system parameters and study further optimization opportunities. Our approach has been focused on caution and thoroughness to ensure that the Waterfall system is developed to the highest standards and is capable of serving its intended purpose.

The outcome of the test that measured the amount of work a server can handle (refer to Table 1) indicated that there was no meaningful connection between the CPU or RAM load and the number of Workers running on a single server. Concurrently, there is a shift in the load structure over time. At the same time, there is a shift in the load arrangement over time. By the third day of operation, the influence of software adaptation mechanisms was observable. A part of the data necessary for work was cashed in shared memory. As a consequence, the processor's burden was reduced by 75-77%. Only when the amount of available memory allowed for saving the necessary information for all the Workers running on the node was such a significant reduction in CPU load achieved. Also, an experiment was conducted to evaluate hashing of data with insufficient RAM for 32 Workers. Despite the 38% increase in memory consumption, only 12% savings in CPU resources were observed. Observations show that doubling the minimum required amount of RAM results in more than four times less load on the processor on the third day of operation. This, combined with automatic optimization of communications and the corresponding reduction in traffic, leads to an average 64% reduction in server maintenance costs at Amazon Web Services prices since the third day.

The table demonstrates that entry to the Waterfall network is more accessible compared to other popular networks of a similar nature. A lower entry threshold is made possible by less demanding software and a lower computational load, with everything else being equal.

One can notice that the test network with fewer nodes requires more costs per server. This is due to the overall cost of maintaining the TestNet infrastructure. When distributing these costs over 32 nodes, we naturally get a smaller amount compared to 8 nodes. In this regard, we make a comparative analysis of expenses only within the rows of the table, but not between different rows.

The cost of user-nodes with a transfer rate of 2 standard transactions per second amounted to 28.7 and 35.2 coins per day, on average, where the optimal number of Workers N_{opt} was equal to 8,192 and 12,288 respectively $R_{opt} = 0.2$.

The implementation of the Waterfall System provides for the possibility of deploying several autonomous Workers on each node with a common ledger and a pool of transactions. Having as many Workers as possible in one node provides an economic benefit, but it negatively affects network decentralization. Their number must have an upper boundary, taking into account technical limitations. A large number of Workers deployed on a single device may not have adequate time to create and process blocks. This leads to a shortfall in rewards and the imposition of penalties.

7. Conclusion

The multishard DAG-based platform Waterfall is a sophisticated yet efficient amalgamation of diverse pre-existing and unique solutions. Tokenomics serves as the tool to maintain coherence among the distinct components and optimize their operations. Although the presented tokenomics framework is tailored for the Waterfall platform, the methods, and approaches outlined in the document could be valuable for creating economic support systems for other decentralized networks.

The conclusions drawn from the article suggest that the general model designed for Waterfall tokenomics can bring about an economic balance that caters to the concerns of all participants within the platform. This equilibrium is achieved while keeping transaction fees at a low level, which is essential for implementing DLTs and smart contracts into applications designed for enterprise-level use. The advantages of this model become apparent when dealing with a high volume of transactions, making the platform more reliable and promoting digital transformation through transparency and trust.

By offering an affordable transaction fee, the Waterfall platform can be utilized for a broad spectrum of services, such as DeFi, IoT, Web3 gaming, digital identity, medical screening systems, and peer-to-peer energy trading, etc. The foundational principles of Waterfall tokenomics align with its DAG-based architecture design, and dynamically adapting macroeconomic mechanisms ensure that the platform performs optimally and sustainably in rapidly changing situations.

Both inflationary and deflationary tendencies can be observed in the economic model depending on initial parameters and further network management. A few possible scenarios of the system evaluation were mathematically simulated and experimentally studied in the testnet.

