Proof of Help: A Fresh Approach to Consensus for Inequality Reduction

Abstract. *In recent years, several blockchain technologies have spotlighted the importance of decentralization. Many consensus protocols ensure that transactions and numerous real-life actions may occur without the need for a central authority. Therefore, it is pertinent to question whether the total absence of central control in financial transactions is always a beneficial concept. As human beings, can we place more trust in a decentralized code than in our inherent need for community?*

Towards the end of this paper, we will propose a novel consensus protocol model. This model is grounded in the reduction of inequality and sustainable development principles.

A.D.

INDEX

For any information and further development

ProofOfHelp@gmail.com

1. INTRODUCTION

a. Decentralization

Decentralization, often described as the dispersion of power and responsibility, stands as one of the most pivotal achievements of the 21st century, alongside the remarkable advancements in Artificial Intelligence. In recent years, its significance has surged across diverse sectors: economics, social dynamics, finance, public administration, information technology, communication, culture, and even the realm of currencies. While the concept of decentralization has recently gained popularity, its **roots** trace back to antiquity.

The origins of decentralization can be glimpsed in **ancient Greek city-states**, where the independent, self-governing nature of each city exemplified a form of local autonomy. This early manifestation of decentralization planted the seeds for subsequent political ideologies and movements centered on the idea of **self-determination**. In many countries around the world, this yearning for decentralization culminated in universal adult suffrage, a cornerstone of **democratic governance**.

The IT era has also had a profound impact on decentralization, pushing the concept to more extreme results. It has evolved from dispersing power and responsibility to as many individuals as possible to the development of systems without an authority. In these “systems”, people only need to agree on a protocol and software, which together define the rules and structure of the decentralized organization. This transformation has given rise to innovative examples which will be explored later.

Today, decentralization continues to evolve and redefine power structures across the globe, leaving an indelible mark on our societies and institutions. Its impact resonates not only in politics but also in the very fabric of our interconnected world.

After having achieved its scope in other fields of humanities, in fact, the most interesting studies about decentralization regard the so-called “**DeFi**” (Decentralized Finance) and “**cryptocurrencies**”.

Even though the explosion of various cryptocurrencies has occurred only in the last five years, the roots of this phenomenon reach much further back in time.

In 1983, David Chaum, a professor in the Department of Computer Science at the University of Berkley, penned a groundbreaking paper titled 'Blind signature for untraceable payments' [1]. This work laid the foundation for the concept of anonymous, untraceable transactions, a cornerstone of modern cryptocurrencies.

Just a year prior, in 1982, Chaum published another seminal paper titled 'Computer Systems Established, Maintained, and Trusted by Mutually Suspicious

[1] Chaum D. (1983) Blind Signatures for Untraceable Payments. In: Chaum D., Rivest R.L., Sherman A.T. (eds) Advances in Cryptology. Springer, Boston, MA. https://doi.org/10.1007/978-1-4757-0602-4_18.

Groups.'[2] This work represents a crucial step in the evolution of blockchain technology and consensus protocols, which are fundamental to the decentralized systems as we know it.

If there were to be a 'Galileo' in the realm of crypto-decentralization, David Chaum would undoubtedly hold that title. His pioneering contributions in the early 1980s paved the way for the crypto revolution we are witnessing today.

Another ingredient for this recipe is Crypto-Anarchism, which is intertwined with the studies of David Chaum and other computer scientists and cryptographers. In 1988, the American engineer Timothy C. May wrote his '*Manifesto*[3]', proclaiming that '*Computer technology* [was] *on the verge of providing the ability for individuals and groups to communicate and interact with each other in a highly anonymous manner*'.

> "*A specter is haunting the modern world, the specter of crypto anarchy*"[4]

The central idea in the Manifesto was that "*cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions".*

b. What is decentralization?

As human beings, we inherently live in societies, whether they are families, tribes, countries, or other smaller or larger groups. In any social structure, rules are essential to govern everyday life and regulate relationships among individuals. These rules provide a framework within which all rights and obligations exist. However, it's important to note that even the most comprehensive legislation cannot address every real-life situation and take into account every single interest existing in a group.

One key concept that addresses this second limitation is decentralization. Decentralization involves transferring the **power to rule** to a larger group of individuals. The more participants, whether individuals or organizations, engage in this process, the more decentralized the context becomes. This approach aims to distribute decision-making and authority, often resulting in greater adaptability and inclusivity within the group.

When we think about a group of people gathered for specific purposes, we can break down the concept of the 'power to rule' into several distinct components:

- Setting the Rules: this involves establishing the main principles in advance.
- Changing the Rules: it refers to updating existing rules to accommodate new developments or to address issues that arise.

