Article | Received 13 September 2023; Accepted 3 December 2023; Published 14 December 2023
https://doi.org/10.55092/blockchain20230010

Distributed resource governance on a blockchain

Thomas E. Portegys [1,*], James R. Wolf [2]

[1] Dialectek, DeKalb, USA
[2] School of Information Technology, Illinois State University, Normal, IL USA

* Correspondence author; E-mail: portegys@dialectek.com.

Abstract: This research proposes a novel method for ensuring fair governance of a common resource recorded on a blockchain. It features a self-governing system of stakeholders, managing resources by taking on the roles of auditors and claimants in place of having an overseeing bureaucracy with its accompanying overhead costs. While self-governing can be subject to fraud and collusion, in the proposed governance system, anonymity, a staple of blockchain transactions, is utilized to mitigate these negative effects. This is done by assigning random anonymous auditors to resource claimants. Cheating, along with improper auditing, will result in penalties for both auditor and claimant. Improper auditing consists not only of allowing unlawful resource use but also denying lawful use. The proposed system is a Decentralized Autonomous Organization (DAO) running on a Hyperledger Fabric blockchain. All activities are recorded as immutable public transactions on the blockchain. A simulation and a blockchain game to support the plausibility of the model are presented.

Keywords: resource governance; blockchain; distributed application; anonymity; Hyperledger

1. Introduction

Technology has densely connected people. While we are awash in information, most organizations retain centralized control and authority structures that concentrate power hierarchically. This reflects the divide-and-conquer strategy, with expertise and skilled specialists occupying niches where people collaborate in close contact, featuring high bandwidth, low latency communication.

While a historically successful scheme, drawbacks of a hierarchical organization include opacity to stakeholders not residing in a particular walled garden and often with concomitant inefficiencies, obsolescences, and malfeasance that take root in more entrenched bureaucracies. People tend to become resigned to this eventuality, demonstrated by complacently paying taxes, premiums and dues, dutifully voting, and showing up to board, town, and union meetings, all the while ceding authority to duly appointed representatives. That people are often unable to identify their elected representatives, for example, testifies to the enervating and disengaging effect of having information and responsibility without direct authority and involvement.

While acknowledging the value of full-time experts and specialists, there is also value in allowing organizational stakeholders to exercise some authority in formulating policies, plans, and actions from the perspective of those affected by these things [1]. The customary problem with this approach is that, although stakeholders are motivated for an organization to succeed, they are also outsiders who are neither sufficiently knowledgeable nor available to perform decision-making roles. Technology offers a means to address this issue. Many complex organizations have already moved in the direction of distributed control with great success -- open source teams are an example of this. The key notion is not just offering openness but also real authority; without authority, interest will wane for many. The advantage is more eyes and hands and less expense. The risk is allowing less knowledgeable people to have a say and whether they will defer to experts when it is appropriate.

Frequently, by choice or circumstance, the resources of a group are cast into a common pool. An example of a choice would be to pay a periodic fee for insurance to lessen the financial severity of a car accident. A natural resource such a river is an example of a circumstantial shared pool, the use of which is sometimes framed as a *commons dilemma* [2], in which the short-term selfish interests of individuals are opposed to long-term group interests. A typical way to ensure proper resource usage is through a regulatory organization. Such organizations commonly incur substantial costs to support a bureaucracy and facilities to administrate rules and laws that govern resource usage.

A type of contract is proposed that is a more economical means of achieving fair resource usage by relying on the stakeholders bound to the contract to enforce the rules rather than relying on a special organization to do so. In other words, it is believed that a flattened distributed administration can operate in a more cost-effective way. It is known that self-enforcement ("the honor system") and mutual enforcement can facilitate cheating and abuse through deal-making, conspiracy and secretive behavior. In the proposed contract, anonymity, a staple of blockchain transactions, is employed to reduce side channels used for collaborative cheating, thus fostering mutually beneficial behavior. This is done by assigning random anonymous auditors to a resource claimant. Cheating and abuse, along with improper auditing, result in penalties. Improper auditing consists not only of allowing unlawful resource use but also denying lawful use.

Anonymous online behavior is well-known to have negative consequences, especially when the identities of those involved in behaviors such as trolling and cyberbullying are hidden from view, but the victims are known [3,4]. However, when anonymity is used equitably, it has been found to reduce the negative effects of power and status differences in decision-making groups [5,6]. Of special relevance to this project, Wright and Stepney [7] note that anonymity is widely used in situations where knowledge of individual users could lead to favoritism, discrimination, or collusion (e.g., voting, the marking of exam papers, review of funding applications, and academic peer-review).

