European Proceedings of
Computers and Technology
EpCT
www.europeanproceedings.com
e-ISSN: 2672-8834
DOI: 10.15405/epct.23021.2

HMMOCS 2022
International Workshop "Hybrid methods of modeling and optimization in complex systems"

MATHEMATICAL MODEL OF BILLING FOR THEOOL DAO

Alexey V. Nenashev (a)*, Rostislav S. Oleshko (b)
*Corresponding author

(a) Samara State Technical University, 244, Molodogvardeiskaya st., Samara, Russia, alexvlnenashev@gmail.com
(b) Samara State Technical University, 244, Molodogvardeiskaya st., Samara, Russia, THEOOL LLC, 159V-13 Stara Zagora st., Samara, Russia, info@the-ool.net

Abstract

The paper discusses the current state and development prospects of Web3 and decentralized autonomous organizations in comparison with Web 2.0. The problems of interaction between participants of decentralized autonomous organizations within the virtual space and integration of a decentralized autonomous organization with the outside world through network inducement algorithms are raised. The possible implementation of such interactions is considered on the example of TheOoL DAO. The functionality of TheOoL DAO is briefly disclosed, aimed at ensuring the security of participants in a decentralized autonomous organization, the complete suppression of the "digital footprint" they leave. The classes and forms of financial relationships of participants in a decentralized autonomous organization are determined. A mathematical model of billing in the serverless secure Internet TheOoL DAO on smart contracts is presented as an integral part of the TheOoL cloud computing and data storage subsystem. This system provides guaranteed automatic payment for services for the provision of computing power for storing and processing data or performing computing tasks and, at the same time, performs the functions of fully automatic control over the execution of the terms of a smart contract by the owners of these capacities. The presented billing system blocks the transfer of personal information between the customer and the service provider, which ensures the privacy and security of the execution of smart contracts.

Keywords: Web3, Web 2.0, decentralized autonomous organization, billing, blockchain

https://doi.org/10.15405/epct.23021.2
Corresponding Author: Alexey V. Nenashev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2672-8834

1. Introduction

One of the most popular and discussed concepts for the development of the Internet has recently become the concept of Web3 (Filipčić, 2022; Goel et al., 2022; Wang et al., 2022). It involves building a new generation Internet based on distributed ledger technology as a peer-to-peer decentralized network with integrated decentralized finance. This distinguishes it from Web2.0 (Newman et al., 2016), in which the main computing and financial capabilities of the network are centralized in the hands of GAFAM (Miguel de Bustos, 2018; Miguel de Bustos & Izquierdo-Castillo, 2019) and large financial capital, owning centralized digital finance systems (Gautier & Lamesch, 2021). Since all members of the Web3 network are legally equal but differ in their needs and the functions they perform through the network, they come together to manage interactions in the form of so-called decentralized autonomous organizations (DAOs) (Mattila et al., 2022; Schillig, 2021; Wulf, 2021). DAO participants are equal subjects. For them, the interaction rules are defined by a set of software scripts that determine the functionality allowed in a particular DAO. The integrity and immutability of such a set of scripts is ensured by the properties of a distributed ledger (Bamakan et al., 2020; Nakamoto, 2007; Zhang & Lee, 2020), namely, the inability to fake previously made entries.

Thus, any serverless Internet system implemented in the Web3 concept can be organizationally defined as a DAO in which the participants, being mutually independent, are divided into customers and performers. The key service absolutely necessary for its existence in such an Internet, as in Web2.0, remains the provision of computing resources for its functioning. The difference lies in the fact that in Web2.0 many customers enter into a direct contract for the provision of services with one of the large centralized performers, while in the Web3 concept such contracts are concluded automatically between equal participants, one of which has a need for resources, and the second has them. surplus. Any member of the network can become such an executor without the slightest restrictions, except for those imposed by predefined scripts of this particular DAO. Initially, DAO scripts are abstract in nature, since they do not have a specific customer, contractor, subject and terms of the contract. From the moment when the listed parameters are defined the corresponding smart contract (an instance of the script with specifically defined execution parameters, sealed with electronic signatures of the parties) is registered in the DAO distributed registry.