[2] Available here https://www.chaum.com/publications/research_chaum_2.pdf

[3] Available here: https://www.activism.net/cypherpunk/crypto-anarchy.html

[4] From The Crypto Anarchist Manifesto.

- Applying the Rules: this entails creating an environment in which the established rules are followed. This may include ensuring that all participants are aware of the existing framework.
- Judging Compliance: this involves evaluating whether the behavior of the group's members aligns with the established rules.
- Enforcing Compliance: This is the authority to ensure that the group adheres to the rules, even in the absence of consensus from one or more participants.

Understanding these components is crucial for effective governance within any group or organization.

c. Forms of decentralization

Democracy, without a doubt, represents one of the earliest forms of decentralization. In democratic organizations (not limited to nation-states), the power to rule is distributed among the participants. This is the **first step**.

However, in complex democratic contexts, it is not always practical for people to directly vote on every single action or decision. In such cases, individuals may vote to elect one or **more representatives**. To prevent the concentration of power, even within a democratic framework, fundamental laws allocate the most significant positions to **collegial bodies**, and representative mandates are limited to **short**, predefined **periods**. This marks the **second step**.

Yet, even in this case, there are still many **risks**. For example:

- **Asymmetrical** distribution or **lack** of **information**: People may not have access to the same information, which can skew decision-making.
- Presence of very **strong power groups** or "lobbies" (military, economical, psychological, commercial, religious, financial, and criminal): These groups can exert undue influence on elected representatives.
- **Misinformation** and the diffusion of **fake news**: False or misleading information can sway public opinion and affect decision outcomes.

For this reason, modern organizations have developed advanced laws, independent audits, and **independent authorities** to regulate the free economy, the free market, the free information, the stock exchange, etc. This represents the **third step**.

History has demonstrated that even with all these safeguards in place, there is still a possibility that something goes wrong. For instance, you still have to "trust" that people you elected will fairly operate for the full duration of their mandate.

Can we **avoid "trusting"**? This is the **fourth step** of decentralization: the fully decentralized world.

In this fully decentralized world, the challenge lies in striking a balance between distributing power widely and ensuring efficient decision-making. It requires **trust in systems**, and no more in individuals. Blockchain technologies are examples of systems where trust is placed in the transparency and immutability of the system rather than in a central authority.

The path to a fully decentralized world is complex, involving not only technological advancements but also shifts in societal norms and governance structures. It's a world where the risks above mentioned—information asymmetry, powerful interest groups, and misinformation—can potentially be mitigated through innovative mechanisms.

By continually questioning and evolving our systems, we move closer to a future where decentralization empowers individuals and safeguards against the pitfalls of concentrated power.

d. Is decentralization always a good idea?

The allure of decentralization lies in its promise of self-reliance and autonomy.

However, even in this seemingly utopian scenario, there's a caveat: you must trust that the decentralized system is ready to handle any unexpected events that life might throw your way—be it a natural disaster, an earthquake, or even a global pandemic. In essence, you have to believe that the system is "reality-proof." While the development of complex AI systems might theoretically reduce some of these risks, there's a more significant issue without a clear global solution.

In the real world, people and companies, local businesses and small enterprises, don't always follow predetermined agreements in a predictable manner. They adjust their behavior subjectively, often extending help to one another and operating ethically. This flexibility allows societies to evolve around a more resilient system that can weather bad times and adapt to failures, whether they stem from internal or external factors.

A "decentralized software-based" economic system, while efficient in many respects, might falter when faced with the unexpected and unpredictable. It may struggle to foster the cooperative and ethical interactions that underpin a safe and resilient environment.

In conclusion, decentralization is an abstract model with significant merits, but it's not a panacea. It may not address all the challenges, particularly in terms of ensuring equality and supporting those who are temporarily or chronically vulnerable. Recognizing its limitations while harnessing its advantages in the right context is essential for crafting a robust and inclusive economic and social framework.

2. APPLICATIONS

As the rapid development of cryptocurrencies and decentralized finance (DeFi) continues, the concept of decentralization has garnered increasing attention. This heightened interest can be attributed to the fundamental role that decentralization plays in these innovative financial systems, where it empowers individuals and enhances security.

a. Cryptocurrencies

Modern cryptocurrencies[5] are virtual currencies[6] based on several central ideas:

- There is no central authority to regulate the emission of new currency or to control transactions.
- A public ledger contains all transactions, allowing anyone to verify if the person claiming to own the money is the real effective owner.
- Nodes vote to confirm and validate transactions, preventing frauds (e.g., spending money they don't have or double-spending schemes).
- The system contains rules for attributing the right to vote. The way this "consensus protocol" works often differentiates one cryptocurrency from another.