Blockchain is an ideal candidate for recording resource transactions since it inherently supports anonymous, distributed, immutable, and public transactions [8]. A blockchain is a distributed database or ledger that is shared among the nodes of a computer network, maintaining a secure and decentralized record of transactions. It guarantees the fidelity and security of data and generates trust without the need for a trusted third party. No individual stakeholder controls the blockchain, and everyone can see the outcome of every transaction. Blockchains also feature smart contracts, which are computer code that resides and runs in the blockchain and provides functional application-specific processing of transactions [9]. These distributed applications are commonly referred to as *dapps* [10].

In the past decade, a number of Decentralized Autonomous Organizations (DAOs) have appeared as smart contracts on blockchains [11], with goals similar to those presented here. Generally, DAOs are member-owned communities without centralized authorities. A well-known example, intended for venture capital funding, was *The DAO*, which amassed 3.6 million ETH in May 2016. ETH is the cryptocurrency of the Ethereum blockchain [12]. Two other prominent examples of DAOs are (1) Uniswap, a decentralized exchange that enables the trading of digital assets, and (2) Yearn.finance, a suite of products in Decentralized Finance (DeFi) that provides lending aggregation, yield generation, and insurance [13]. Riaza and Gnabo [14] have found DAOs to be more efficient than bureaucracies for crypto-asset markets. Our DAO, originally specified by the authors in 2011 [15], predates other DAOs, since the smart contract capability to implement them only appeared around 2014. Our DAO was previously constructed as a Google App Engine [16] cloud service. It has been ported to a smart contract for this project.

DAOs manage resources and typically grant authority over the resources to members according to their wealth as measured by a recognized currency, such as ETH. This can effectively result in a centralized control of resources by a few wealthy members. In contrast, our DAO is egalitarian, with no distinction between members other than the transient roles they play during transactions. The consensus mechanism for most DAOs is voting, meaning all members potentially participate in every transaction. Our DAO chooses an anonymous subset of its members in the roles of auditors to adjudicate a transaction in a more rigorous manner. We believe it is also novel in the way it embodies checks-and-balances to enforce fairness and curtail cheating. This is an ambitious goal: a simulation such as that presented here can only be taken as a hint as to the viability of the system; trials with stakeholders to compare its performance *vs.* a bureaucratic system are required to make a firm evaluation.

DAOs do pose concerns. For one, their legal status remains unsettled. Some jurisdictions may recognize DAOs as legal entities, while others may view them as a type of contract or arrangement. Regardless of its legal status, a DAO may still have to follow other laws and rules, such as those related to taxes, anti-money laundering, and data protection. In addition, a smart contract's code is visible to all, and is difficult to alter once the system is up and running, since any change may be seen as a modification of the contract. A known security hole may thus be left open to exploitation until a consensus is reached as to how and when to fix it.

Other features on the technological landscape that facilitate the proposed organization are the ubiquity and ever-lower latency of online interactions, allowing prompt auditing activity to take place, and the deep reach and rich fidelity of digital information sources, allowing intensive remote verification of resource claims.

In the following sections, the DAO rules, a preliminary simulation, and a Hyperledger Fabric blockchain [17] game to support further investigations are presented.