2. Problem Statement

The problems of interaction are resolved at the organizational level in the virtual space of the DAO, but the problems of managing the functioning of computing resources at the technical level and the behavior of their owners in the real world, namely the level of availability and quality of the resources provided, remain unaccounted for. Since performers within the DAO are not affected by the usual legal and financial motivations, you should consider creating such motivations directly within the network. In fact, executors, being absolutely free in their actions, can provide access to resources with low reliability, low performance, or withdraw them from circulation at any time without any legal consequences for themselves. Which, accordingly, may lead to a violation of the availability or integrity of the data and computing processes that they contracted to serve under the smart contract.

https://doi.org/10.15405/epct.23021.2
Corresponding Author: Alexey V. Nenashev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2672-8834

3. Research Questions

To solve this problem the study considered the following questions:

- What is TheOoL DAO from an organizational and technical point of view?
- On what principles is the TheOoL DAO network organized?
- What classes of financial interactions exist in the TheOoL DAO network?
- How is it possible to build billing algorithms in the TheOoL DAO network in compliance with the principles of network organization and respect for the interests of the parties to financial interactions?

4. Purpose of the Study

The search for answers to the questions posed should lead to such an organization of the billing tool (Hunter & Thiebaud, 2003), which will allow, on the one hand, to take into account the quality of service (QoS) requirements of the customer, and on the other hand, provide the performer with sufficient motivation for rigorous maintaining high QoS (Shaban et al., 2012; Swathi et al., 2020). The third, but no less important, function of the DAO billing system should be competitive and transparent pricing.

5. Research Methods

The authors used universal scientific research methods, as well as methods of system analysis.

5.1. TheOoL DAO: Functional Purpose and Principles of Organization

Internet TheOoL.net (Nenashev & Khryashchev, 2019; Nenashev et al., 2021; TheOoL White Paper, 2022) is a decentralized application (DApp) (Marchesi et al., 2020; Wu, 2019) that implements DAO algorithms. It combines the functions of private web hosting, a secure audio-video-text communication system and a payment system, as well as an environment for developing and executing custom DApps. DAO TheOoL at the user level implements two main principles (Nenashev et al., 2021; TheOoL White Paper, 2022): abstraction of the user and user data from the technology of their processing, storage and delivery; management of information and its distribution solely by the user-owner of this information. The implementation of the first principle, on the one hand, excludes the identification of the ownership of information by a specific user by the owners of the technical infrastructure where information is directly stored and processed, and on the other hand, it excludes the possibility of disrupting the operation of this infrastructure by user actions. The second principle is aimed at ensuring the complete anonymity of the network participant, suppressing his digital footprint.

On a technical level, TheOoL.net is a peer-to-peer network of data storage, processing and access nodes that provides users with private network space and full control over their digital footprint. Network communication in this network provides affordable, high-speed cloud services for secure distributed computing and cloud storage, as well as tools for automatic price regulation within the system (Nenashev & Khryashchev, 2019; Nenashev et al., 2021; TheOoL White Paper, 2022). Designed primarily to build ultra-secure geographically distributed corporate automated information systems with low information

https://doi.org/10.15405/epct.23021.2
Corresponding Author: Alexey V. Nenashev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2672-8834

security and infrastructure maintenance costs (Nenashev & Khryashchev, 2019), TheOoL.net can be used by private network participants as a private network space.

5.2. TheOoL DAO: Classification of Participants and Analysis of Activities

TheOoL.net defines three classes (roles) of participants: providers of computing resources (performers), content owners/providers (customers), and content consumers (readers).

The Contractor provides for a fee the computing resources belonging to him, while providing the QoS level required by TheOoL.net rules.

The customer places the content in the TheOoL cloud on the computing resources of the performers. At the same time, it determines the QoS requirements, the content retention period, and the number of content backups. When placing content, the customer determines the order of access to content by readers: exclusive (m), group (g) (with the ability to edit (rw) or without it (r) or public (p), paid (c) or free (f).