On the other hand, some of the common goals are:

- Creating money and financial services accessible to all.
- Building a solid investment instrument with a proper value.
- Establishing a currency without borders.
- Introducing a system with no restrictions or interference.
- Providing a “fair” level of anonymity."

While many have delved into the detailed history of cryptocurrencies and decentralized finance, for our purposes, it's important to note that a multitude of cryptocurrencies exist today, each with its own dedicated community of supporters. These cryptocurrencies are increasingly accepted as a method of payment in numerous online and, at times, physical stores.

b. Decentralized Finance

The Decentralized Finance[7] (DeFi) represents a revolutionary form of finance built upon blockchain technology, operating independently of central authorities such as Central Banks, financial institutions, and brokers. In the DeFi ecosystem, various participants in the financial landscape, including buyers, sellers, lenders, and borrowers, interact directly through a peer-to-peer system, with all transactions

[5] Aleksander Berentsen and Fabian Schar, "A Short Introduction to the World of Cryptocurrencies," Federal Reserve Bank of St. Louis Review, First Quarter 2018, pp. 1-16. https://doi.org/10.20955/r.2018.1-16.

[6] For more on Virtual Currencies: European Central Bank (2012) Virtual Currency Schemes. www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[7] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 2020 “*Decentralized Finance*”, Journal of Financial Regulation, Volume 6, Issue 2, 20 September 2020, Pages 172–203, https://doi.org/10.1093/jfr/fjaa010

recorded on a transparent public ledger. The cornerstones of De-Fi are 'smart contracts' and 'Decentralized Apps' (DApps). These are powered by the same technology that underlies cryptocurrencies the consensus protocol.

DeFi's mission is to democratize finance, making financial services more accessible and reducing the control of centralized financial institutions. It's a new financial frontier that challenges the traditional financial system's norms and offers a potential path to financial inclusion.

c. Consensus protocol

Every cryptocurrency and DeFi ecosystem relies on a "*consensus protocol*"[8] to determine the validity of transactions, confirm the system's status, and maintain the integrity of the blockchain. Since there is no central authority, the only way to prevent abuse and errors is to establish rules that all users or nodes in the system must adhere to when sending or accepting transactions.

In essence, some users or nodes (which may or may not overlap, depending on the protocol) must vote on whether each transaction should be added to the public ledger. The ideal decentralized system grants each individual one vote, following a 'one-person one vote' principle. However, it can be challenging to identify every user without a central authority to verify their identities. The existence of multiple accounts for a single person can undermine this democratic voting process.

Hence, consensus protocols also play a crucial role in distributing the right to vote. While achieving the 'one person one vote' goal may seem distant, consensus protocols aim to prevent any single user from controlling the voting power, thereby avoiding centralization and ensuring that no one individual can make decisions for the entire network.

Nowadays, there are two primary types of consensus protocols, with many others consisting of variants or combinations of these two[9]:

(1) Proof of Work (PoW): In the case of Proof of Work, participants have to engage in a computational task to obtain the right to vote on network decisions. This computational task typically involves solving complex mathematical puzzles, such as the cryptographic puzzles used in Bitcoin. The more computational power a participant possesses, the more they can contribute to the network's security and validate blocks containing transactions. Unfortunately, the "work" in Proof of Work mainly serves the purpose of securing the network and may not have any additional utility. It's

[8] Shijie Zhanga Jong, Hyouk Leeb, 2019 "*Analysis of the main consensus protocols of blockchain*", ICT Express Volume 6, Issue 2, June 2020, Pages 93-97.

[9] For a complete classification, which also includes protocols that differ from this two schemes: Sarah Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework, Expert Systems with Applications", Volume 168, 2021.

challenging, though not impossible, to imagine consensus protocols where the work involved is also inherently useful.

(2) Proof of Stake (PoS): with Proof of Stake, participants are required to demonstrate ownership of a certain amount of tokens. This ownership acts as collateral, ensuring that they have a vested interest in the network's security and stability. By holding and "staking" their coins, participants earn the right to vote on network decisions.

Real-world examples of these consensus mechanisms include Bitcoin[10] as a prominent example of Proof of Work, where miners use their computational power to solve cryptographic puzzles and validate transactions. Ethereum, another major blockchain, went from Proof of Work to Proof of Stake in Ethereum 2.0[11], a move (also) aimed at improving energy efficiency and reducing the environmental impact of the network.