2. Organizational rules

1) Initially, stakeholders each contribute an amount into a resource pool called a commons. This amount is denoted as Rc_i for stakeholder *i*. The commons thus contains $Rc = \sum Rc_i$. Rc_i is always the same value for all stakeholders, signifying an equal ownership of Rc. In addition, each stakeholder has a personal account denoted by Rp_i. This amount can vary in value.
2) A resource entitlement for claimant *i*, Ec_i, is the evidence supporting a resource claim. For example, an entitlement for a pair of shoes would typically run in the tens of dollars, although fringe cases can run down into a few dollars and up into hundreds or even thousands of dollars. Ec_i is decremented from Rp_i, signifying a loss of resources for the stakeholder.
3) The stakeholder, assuming the role of claimant, uses Ec_i to select a claim amount, Cc_i that will pass auditing and satisfy Ec_i. An amount less than the entitlement might tend to have a better audit outcome, while a greater amount signifies "cheating" that grants resources exceeding the entitlement. Cc_i is selected before any auditors are assigned to the claim and cannot be modified later. Ec_i is not revealed to the auditors as part of the claim.
4) The claim is then assigned a number of random auditors taken from a pool of resource stakeholders. In order to discourage collusion, the claimant and auditors remain anonymous to each other. The number of auditors is also unknown to all. An auditor is allowed to anonymously communicate with the claimant to provide further claim information.
5) An auditor examines the claim evidence to determine a grant amount, Ga_i. To prevent collaborative cheating, Ga_i cannot be greater than Cc_i. The mean of all the auditor grant amounts, $\overline{Ga_i}$, is the amount of resources granted to the claimant ($Gc_i = \overline{Ga_i}$).Rp_i is then incremented by Gc_i, signifying a resource compensation.
6) To promote claimant honesty, if $Gc_i < Cc_i$, a penalty, Pc_i, is subtracted from the grant that is a function of the difference between the claim and the grant ($Pc_i = f\Delta(Cc_i, Gc_i)$). This will steer claimants away from making excessive claims. Pc_i is then added to the commons.
7) To promote auditor honesty, each auditor is penalizedPa_i in proportion to the difference between the auditor's grant and the claim grant ($Pa_i = f\Delta(Ga_i, Gc_i)$). This is meant to discourage both unfair denial and illegitimate generosity to claims. Thus an auditor who colludes with a claimant to grant a large claim runs the risk of penalization by deviating from the grant mean. Pa_i is then added to the commons.
8) Here are three ways to evaluate, or score, the system:
   a. As in the Phase 1 simulation, a measurement of the preference ratio for a competing regulatory *vs.* the distributed system can be used as a score. The regulatory agency

system exacts a processing fee from all stakeholders per claim. At the end of a session, each stakeholder will prefer the system that is more financially beneficial.

b. The standard deviation of the stakeholder resources, $R_i = Rp_i + Rc_i$, can be used as a score. A perfect score is zero, indicating that every entitlement/claim/grant triplet was for the same amount and there were thus no penalties. Cheating, denial of resources or penalties will likely skew the resources of the stakeholders; for example, successful cheaters will have relatively more resources than other stakeholders.

c. A measurement of the depletion of the commons resources. This would be computable from the initial and final commons resources and the total entitlements. If the final commons amount is less than initial amount less the total entitlements, then the commons has been excessively depleted.

9) Optionally, since auditor effort has an expense, the resource pool will be reduced for the time spent by auditors to process claims. This will curtail the excessive use of auditors.

Expected Results

It might be expected that the best long-term strategy would be to grant the probability distribution midpoint amount for every claim. However, in the short term, this will result in grants that statistically vary from the entitled amounts. Stakeholders trade transactional privacy in return for the possibility of lower costs. Having stakeholders alternately take on the roles of claimant and auditor encourages cooperative *tit for tat* behavior [18].

Independent Variables

Possible independent variables to use for evaluation include:

- Commons resource amount.
- Number of stakeholders.
- Average number of auditors.
- Penalty functions.

3. Simulation

A simulation using autonomous software agents as stakeholders was done to better understand the problem space and plausibility of the concepts. The simulation compared a *regulatory agency* system with a proposed *distributed* one. Stakeholders are enrolled in both systems for comparison. Stakeholders pool their resources that they can make claims on. In the regulatory agency system, stakeholders pay a fee to adjudicate claims, ensuring that no cheating occurs. In the distributed system, cheating can happen, dampened by the presence of claim auditors.

A run consists of a number of rounds. In each round, resources are reset to be equally distributed. In the regulatory system, fees are deducted from each member. Then claims are dispersed to a random set of stakeholders. A claim represents an amount that can be lawfully withdrawn from the commons resources. A granted claim increments the resources of the claimant, and equally reduces the resources of all non-claimant stakeholders by an amount that cumulatively adds up to the grant.

In the regulatory agency system, all claims are lawful and granted, since claims are adjudicated by an infallible regulatory agency. In the distributed governance system, all lawful claims are also granted; however, a claim also represents an opportunity to cheat by withdrawing an unlawful amount of resources. Stakeholders have a parameterized tendency to cheat. An auditor is assigned to each claim. The auditor probabilistically detects unlawful claims. If cheating is detected, the claimant is penalized by losing their resources, which are equally distributed to the other stakeholders. If the auditor erroneously allows an unlawful claim, the claim is processed as if it were lawful. Lawful claims are not determined to be unlawful.