The exclusive storage mode assumes a level of security comparable to storing data on a personal computer offline. In this mode, access to content and information about the existence of content in the TheOoL network is available only to the customer. Group access, regardless of the mode (rw or r), provides security comparable to working in an isolated local network, with the exception of controlling access to the work nodes of readers - members of an admitted group, if they are outside a certain controlled zone. In this case, the effectiveness of the subsystem of protection against unauthorized access built into TheOoL nodes is determined solely by the personal discipline of readers. The public order of access allows access to read content to any reader in the TheOoL network but does not allow you to determine the customer - the owner of the content, nor does it allow the customer or other persons to collect information about content readers.

A certain legal relationship (smart contract) is established between readers and the content owner within TheOoL DAO, which determines the rules and order of access to content: access time parameters, access mode [r/rw; c/f]. If a public access order is established, an open contract with access mode [r; f] signed by the customer. For readers, the smart contract in the modes [r/rw; f] is advisory in nature and does not require their consent at the time of its generation. Smart contracts in [r/rw; c] require the mandatory consent of all parties. The customer forms [r/rw; c] and sends it to many potential readers as an offer, which they can accept at their discretion during the validity period of the smart contract. Simultaneously with the conclusion of a contract between the customer and his readers, when placing content, a smart contract is formed between the customer and a group of performers.

5.3. TheOoL DAO: Classification of Financial Interactions

Internet TheOoL.net assumes that the services of performers and access to content within the framework of smart contracts must be paid for and some commission must be charged from each payment. Since integration with an external payment service can lead to a number of vulnerabilities, an internal payment tool was implemented that allows billing and payments to be made directly inside the secure space of TheOoL DAO. The methods for constructing a mathematical model for billing the TheOoL network are determined by the architecture of this network, its purpose and the mathematical model of the network, which is a queuing network designed to process large sets of structured data in real time (Nenashev et al., 2021).

https://doi.org/10.15405/epct.23021.2
Corresponding Author: Alexey V. Nenashev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2672-8834

For the purposes of this study, 2 main classes of financial interactions (smart contracts) can be defined in TheOoL network: 1. Reader-customer interaction; 2. Interaction between the customer and the performer. From the point of view of building a billing system, interactions of the first class are of no interest, since the parameters of contracts and the order of their execution are determined by counterparties voluntaristically. Therefore, we will focus on the interactions of the second class, the rules of which completely determine the algorithms of the network.

6. Findings

6.1. Mathematical Model of TheOoL DAO Billing

Billing in TheOoL DAO begins with the fact that the contractor forms an offer towards an arbitrary customer (public offer) when registering the contractor's hardware node. The performer node in the network characterizes the rating $\varepsilon_j(t_i)$, which is the ratio of the availability functions $d\big(t_i, d(t_{i-1})\big)$ and performance $r\big(t_i, \overline{V_j}\big)$ of the node:

$$\varepsilon_j(t) = r\big(t_i \overline{V_j}\big) / \, d\big(t_i, d(t_{i-1})\big) \tag{1}$$

Here $t_i = t_{i-1} + \delta,\ i = \overline{0 \dots k}$ is a discrete moment of time in the interval, $[t_0, t_k]$, t_0 is the moment of registration of the executor node in the network, t_k is the moment of exclusion of the executor node from the network, δ is a discrete time step, $\overline{V_j}$ is the vector of available node resources at time t_i taking into account the queue of jobs (Nenashev et al., 2021), $j = \overline{1 \cdots \xi_c}$ is the sequence number (identifier) of the node among ξ_c available performer node system.

At time t_0 the primary rating of the node $\varepsilon_j(t_i)$ is performed. The network requirements for the availability factor are determined by the equation $0{,}9 \pm 0{,}05 \le d(t_i, d(t_{i-1}))$. At the time of network initialization, the availability factor is $d(t_0) = 1$, and then it is determined by the functional:

$$d\big(t_i, d(t_{i-1})\big) = \begin{cases} 1,\ i = \overline{0 \dots 100} \\ d\big(t_i, d(t_{i-1})\big),\ i > 100 \end{cases} \tag{2}$$

If the availability parameter is below the expected values for 50 evaluation cycles, the performer node will be forcibly removed from the network.

