# Seção 8 - INCENTIVE MECHANISMS AND ACCOUNTABILITY

Aluno: **Luiz Carlos**

Professor: Francisco Sant‘anna

Universidade do Estado do Rio de Janeiro – UERJ

**Apresentação sobre a seção e o artigo escolhidos**

**Rio de Janeiro, 29 de Setembro de 2022**

# Agenda

# Seção

# Escolha e leia uma outra seção do artigo



Additional measures for deniability can be incorporated by inhibiting the use of traffic analysis for concluding where a file was read from. For example, in Mnemosyne [Hand and Roscoe 2002], during the retrieval of a file, more nodes than those needed will be contacted and more files will be retrieved so that the actual file targeted will be disguised.

It should be noted that structured systems are apparently nondeniable, as the identifiers of the files stored at the nodes are bound to the node addresses; if a file is known to exist in the network, its location, and, therefore, the identity of the node that stores it, is also known. On the other hand, the owner of the node has not necessarily requested the file, and, in any event, has no control over whether the file will be stored in their node, and, in this sense, cannot be held responsible for it.

## 8. INCENTIVE MECHANISMS AND ACCOUNTABILITY

The operation, performance and availability of an uncontrolled decentralized peer-to-peer system relies to a large extent on the voluntary participation of its users. It is, therefore, necessary to employ mechanisms that provide incentives and stimulate cooperative behavior between the users, as well as some notion of accountability for actions performed.

In the absence of such provisions, the results can range from significant degradation of performance to variable and unpredictable availability of resources, or even to complete collapse.

An example of uncooperative behavior is the so-called "free-rider" effect, where users only consume resources without contributing any. This can be interpreted as a manifestation of the "Tragedy of the Commons" [Harding 1968], which argues that people tend to abuse shared resources that they do not have to pay for in some way.

Providing incentives and accountability in peer-to-peer networks with transient populations of users, where it is hard to identify peers and obtain information about their past behavior in order to predict their future performance, can be a particularly challenging task, especially due to the absence of a ubiquitous, effective, robust, and secure system for making and accepting anonymous micropayments.

Two general categories of solutions are proposed:

—Trust-based Incentive Mechanisms. Trust is a straightforward incentive for cooperation, in which one engages in a transaction based on whether he/she trusts the other party. Reputation mechanisms belong in this category.

—Trade-based Incentive Mechanisms. In trade-based incentive mechanisms, one party offering some service to another is explicitly remunerated, either directly or indirectly. This category is mainly represented by various micropayment mechanisms and resource trading schemes.

### 8.1. Reputation Mechanisms

Online reputation management systems can be described as large-scale "online word-of-mouth communities" in which individuals share opinions about other individuals.

Centralized reputation systems (such as the one found in eBay) are successful to a large extent because people trust the reputation information presented by them [Dellarocas 2001]. In a peer-to-peer network, however, there is no single, recognizable organization or entity to maintain and distribute reputation information. As a result, reputation information must be distributed throughout the network, and hosted on many different nodes.

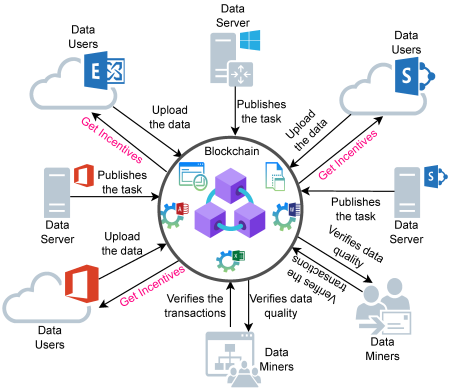
The main goal of a peer-to-peer reputation mechanism is to take the reputation information that is locally generated as a result of an interaction between peers, and spread it throughout the network to produce a global reputation rating for the network nodes. In the process, such reputation information must be kept secure and available. Various complex reputation management mechanisms have been developed to address these challenging tasks.



- Qual é número/título da seção escolhida?
- Seção 8 - INCENTIVE MECHANISMS AND ACCOUNTABILITY

# Do que se trata a seção/tema?

- Aborda possíveis soluções para o problema da participação voluntária dos usuários;
- É necessário empregar mecanismos que incentivem e estimulem o comportamento cooperativo entre os usuários;
- Bem como alguma noção de accountability (responsabilização) pelas ações realizadas.