After each round, stakeholder resources in both systems are compared. So for example, if there were 5 stakeholders, and 2 of them had more resources in the regulatory system than in the distributed one, then 0.4 (40%) would prefer the regulatory system. At the end of the run, the average regulatory preference across rounds is calculated.

Here is an example round with 5 stakeholders, no claims, and a fee of 1 for the regulatory system:

```
Run regulatory:
Claims:
None
Tabulations:
Stakeholder = 0, assets = 9.0
Stakeholder = 1, assets = 9.0
Stakeholder = 2, assets = 9.0
Stakeholder = 3, assets = 9.0
Stakeholder = 4, assets = 9.0

Run distributed:
Claims:
None
Tabulations:
Stakeholder = 0, assets = 10.0
Stakeholder = 1, assets = 10.0
Stakeholder = 2, assets = 10.0
Stakeholder = 3, assets = 10.0
Stakeholder = 4, assets = 10.0

Preferences:
Stakeholder = 0 prefers distributed (9.0 < 10.0)
Stakeholder = 1 prefers distributed (9.0 < 10.0)
Stakeholder = 2 prefers distributed (9.0 < 10.0)
Stakeholder = 3 prefers distributed (9.0 < 10.0)
Stakeholder = 4 prefers distributed (9.0 < 10.0)
Regulatory preference = 0.0
```

Here is a round with claims (resources can become negative):

```
Run regulatory:
Claims:
Stakeholder = 0, resolution = grant lawful
Stakeholder = 2, resolution = grant lawful

Tabulations:
Stakeholder = 0, assets = 69.0
Stakeholder = 1, assets = -31.0
Stakeholder = 2, assets = 69.0
Stakeholder = 3, assets = -31.0
Stakeholder = 4, assets = -31.0

Run distributed:
Claims:
Stakeholder = 0, resolution = grant lawful
Stakeholder = 2, resolution = grant cheat

Tabulations:
Stakeholder = 0, assets = 50.0
Stakeholder = 1, assets = -50.0
Stakeholder = 2, assets = 150.0
Stakeholder = 3, assets = -50.0
Stakeholder = 4, assets = -50.0

Preferences:
Stakeholder = 0 prefers regulatory (69.0 >= 50.0)
Stakeholder = 1 prefers regulatory (-31.0 >= -50.0)
Stakeholder = 2 prefers distributed (69.0 < 150.0)
Stakeholder = 3 prefers regulatory (-31.0 >= -50.0)
Stakeholder = 4 prefers regulatory (-31.0 >= -50.0)
Regulatory preference = 0.8
```

If the distributed system works sufficiently well, due to its low overhead, it will tend to pay off better than the regulatory system and tend to have more satisfied stakeholders. However, if cheating is excessively granted, the regulatory system will tend to pay off better for stakeholders other than the successful cheaters.

Here are the simulation parameters:

1) BUREAUCRACY_FEE: this is how much a member pays the regulatory agency per round.
2) CLAIM_PROBABILITY: probability per round of a member initiating a claim.
3) LAWFUL_CLAIM_AMOUNT: a lawful claim amount.
4) UNLAWFUL_CLAIM_AMOUNT: an unlawful claim amount.

5) CLAIMANT_CHEAT_PROBABILITY: probability that a claimant makes an unlawful claim.
6) AUDITOR_ERROR_PROBABILITY: probability that an auditor fails to catch an unlawful claim.

The BUREAUCRACY_OVERHEAD must be greater than zero, since the regulatory agency does not work for free. This implies that the total value of its members will diminish over time, since in this system, there is no incoming value. We use CLAIMANT_CHEAT_PROBABILITY and AUDITOR_ERROR_PROBABILITY as independent variables, setting the other parameters to positive values, with the constraint that UNLAWFUL_CLAIM_AMOUNT is greater than LAWFUL_CLAIM_AMOUNT.

Simulations were run for 50 rounds with 100 stakeholders, varying the independent variables from 0 to 0.4. Table 1 shows the effect of auditing claims on preference for the regulatory agency *vs.* the distributed system. When there is no cheating, the distributed system is preferred, as there are no fees to pay. As cheating increases, but with errorless auditing to catch it, the distributed system is also preferred. It is only under the conditions of cheating and error-prone auditing, resulting in losses to non-cheaters, that the regulatory agency system gains in preference.