Future work on Waterfall tokenomics will focus on researching the economic aspects of interactions between various homomorphic Sharding networks, forming transaction fees based on the external exchange rate, voting for economic parameters, and

developing the mechanics required for implementing different incentivization strategies. Additionally, the economic issues of on/off-boarding process will also be explored, and simulations will be conducted to evaluate the effectiveness of various strategies. Overall, the article highlights the potential benefits of Waterfall tokenomics in promoting decentralized technologies and creating a more transparent and trustworthy digital environment.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] S. Grybniak, Y. Leonchyk, R. Masalskyi, I. Mazurok, O. Nashyvan, "Waterfall: Salto Collazo. Tokenomics," 2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health), Bucharest, Romania, 2022, 2022, doi: 10.1109/SmartBlock4Health56071.2022.10034521

[2] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, M. Alshamari, Y. Cao, "A survey on blockchain technology: evolution, architecture and security," IEEE Access, **9**, 61048-61073, 2021, doi: 10.3390/s22145274.

[3] A. T. Sherman, F. Javani, H. Zhang, E. Golaszewski, "On the origins and variations of blockchain technologies," IEEE Security & Privacy, **17**(1), 72-77, 2019, doi: 10.1109/MSEC.2019.2893730.

[4] S. Grybniak, Y. Leonchyk, R. Masalskyi, Igor Mazurok, Oleksandr Nashyvan, Ruslan Shanin "Decentralized platforms: goals, challenges, and solutions," 2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI), 62-67, doi: 10.1109/RTSI55261.2022.9905225.

[5] H. Pervez, M. Muneeb, M. U. Irfan, I. U. Haq, "A comparative analysis of DAG-based blockchain architectures," 12th International Conference on Open Source Systems and Technologies (ICOSST), 27-34, 2018, doi: 10.1109/ICOSST.2018.8632193.

[6] F. M. Benčić, I. P. Žarko, "Distributed ledger technology: blockchain compared to directed acyclic graph," IEEE 38th International Conference on Distributed Computing Systems, 1569-1570, 2018, doi: 10.1016/j.technovation.2023.102711.

[7] Q. Wang, J. Yu, S. Chen, Y. Xiang, "SoK: diving into DAG-based blockchain systems," preprint arXiv:2012.06128, 2020, doi: 10.48550/arXiv.2012.06128.

[8] R. Selkis, A Messari report: Crypto theses for 2023, 2023, https://messari.io/crypto-theses-for-2023.

[9] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, W. J. Knottenbelt, "Sok: decentralized finance (DeFi)," preprint arXiv:2101.08778, 2021.

[10] L. Dam, What is Web3 Gaming? How is it different from Traditional Gaming? 2023, https://ekoios.vn/web3-games-and-traditional-games-comparison.

[11] E. Tijan, S. Aksentijević, K. Ivanić, M. Jardas, "Blockchain technology implementation in logistics," Sustainability, **11(4)**, 1185, 2019, doi: 10.3390/su11041185.

[12] R. M. Garcia-Teruel, "Legal challenges and opportunities of blockchain technology in the real estate sector," Journal of Property, Planning and Environmental Law, 2020, doi: 10.1108/JPPEL-07-2019-0039.

[13] J. Lee, "BIDaaS: Blockchain based ID as a service," IEEE Access, **6**, 2274-2278, 2018, doi: 10.1109/ACCESS.2017.2782733.

[14] N. Kshetri, J. Voas, "Blockchain-enabled e-voting," IEEE Software, **35**(4), 95-99, 2018, doi: 10.1109/MS.2018.2801546.

[15] S. Grybniak, D. Dmytryshyn, Y. Leonchyk, I. Mazurok, O. Nashyvan, R. Shanin, "Waterfall: a scalable distributed ledger technology," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), 1-6, 2022, doi: 10.1109/iGETblockchain56591.2022.10087112.

[16] C. T. Nguyen, D. Thai Hoang, D. N. Nguyen, D. Niyato, H. T. Nguye, E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities," IEEE Access, **7**, 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[17] S. Grybniak, D. Dmytryshyn, Y. Leonchyk, I. Mazurok, O. Nashyvan, R. Shanin, "Waterfall: Gozalandia. Distributed protocol with fast finality and proven safety and liveness," IET Blockchain, 1–12, 2023, doi: 10.1049/blc2.12023.

[18] K. Lau, Ethereum 2.0. An introduction, Crypto.com, 25 p, 2020.

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

[20] L. W. Cong, Y. Li, N. Wang, "Tokenomics: dynamic adoption and valuation," The Review of Financial Studies, **34**(3), 1105-1155, 2021, doi: 10.1093/rfs/hhaa089.