After being included in the network, each node sets a calculated rating and forms a pool of public offers to use its resources in one configuration or another. Thus, a vector of prices for the use of the computing resources of the node $\bar{C}_j^c$ will be formed, which contains the minimum prices acceptable for the owner of the node. Each coordinate $\bar{C}_j^c$ is equivalent to the coordinate $\overline{V_j}$, in other words, the sets of coordinates of these vectors are equivalent: $\left|\bar{C}_j^c\right| = \left|\overline{V_j}\right|$. Additionally, each executor node is assigned a queue of unaccepted works $\psi_j(t_i)$ and based on $\overline{V_j}$ the maximum length of the queue of unaccepted works $\varphi_j \ge \left|\psi_j(t_i)\right|$ (Nenashev et al., 2021). From the public offers of the executor nodes $P_j(t_i) = \left\{\varepsilon_j(t_i), \bar{C}_j^c, \overline{V_j}, \psi_j(t_i), \varphi_j\right\}$, taking into account (1) and (2), a set of K public offers for the provision of computational resources available to the customer at time t_i:

https://doi.org/10.15405/epct.23021.2
Corresponding Author: Alexey V. Nenashev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2672-8834

$$K = \begin{Bmatrix} P_1(t_i) \\ \dots, \\ P_{\xi_c}(t_i) \end{Bmatrix} \tag{3}$$

The set K remains relevant until the end of the cycle and is updated at time t_{i+1}.

If it accepts an offer from a node owned by a specific contractor, the contractor receives a reward from this customer through the TheOoL payment subsystem. As an address for receiving payment for performing computational work, the network uses the identifier of the node (j), which belongs to a particular performer $\Lambda_c = \{\omega_c, \Omega_c, \Xi_c\}$, here $\omega_C = \{skey, pkey, UID\}$ is the identifier of the key $skey$, public key $pkey$ and network identifier UID, which is also the main address for receiving rewards, $\Omega_c = F(\omega_C \Xi_c)$ - a set of pseudo addresses for accruing rewards generated for each j-th node belonging to the performer from the set $\Xi_c \in [1, \xi_c]$. When receiving income from the execution of offers $P_j(t_i)$, an abstract movement of funds $j \to \omega_c^j,\ \omega_c^j \in \Omega_c$ is recorded in the blockchain of the built-in payment system TheOoL, but in fact, the movement $j \to \omega_c$ is performed, which is verified by a group of 3 randomly selected nodes consensus, which confirm the legitimacy of debiting from j account "nowhere" and crediting to account ω_c "nowhere". Thus, information about the owner of the executor nodes is not available for external analysis, except for the fact that a particular ω_c address receives rewards from owning unknown nodes in the set $[1, \xi_c]$ (due to the presence of such incoming transactions).

The customer, for his part, places in the TheOoL network a computational task (content) $L_m = \{l_1^m, \dots l_n^m\},\ m = \overline{1 \dots \xi_q}$, which is divided by the algorithm of the subscriber node into elementary subtasks $l_r^m,\ r = \overline{1 \dots n}$ (Nenashev et al., 2021). Then one sets the network requirements and access parameters $B_m = \{B_1^m, \dots, B_n^m\},\ m = \overline{1 \dots \xi_q}$, determines the maximum acceptable price level $C_m = \{\bar{C}_1^m, \dots, \bar{C}_n^m\}$, $m = \overline{1 \dots \xi_q}$, indicates the lifetime of the computational task in the network T_m multiple of δ and the requirements for QoS by specifying the minimum allowable rating level of the executor node ε_m. Moreover, $|L_m| = |B_m| = |C_m|$. The elementary tasks $w_r^m = \{T_m, \varepsilon_m, l_r^m, B_r^m, \bar{C}_r^m\},\ r = \overline{1 \dots n}$ obtained in this way are connected into the super task $W_m = \{T_m, \varepsilon_m, L_m, B_m, C_m\}$ with a common address for charging and debiting payments m, and the product $T_m \cdot C_m$ determines the rules for their further distribution among subaccounts $r,\ r = \overline{1 \dots n}$ associated with elementary subproblems l_r^m. Then from (3) we select a suitable performer

$$P = \min_{\sum \bar{C}_j^c} \{P_j(t_i) | (\varepsilon_m \geq \varepsilon_j(t_i)) \wedge (\varphi_j \geq |\Psi_j(t_i)|) \wedge \left(\sum \bar{C}_j^c \leq \sum \bar{C}_r^m\right) \wedge \left(\forall B_r^m \leq \forall \bar{V}_j\right)\}$$

For each $w_r^m \in W_m$ we write this w_r^m to the queue of unaccepted jobs of the executor node selected for it $w_r^m \Rightarrow \Psi_j(t_i)$.