Table 1. Regulatory agency preference as a function of claimant cheating and auditor errors.

Audit error probability		Cheat attempt probability				
		0.0	**0.1**	**0.2**	**0.3**	**0.4**
	0.0	0.0	0.02	0.05	0.07	0.10
	0.1	0.0	0.04	0.04	0.06	0.09
	0.2	0.0	0.09	0.07	0.07	0.13
	0.3	0.0	0.19	0.16	0.19	0.19
	0.4	0.0	0.28	0.31	0.30	0.34

One conclusion to be drawn from the simulation is that the presence of claim auditors, even mistake-prone ones, has a powerful dampening effect on the success rate of cheaters, resulting in a significant stakeholder allegiance to the distributed system.

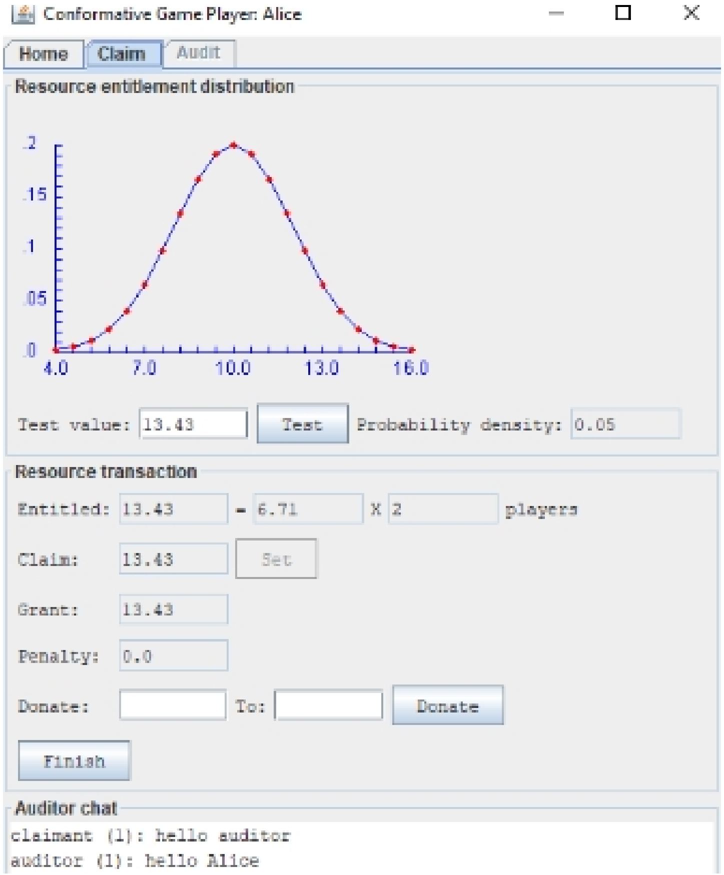
4. Blockchain game

A game is presented to help determine the viability of the organization using players as stakeholders.

The game consists of a Hyperledger Fabric blockchain application that allows a host and players to participate in a game that embodies the rules. The client interfaces for the game have been designed for the stakeholder roles of claimant and auditor. The Hyperledger Fabric code may be found at https://github.com/dialectek/ConformativeChain. A previous incarnation of the app resides on the Google App Engine at http://conformativegame.appspot.com [15]. The blockchain instantiation is a direct port of the App Engine functionality, thus contains an administrative client that lets a user orchestrate transactions according to the rules. The rules will be fully incorporated into the blockchain code in a future release to complete the smart contract.

Figure 1 shows the state of player "Alice" as a claimant at the conclusion of a successful claim transaction. For anonymity and authentication purposes, the player name could also be a public key provided to a user. Alice is entitled to a claim of 13.43 from the common resources. This value was probabilistically sampled from the shown distribution, which represents an abstraction of some event incurring an expense that justifies a claim. This obviously means that a particular claim could appear excessive or too low to auditors. In this case, the auditor has granted the entire claim. The claimant and auditors can optionally chat with each other before the auditors determine a grant amount. A penalty is then calculated from the difference between the claim and the grant amount, which in this case is 0.

Figure 2 shows the claim transaction completion of the auditor, "Bob", who has granted the entire claim. Since Bob was the only auditor for this claim, the consensus grant is equal to Bob's grant, and thus there is no penalty for Bob.