Each consensus mechanism has its own set of advantages and disadvantages. Proof of Work offers robust security but is energy-intensive and has a higher barrier to entry. Proof of Stake is more energy-efficient and eco-friendly but may raise concerns about the concentration of power among the wealthy that hold significant stakes in the network.

In both cases, the protocol rewards participants with a certain amount of cryptocurrency for their efforts in demonstrating their right to vote.

Owners of fiat currency primarily had two ways to obtain capital gains:

- Trading the currency to exploit market volatility (or holding the currency for the same reason, e.g., forex trading).
- Investing in other assets to grow their wealth over time.

Cryptocurrencies, as said before, offer this third option: Mining.

The distribution of voting power and resources in cryptocurrency ecosystems, anyway, poses several pressing concerns. At its core, the protocol often mirrors the old "fiat money balance of power," perpetuating inequalities and sometimes even exacerbating them. This issue isn't merely theoretical; it has real-world consequences.

One significant risk lies in the possibility that entities with influence over the traditional economy could extend their control into the crypto realm. For instance, in a proof-of-work-based environment, wealthier entities can afford increasingly powerful mining machines, amplifying their dominance. In a proof-of-stake environment, the ability to vote is often linked to the amount of cryptocurrency one holds, creating a system where the rich can buy their influence. This concentration of voting power also translates into the uneven distribution of newly created coins. Consequently, even though cryptocurrencies are touted as democratizing financial sys-

[10] Nakamoto, S. 2008. "*Bitcoin: A Peer-to-Peer Electronic Cash System*". bitcoin.org. https://bitcoin.org/bitcoin.pdf

[11] Buterin Vitalik, 2020, "*Why Proof of Stake (Nov 2020)*" https://vitalik.ca/general/2020/11/06/pos2020.html

tems, the fees users pay for each transaction are often disproportionately distributed.

Paradoxically, the cryptocurrency movement, including some of its more anarchist factions, has inadvertently laid the groundwork for a new form of a pyramid-like model, where a select few wield disproportionate influence.

In addition to these economic concerns, there's the alarming environmental issue[12]. Proof of work systems, while providing security to the network, consume vast amounts of energy. This has given rise to concerns about the relative carbon footprint, with some cryptocurrencies being criticized.

The problems at hand are significant, but they also present opportunities for innovation and change.

For a comprehensive understanding, it's essential to acknowledge the existence of a third protocol: Practical Byzantine Fault Tolerance (PBFT). While not as widely adopted as Proof of Work and Proof of Stake, PBFT holds a significant role in some major cryptocurrencies. Serving as a distributed consensus mechanism, PBFT is specifically designed to facilitate an agreement among a network of nodes, even in the presence of potentially faulty or malicious nodes. Unlike certain other consensus mechanisms, PBFT excels in situations where a certain degree of Byzantine (malicious) behavior is anticipated. This capability is fundamental for maintaining the reliability and security of blockchain networks. However, it's worth noting that, given the paramount importance of communication among nodes in such protocols, PBFT may encounter challenges in highly scalable environments.

[12] Moritz Wendl, My Hanh Doan, Remmer Sassen, The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review, Journal of Environmental Management, Volume 326, Part A, 2023, 116530, ISSN 0301-4797, https://doi.org/10.1016/j.jenvman.2022.116530

3. PROOF OF HELP

a. Introduction

"Proof of Help" is a consensus protocol focused on reducing inequality. In Proof of Help, the authority to approve transactions is granted to nodes proportionally based on the amount of tokens they choose to donate to valuable projects.

Protocols based on Proof of Help could accept donations using a dedicated token, but they can theoretically function with existing ones, such as cryptocurrencies or cryptoassets. While the choice of a native token is not inherently embedded in the logical structure of Proof of Help, it could be the one that better reflects the inner nature of the protocol. If the core idea of Proof of Help is to reduce inequalities, it should minimize the use of tokens associated with Proof of Stake or Proof of Work, which, in theory, could exacerbate such inequalities.

In Proof of Help protocols (PoHp), nodes should contribute a certain amount of tokens to a worthy project to obtain the power to validate transactions. The validation process allows nodes to receive a reward through fees or the emission of new tokens.

A PoHp is necessarily backed by a decentralized autonomous organization (DAO) responsible for selecting "worthy projects." The PoH DAO should have a complexity that aligns with the intricacies of the market in which the blockchain operates. The PoH DAO selects projects funded (with the token) by donors who become validators, receiving a validation Token.

b. Proof of Help Dao (PohD)

As mentioned before, a decentralized autonomous organization (DAO) is an essential part of a Proof-of-Help Protocol (PoHp). Without a system to sort out worthy projects, it could be easy for a malicious entity to transfer funds to themselves or to causes that don’t reduce inequalities.