At time t_{i+1} the control algorithm generates smart contracts $SK_m = F_{SK}(\{sk_1^m, \dots, sk_n^m\}),\ sk_r^m = F_{sk}(w_r^m, P), r = \overline{1 \dots n}$, where F_{SK} and F_{sk} are predefined scripts of smart contracts for the execution of the customer's computational task and its elementary subtask, respectively. The actual payment (transfer of funds from the customer to the contractor) is performed at the end of each discrete step δ, which allows the contract to be automatically terminated ahead of schedule if the contractor violates the established QoS requirements. In this case, a new executor node is assigned to execute the task.

https://doi.org/10.15405/epct.23021.2
Corresponding Author: Alexey V. Nenashev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2672-8834

The customer, like the contractor, has the identifier $\omega_z = \{skey,\ pkey,\ UID\}$ in which the UID, like the contractor, plays the role of the main address for crediting or debiting payments. The customer transfers funds to this address to pay for the services of contractors from external payment systems through interfaces built into TheOoL payment system. The processing of customer payments related to the execution of tasks set by him in the TheOoL network is carried out through the payment virtualizing entity $\Lambda_z = \{\omega_z, \Omega_{z,} W_z\}$, which contains a set of addresses of existing super contracts W_z and $\Omega_{z,} = F(\omega_z, W_z)$ - a set of pseudo addresses for transferring rewards due to the performers of the m-th contract from the set $W_z \epsilon [1, \xi_q]$. When making payments, the abstract movement of funds $\omega_z^m \to m,\ \omega_z^m \in \Omega_z$, but in fact, the movement $\omega_z \to m$, which is verified similarly to the process of moving rewards to the accounts of performers, which makes it possible to hide the content of the customer's payments from an external observer, except for the very fact of their commission.

7. Conclusion

Thus, the presented billing system ensures the fulfillment of the main declared principles of TheOoL DAO (Nenashev & Khryashchev, 2019; Nenashev et al., 2021; TheOoL White Paper, 2022), excluding the disclosure of the financial activity of network participants without their personal, actively expressed desire. At the same time, it ensures reliable and automatic fulfillment of the obligations assumed by the network participants. Due to the subsystem of QoS (1) ratings embedded in it, the presented billing system motivates the performer to perform his work efficiently and constantly take care of improving his computing power. The availability control function $d(t_i, d(t_i - 1))$ is responsible for quality motivation, since in case of violation of the accessibility requirements, the performer is deprived of the due remuneration. The productivity function $r(t_i, \overline{V_j})$ is responsible for the motivation to increase computing power.

Pricing in the TheOoL network is exclusively market-based and is carried out through the Depth of Offers (3). In the face of a shortage of computing resources, customers can compete for them by raising the price while lowering the rating requirements, which increases the income of performers and motivates them to include additional and more productive computing power in the TheOoL network. The surplus of computing resources allows customers to buy the best capacities at a lower price, which forces performers to compete and squeezes the least quality and/or inefficient performers in terms of revenue/cost ratio out of TheOoL network.

Acknowledgments

The work was commissioned by TheOoL LLC, Samara, Russia and with the assistance of the Foundation for the Promotion of Small Forms of Enterprises in the Scientific and Technical Sphere (Innovation Promotion Fund), Moscow, Russia, contract No. 4716GS1/79594 of 09/13/2022.