Test value: 13.43 Probability density: 0.05

Entitled: 13.43 = 6.71 X 2 players

Claim: 13.43

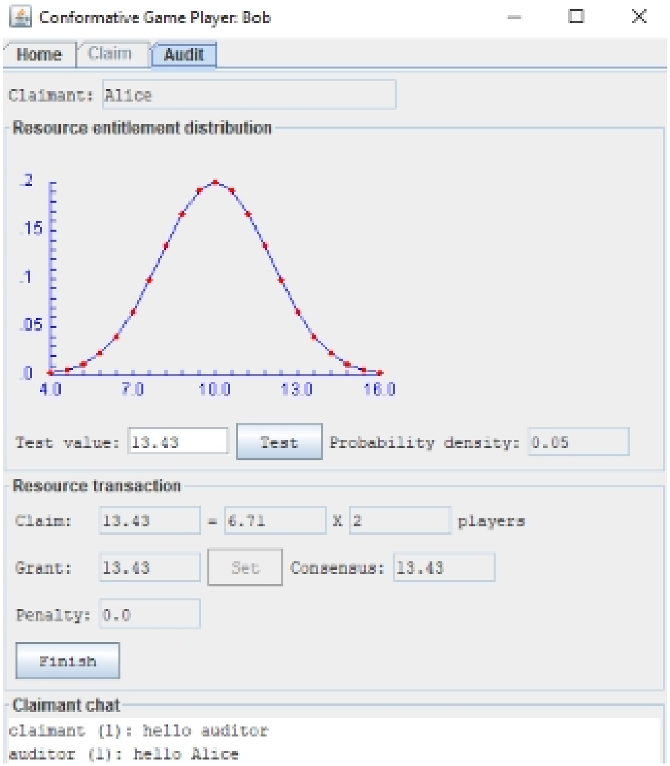
Grant: 13.43

Penalty: 0.0

Donate: To:

claimant (1): hello auditor
auditor (1): hello Alice

Figure 1. Claimant transaction completion.



Claimant: Alice

Test value: 13.43 Probability density: 0.05

Claim: 13.43 = 6.71 X 2 players

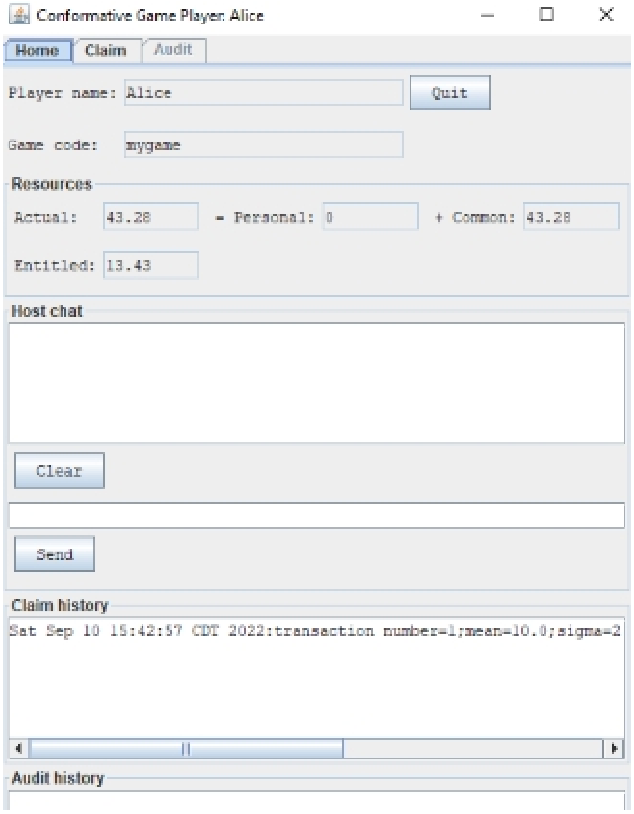
Grant: 13.43 Consensus: 13.43

Penalty: 0.0

```
claimant (1): hello auditor
auditor (1): hello Alice
```

Figure 2. Auditor transaction completion.

Figure 3 shows that Alice has received 13.43 in resources from the common resource pool, and equal deductions have been made from each player's common resources to fund the grant.