Direct or delegated voting power on projects (depending on the complexity of the market) should be one of the most important parts of the protocol. The governance of the DAO could be related to the validation process, either directly or indirectly. In other words, the management of the DAO could be assigned to the owners of validation tokens.

To minimize the possibility of malicious activity and the risk of operators being able to donate to their own projects, protocols could distinguish between the Validation Period and the DAO Voting power. This could be achieved by introducing a delay of one or more periods, beginning with the validation power. Following this path, donors could receive validation tokens for the first period and governance tokens for the second (or third) period.

Another possible security feature could be to increase the time between the decision to promote a project and the time it can receive donations, or to make it necessary for projects to be approved by at least two different governance bodies before they can receive funds.

c. Philanthropic vs circular model

PoH Donors should be able to transfer their founds in a given period of time (t), obtaining the validation tokens only at the end of this period (t). This validation tokens should remain valid for the entire following period (t+1). In t+1 new donors will contribute to the system receiving validation tokens for the period t+2.

PoHp could be designed to reward validators with a certain number of tokens, independently by the amount of tokens used for donation. The Amount received could be in fact only related to the value of the fee, the percentage of the validation power in relationship to other validators, the eventual introduction of new "coins". Consequently, the received tokens (in each period) may be even less than the donated amount, adopting a philanthropic model where the value is flexible. This doesn't exclude the possibility of a higher number of token received, where it happens beyond the willing of the donor.

Alternatively, PoHp could be set to reward validators with an amount of tokens equal to or greater than the donated tokens, establishing a circular model.

In the first case, the protocol could only limit the validity of the validator tokens to a certain period of time (or number of validations), fixing the value of the fee from the outset, and eventually allowing the possibility to reward validators with new tokens. In the second case, it should be possible to:

- Not fix the amount of time necessary to properly reward validators, allowing this period to float.
- Adjust the fee or emission of new tokens (to reward the validator with the fixed amount).
- Implement a combination of the two.

Although all possible solutions appear valid, the last one could be the easiest to implement, considering the need to ensure a minimum time for governance and a time limit to allow other donor investors to participate in the project. A floating period of time (with a cap) and a flexible fee (or with the emission of new tokens to compensate) could be the most easily applicable model.

Similarly, both the philanthropic and circular models are valid, although the circular model could be the one that most incentivizes the system to grow.

d. Foundation

Since PoHps require more steps, it is essential to have a community of developers to maintain the system and keeping it safe and suitable for the relevant markets. The foundation could be funded by the emission of new tokens or keeping a small amount of the total donation (donation fee) in a transparent and fair manner. The governance of the foundation can also be assigned to the donors. In this case, it would be useful to further separate the validation process, the management of the

DAO, and the Governance of the foundation. It is also possible to imagine a collegial body which members can be replaced in turn.

e. Donation

The donation process should be certified on the system's Blockchain. If possible, projects should receive the donation in the native token directly to their wallets. DAO Management or the protocol itself could restrict the maximum number of tokens that a single project can receive. Depending on the complexity of the market and the level of transparency, the protocol could give donors the possibility to:

- Determine only the amount of token to donate, distributing them following the DAO rules or proportionally to the projects.
- Selecting a pillar or a cluster of projects (in that case the DAO should group project according to pre-determined criteria).
- Selecting an individual project.

f. Projects

Under a specific set of rules, the opportunity to present a project for donation should be accessible to everyone in the network. The DAO, the Foundation, or the founders of the network could limit the types of projects allowed to specific sectors. Likewise, they can define the minimum information required for a project to secure funding. Depending on the network's complexity, projects could be organized into groups and pillars based on their scope. Projects equipped with their own blockchain tracking system for received funds should be given preference.

g. Community

A strong community should be an integral part of every PoH Protocol to promote the system and safeguard the mutualistic scope. The DAO and Foundation should collaborate with the community of users and voters to create a safe space for everyone to invest and make transactions.

h. Users

Users of tokens should not need to become nodes or investor. They should only need to have a private key and the public key or the address of their wallet. Users should be able to submit transactions paying a fee. This fee should be designed not to limit or disincentives small transactions.

4. CONCLUSIONS

Actual cryptocurrencies have many merits; the most important is addressing inequality in the actual financial system. They also have developed a very important technology that has proven to function preventing serious general malicious attack at the ecosystem itself.

In this way, they drew attention of the great public on these alternative assets paving the way to an equal and fair system.

In this short paper, is presented a protocol that could be the backbone of every practical application of decentralized finance.

It should be a great moment to use all these incredible progresses and achievements to start a new era of decentralized welfare and a more sustainable existence of the humanity.