References

Bamakan, S. M. H., Motavali, A., & Babaei Bondarti, A. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications, 154*, 113385. https://doi.org/10.1016/j.eswa.2020.113385

Filipčić, S. (2022). Web3 & DAOs: an overview of the development and possibilities for the implementation in research and education. *45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO),* 1278-1283. https://doi.org/10.23919/MIPRO55190.2022.9803324

Gautier, A., & Lamesch, J. (2021). Mergers in the digital economy. *Information Economics and Policy, 54*, 100890. https://doi.org/10.1016/j.infoecopol.2020.100890

Goel, A. K., Bakshi, R., & Agrawal, K. K. (2022). Web 3.0 and Decentralized Applications. *Materials Proceedings, 10*(1), 8. https://doi.org/10.3390/materproc2022010008

Hunter, J. M., & Thiebaud, M. E. (2003). *Telecommunications Billing Systems: Implementing and Upgrading for Profitability.* McGraw-Hill.

Marchesi, L., Marchesi, M., & Tonelli, R. (2020). ABCDE—agile block chain DApp engineering. *Blockchain: Research and Applications, 1*(1-2), 100002. https://doi.org/10.1016/j.bcra.2020.100002

Mattila, V., Dwivedi, P., Gauri, P., & Rahman, M. (2022). Mapping out the DAO Ecosystem and Assessing DAO Autonomy. *International Journal of Computer Science and Information Technology Research, 10*(1), 30-34.

Miguel de Bustos, J.-C. (2018). GAFAM, Media and Entertainment Groups and Big Data. *Les Enjeux de l'information et de la communication, N° 17/3A*(S1), 39-51. https://doi.org/10.3917/enic.hs4.0039

Miguel de Bustos, J. C., & Izquierdo-Castillo, J. (2019). Who will control the media? The impact of GAFAM on the media industries in the digital economy. *Revista Latina de Comunicación Social, 74*, 803-821. https://doi.org/10.4185/RLCS-2019-1358en

Nakamoto, S. (2007). *Bitcoin: A peer-to-peer electronic cash system*. http://bitcoin.org/bitcoin.pdf

Nenashev, A., & Khryashchev, V. (2019). The Economics of Introducing the Peer-to-peer System of Storage and Processing of Protected Information at an Enterprise. *In 2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP)* (pp. 769-772). IEEE. https://doi.org/10.1109/CSCMP45713.2019.8976720

Nenashev, A. V., Tolstenko, A. Y., & Oleshko, R. S. (2021). Model of the peer-to-peer distributed system for securable information storage and processing without traffic prioritization (THEOOL project). *In CEUR Workshop Proceedings* (Vol. 2899, pp. 141-150). https://doi.org/10.47813/dnit-mip3/2021-2899-141-150

Newman, R., Chang, V., Walters, R. J., & Wills, G. B. (2016). Web 2.0—The past and the future. *International Journal of Information Management, 36*(4), 591-598. https://doi.org/10.1016/j.ijinfomgt.2016.03.010

Schillig, M. (2021). Some Reflections on the Nature of Decentralized (Autonomous) Organizations (September 1, 2021). *King's College London Law School Research Paper Forthcoming.* https://doi.org/10.2139/ssrn.3915843

Shaban, M., Noory, R., & Yaseen, D. A. (2012). Billing System Design Based on Internet Environment. *International Journal of Advanced Computer Science and Applications, 3*(9). https://doi.org/10.14569/ijacsa.2012.030934

Swathi, B., Kumar, A., Kumar, I., & Venkat, V. (2020). Implementation of Improved Billing System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 37-41. https://doi.org/10.32628/cseit2062168

TheOoL White Paper. (2022). TheOoL DAO. https://theool.net/doc/TheOoLWhitePaper.pdf

Wang, Q., Li, R., Wang, Q., Chen, S., Ryan, M., & Hardjono, T. (2022). Exploring Web3 From the View of Blockchain. *arXiv, 2022.* https://doi.org/10.48550/ARXIV.2206.08821

Wu, K. (2019). An Empirical Study of Blockchain-based Decentralized Applications. *arXiv, 2019.* https://doi.org/10.48550/ARXIV.1902.04969

Wulf, K. (2021, March 6). A Decentralized Autonomous Organization (DAO) of DAOs. https://doi.org/10.2139/ssrn.3799320

Zhang, S., & Lee, J.-H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, *6*(2), 93-97. https://doi.org/10.1016/j.icte.2019.08.001