Player name: Alice

Game code: mygame

Actual: 43.28 = Personal: 0 + Common: 43.28

Entitled: 13.43

```
Sat Sep 10 15:42:57 CDT 2022:transaction number=1;mean=10.0;sigma=2
```

Figure 3. Claimant resource acquisition.

5. Conclusion

The hope of this research is to propose a feasible method for governing a common resource that uses anonymity in the role of auditors drawn from a pool of stakeholders. A preliminary simulation points to the plausibility of the method, chiefly by exhibiting a dampening effect that auditing has on cheating. A more thorough test platform is laid out with the blockchain game. However, trials with actual stakeholders to compare its performance *vs.* a bureaucratic system are necessary to yield a conclusive evaluation.

On a larger scale, this DAO aims to raise awareness of how organizations might leverage a technological landscape that is connecting people into ever denser communication webs. Blockchain fits in as a means of spanning proprietary and localized databases with a shared ledger of public transactions and operations.

Acknowledgments

No external funding was used for this work.

Conflicts of interests

The authors declared that they have no conflicts of interests.

Authors' contribution

T.P. conceived of the presented idea. T.P. and J.W. developed the idea and researched the literature. T.P. wrote the code and performed the simulations. All authors contributed to the final manuscript.

References

[1] Phillips KW., Liljenquist KA., Neale MA. Is the pain worth the gain? The advantages and liabilities of agreeing with socially distinct newcomers. *Pers Soc Psychol Bull* 2009, 35:336-350.

[2] Hardin G. "The Tragedy of the Commons". *Science* 1968, 162 (3859):1243–1248.

[3] Herring S, Job-Sluder K, Scheckler R, Barab S. Searching for Safety Online: Managing "Trolling" in a Feminist Forum. *Inf. Soc.* 2002, 18(5):371-384.

[4] Tokunaga RS. Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Comput. Hum. Behav.* 2010, 26(3):277-287.

[5] Kiesler S, Sproull L. Group decision making and communication technology. *Organ Behav Hum Decis Process* 1992, 52(1):96–123.

[6] Dubrovsky VJ, Kiesler S, Sethna BN. The equalization phenomenon: Status effects in computer-mediated and face-to-face decision-making groups. *Hum Comput Interact* 1991,6(2):119-46.

[7] Wright J, Stepney S. Enforcing behaviour with anonymity. In *Proceedings of The Workshop on Applications of Private and Anonymous Communications*, Istanbul, Turkey, September 22-25, 2008, pp. 1-8.

[8] The Economist. "Blockchains: The great chain of being sure about things. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency." 2016. Available: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (accessed on 10 August 2023).

[9] Governatori G, Idelberger F, Milosevic Z, Riveret R, Sartor G, *et al.* On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artif. Intell. Law.* 2018, 26 (4):33.

[10] Cui W, Sun Y, Zhou J, Wang Y, Huang L, *et al*. Understanding the Blockchain Ecosystem with Analysis of Decentralized Applications: an Empirical Study. In *Proceedings of the 5th International Conference on Management Engineering, Software Engineering and Service Sciences*, Chengdu, China, January 8-10, 2021, pp. 38–44.

[11] Hassan S, De Filippi P. Decentralized Autonomous Organization. *Internet Policy Rev.* 2021, 10(2).

[12] Popper N. Move Over, Bitcoin. Ether Is the Digital Currency of the Moment. 2017. Available: https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html (accessed on 20 July 2023).

[13] Medium. DAOs Are Better Than Companies. 2021. Available: https://medium.com/coinmonks/daos-are-better-than-companies-2ab3e6e50a14 (accessed on 25 July 2023)

[14] Riaza BP, Gnabo JY. Decentralized Autonomous Organizations (DAOs): Catalysts for enhanced market efficiency. *Finance Res. Lett.* 2023, *58 Pt B*.

[15] Portegys T., Wolf JR. Distributed Resource Governance Using Asymmetric Anonymity. 2011. Available: https://www.researchgate.net/publication/335475264_Distributed_Resource_Governance_Using_Asymmetric_Anonymity (accessed on 5 July 2023).

[16] Anonymous. Google App Engine. 2008. Available: https://cloud.google.com/appengine# (accessed on 10 July 2023).

[17] Anonymous. Architecture Reference. 2022. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/architecture.html (accessed on 10 August 2023).

[18] Axelrod R. *The Evolution of Cooperation*. New York: Basic Books, 1984.