[21] G. A. Pierro, H. Rocha, "The influence factors on Ethereum transaction fees," IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 24-31, 2019, doi: 10.1016/j.bcra.2022.100074.

[22] E. Anceaume, A. D. Pozzo, T. Rieutord, S. Tucci-Piergiovanni, "On finality in blockchains," preprint arXiv:2012.10172, 2020, doi: 10.4230/LIPIcs.OPODIS.2021.6.

[23] P. Freni, E. Ferro, R. Moncada, "Tokenomics and blockchain tokens: a design-oriented morphological framework," Blockchain: Research and Applications, **3**(1), 2022, doi: 10.1016/j.bcra.2022.100069.

[24] O. Letychevskyi, "Creation of a self-sustaining token economy," The Journal of The British Blockchain Association, **5**(1), 2022, doi: 10.31585/jbba-5-1-(4)2022.

[25] J. A. Kroll, I. C. Davey, E. W. Felten, "The economics of Bitcoin mining or, Bitcoin in the presence of adversaries," 12th Workshop on the Economics of Information Security, 2013, doi: 10.36484/liberal.662625.

[26] S. Davidson, P. de Filippi, J. Potts, "Economics of blockchain," Public Choice Conference, 2016, doi: 10.2139/ssrn.2744751.

[27] L. W. Cong, Y. Li, N. Wang, "Blockchain and tokenomics," COJ Reviews & Research, **1**(1), 2018, doi: 10.1093/rfs/hhz007.

[28] A. Yakovenko, Solana: a new architecture for a high performance blockchain v0.8.13, Whitepaper, 2018, https://solana.com/solana-whitepaper.pdf.

[29] W. Silvano, R. Marcelino, "Iota Tangle: a cryptocurrency to communicate Internet-of-Things data," Future Generation Computer Systems, **112**, 307-319, 2020, doi: 10.1016/j.future.2020.05.047.

[30] J. J Reuben, A. Joshua, "Blinkchain - a regulation friendly proof-of-speed blockchain v0.1," available at SSRN 4267038, 2022.

[31] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, "SoK: consensus in the age of blockchains," 1st ACM Conference on Advances in Financial Technologies, 183-198, 2019, https://arxiv.org/pdf/1711.03936.pdf.

[32] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. Liang, D. I. Kim, "A survey on applications of game theory in blockchain," preprint arXiv:1902.10865, 2019, doi: 10.13868/j.cnki.jcr.000287.

[33] K. Iyer, C. Dannen, "Crypto-economics and game theory. Building Games with Ethereum Smart Contracts," Apress Berkeley, 129–141, 2018, doi: 10.1007/978-1-4842-3492-1_6.

[34] Z. Chang, W. Guo, X. Guo, Z. Zhou, T. Ristaniemi, "Incentive mechanism for edge-computing-based blockchain," IEEE Transactions on Industrial Informatics, **16** (11), 7105–7114, 2020, doi: 10.1109/TII.2022.3163550.

[35] S. Motepalli, H. Jacobsen, "Reward mechanism for blockchains using evolutionary game theory," IEEE 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 217-224, 2021, doi: 10.1109/BRAINS52497.2021.9569791.

[36] A. Salau, R. Dantu, K. Morozov, S. Badruddoja, K. Upadhyay, "Making blockchain validators honest," 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), 267-273, IEEE, 2022, September, doi: 10.1109/BCCA55292.2022.9921952.

[37] I. Mazurok, V. Pienko, Y. Leonchyk, "Empowering fault-tolerant consensus algorithm by economic leverages," ICTERI Workshops, 465-472, 2019, doi: 10.1049/blc2.12023.

[38] Y. Amoussou-Guenou, A. Pozzo, M. Potop-Butucaru, S. Tucci-Piergiovanni, "Correctness and fairness of tendermint-core blockchains", preprint arXiv:1805.08429, 2018, doi: 10.4230/LIPIcs.OPODIS.2018.16.

[39] P. Chafe, A. Mashatan, A. Munro, B. Goncalves, D. Cameron, J. Xu, Dandelion network whitepaper, 22 p, 2022, https://dandelionnet.io/wp-content/uploads/2022/09/dandelion_whitepaper.pdf.