[1]

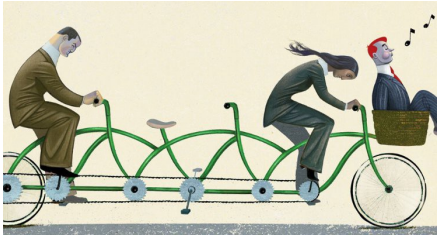
# Dê um exemplo concreto de um cenário relacionado ao seu tema

- Um exemplo concreto relacionado a esse tema é o Freechains, um projeto da rede P2P permissionless com sistema de reputação de autoria;
- O Freechains se adequa ao tema proposto nesta seção do artigo, qual seja, por exemplo, excessos, abusos, SPAM, fake news em fóruns públicos, sendo adequado, portanto, um mecanismo de reputação.

# Quais são os desafios científicos relacionados ao seu tema? Por quê?

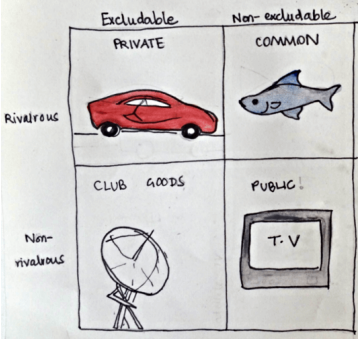
1. Comportamento não cooperativo é o chamado efeito “free-rider”

- No efeito ”free-rider” os usuários apenas consomem recursos sem contribuir com nenhum;



[2]

- Isso pode ser interpretado como uma manifestação da “Tragédia dos Comuns”;

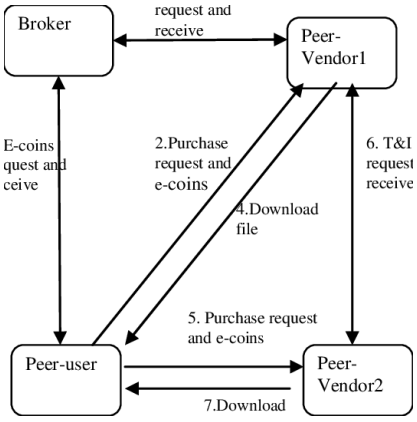



- [3]

- A Tragédia dos Comuns argumenta que as pessoas tendem a abusar de recursos compartilhados pelos quais não precisam pagar de alguma forma.

# Quais são os desafios científicos relacionados ao seu tema? Por quê?

- Fornecer incentivos e responsabilização em redes peer-to-peer com populações transitórias de usuários, onde é difícil identificar peers e obter informações sobre seu comportamento passado para prever seu desempenho futuro;
- Especialmente devido à ausência de um sistema onipresente, eficaz, robusto e seguro para fazer e aceitar micropagamentos anônimo;
- Aqui é importante esclarecer que, à época de concepção desse artigo (2004), a rede Bitcoin ainda não existia.



[4]

# Desafios científicos considerando sistemas centralizados e sistemas P2P

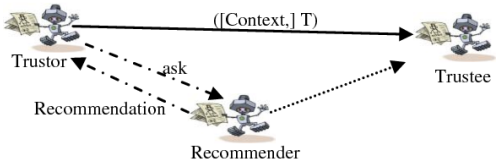



**Fig 1: Trust relation**

[5]

- Sistemas de reputação centralizados (como o encontrado no eBay) são bem-sucedidos em grande parte porque as pessoas confiam nas informações de reputação apresentadas por eles;
- Em uma rede peer-to-peer, no entanto, não existe uma organização ou entidade única e reconhecível para manter e distribuir informações de reputação
- Como resultado, as informações de reputação devem ser distribuídas por toda a rede e hospedadas em muitos nós diferentes.

# Artigo

# Escolha algum artigo que foi citado na seção

## The EigenTrust Algorithm for Reputation Management in P2P Networks

Sepandar D. Kamvar
Stanford University
sdkamvar@stanford.edu

Mario T. Schlosser
Stanford University
schloss@db.stanford.edu

Hector Garcia-Molina
Stanford University
hector@db.stanford.edu

### ABSTRACT

Peer-to-peer file-sharing networks are currently receiving much attention as a means of sharing and distributing information. However, as most of these networks rely on the anonymous, open nature of these networks offer an almost ideal environment for the spread of self-replicating inauthentic files.