[40] O. Antonenko, S. Grybniak, D. Guzey, O. Nashyvan, R. Shanin, "Subnetworks in BlockDAG," 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), 1-6, doi: 10.1109/iGETblockchain56591.2022.10087101.

[41] R. Dennis, G. Owen, "Rep on the block: a next generation reputation system based on the blockchain," IEEE 10th International Conference for Internet Technology and Secured Transactions (ICITST), 131-138, 2015, doi: 0.1109/ICITST.2015.7412073.

[42] Z. Zhou, M. Wang, C. Yang, Z. Fu, X. Sun, Q. Wu, "Blockchain-based decentralized reputation system in E-commerce environment," Future Generation Computer Systems, **124**, 155-167, 2021, doi: 10.1016/j.future.2021.05.035.

[43] I. Mazurok, Y. Leonchyk, S. Grybniak, O. Nashyvan, R. Masalskyi, "An incentive system for decentralized DAG-based platforms," Applied Aspects of Information Technology, **5**(3), 196–207, 2022, doi: 10.15276/aait.05.2022.13.
[44] W. Li, S. Andreina, J. Bohli, G. Karame, "Securing proof-of-stake blockchain protocols," Data privacy management, cryptocurrencies and blockchain technology, 297-315, Springer, Cham, 2017, doi: 10.1007/978-3-319-67816-0_17.
[45] T. Roughgarden, Transaction fee mechanism design for the Ethereum blockchain: an economic analysis of EIP-1559, 2020, doi: https://timroughgarden.org/papers/eip1559.pdf.
[46] Solana Foundation, Transaction fees, 2022, https://docs.solana.com/ru/transaction_fees.
[47] R. Masalskyi, "DAG Distributed Ledger Modeling," The 1st Student Sci. Conf. of Joint Res, Cooperation between Odesa I.I. Mechnikov National University and Huaiyin Institute of Technology, 171–175, 2022.
[48] Polkadot, Understanding the Polkadot treasury, Medium, 2021, https://polkassembly.medium.com/understanding-the-polkadot-treasury-816821ffc589.
[49] Cardano, Monetary policy, Cardano docs, https://docs.cardano.org/explore-cardano/monetary-policy.
[50] NEAR, Ecosystem treasury DAO, 2021, https://gov.near.org/t/near-ecosystem-treasury-dao/2946
[51] J. F. Nash Jr., "Equilibrium points in n-person games," Proceedings of the national academy of sciences, **36**(1), 48-49, 1950, doi: 10.1515/9781400884087-007.
[52] L. Lamport, "Proving the correctness of multiprocess programs," IEEE Transactions on Software Engineering, SE-**3**(2), 125–143, 1977, doi: 10.1109/TSE.1977.229904.
[53] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, A. Sarower, "Blockchain attacks analysis and a model to solve double spending attack," International Journal of Machine Learning and Computing, **10**(2), 352-357, 2020, doi: 10.18178/ijmlc.2020.10.2.942.
[54] Y. Huang, J. Tang, Q. Cong, A. Lim, J. Xu, "Do the rich get richer? Fairness analysis for blockchain incentives," International Conference on Management of Data, 790-803, 2021, doi: 10.1145/3448016.3457285.
[55] D. Rose, E. Machery, S. Stich, M. Alai, A. Angelucci, R. Berniūnas, E. Buchtel, A. Chatterjee, H. Cheon, I. Cho et al., "Nothing at stake in knowledge," Noûs, 224–247, 2019, doi: 10.1111/nous.12211.
[56] K. Qin, L. Zhou, A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?" 2022 IEEE Symposium on Security and Privacy (SP), 198-214, 2022, May, doi: 10.1109/SP46214.2022.9833734.
[57] D. Malkhi, P. Szalachowski, "Maximal extractable value (MEV). Protection on a DAG," preprint arXiv:2208.00940, 2022, doi: 10.48550/arXiv.2208.00940.
[58] Waterfall, Waterfall testnet 3. Test 9, 2022, https://waterfall.foundation/testnet_3_test_9.