We describe an algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads. We present a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network.

In simulations, this reputation system, called EigenTrust, has been shown to significantly decrease the number of inauthentic files on the network, even under a variety of conditions where malicious peers cooperate in an attempt to deliberately subvert the system.

### Categories and Subject Descriptors

C.2.4 [Computer-Communication Networks]: Distributed Systems—*Distributed applications*; H.3.3 [Information Systems]: Information Systems; Retrieval—*Selection*; H.3.7 [Information Systems]: Database Management—*Security, integrity and protection*

### General Terms

Algorithm, Performance, Theory

### Keywords

Peer-to-Peer, reputation, distributed eigenvector computation

### 1. INTRODUCTION

Peer-to-peer file-sharing networks have many benefits over centralized client-server approaches to data distribution, including improved robustness, scalability, and diversity of available data. However, the open and anonymous nature of these networks leads to a complete lack of accountability for the content a peer puts on the network, opening the door to abuses of these networks by malicious peers.

Attacks by anonymous malicious peers have been observed on today's popular peer-to-peer networks. For example, malicious users have used these networks to introduce viruses such as the *VBS.Gnutella* worm, which spreads by making a copy of itself in a peer's Gnutella program directory; then modifying the Gnutella ini file to allow sharing of *.vbs files [19]. For more common have been inauthentic file attacks, where malicious peers respond to virtually any query providing "decoy files" that are tempered with or do not work.

It has been suggested that the future de-emphasis of P2P systems will depend largely on the availability of social methods for assuring that peers obtain reliable information on the quality of resources they are receiving [8]. In this context, attempting to identify malicious peers that provide inauthentic files is superior to attempting to identify inauthentic files themselves, since malicious peers can easily generate a virtually unlimited number of inauthentic files if they are not banned from participating in the network. We present such a method wherein each peer $i$ is assigned a unique *global trust value* that reflects the experiences of all peers in the network with peer $i$. In our approach, all peers in the network participate in computing these values in a distributed and node-symmetric manner with minimal overhead on the network. Furthermore, we describe how to ensure the security of the computation, minimizing the probability that malicious peers in the system can lie to their own benefit. And finally, we show how to use these values to identify peers that provide material deemed inappropriate by the users of a peer-to-peer network, and effectively isolate them from the network.

### 2. DESIGN CONSIDERATIONS

There are five issues that are important to address in any P2P reputation system.

1. The system should be *self-policing*. That is, the shared ethics of the user population are defined and enforced by the peers themselves and not by some central authority.
2. The system should maintain *anonymity*. That is, a peer's reputation should be associated with an opaque identifier (such as the peer's Gnutella manager rather than with an externally associated identity (such as a peer's IP address).
3. The system should not assign any *profit to newcomers*. That is, reputation should be obtained by consistent good behavior through several transactions, and it should not be advantageous for malicious peers with poor reputations to continually change their opaque identifiers to obtain newcomer status.
4. The system should have *minimal overhead* in terms of computation, infrastructure, storage, and message complexity.
5. The system should be *robust to malicious collectives* of peers who know one another and attempt to collectively subvert the system.

Copyright is held by the author/owner(s).
*WWW2003*, May 20-24, 2003, Budapest, Hungary.
ACM 1-58113-680-3/03/0005.

- Qual foi o artigo que você escolheu se aprofundar?
- The Eigentrust algorithm for reputation management in p2p networks KAMVAR et al. [6]

# Por que este artigo foi escolhido?

- Primeiramente porque, em pesquisa ao Google Scholar em 16/09/2022, dentre todos os artigos citados na seção sobre mecanismos de reputação, esse foi, de longe, o artigo com a maior quantidade de citações (5.527 no total em 28/09/2022)

- Segundo porque o artigo propõe uma solução para o gerenciamento de reputação.

# Referências

# Referências I


Sweta Bhattacharya, Rajeswari Chengoden, Gautam Srivastava, Mamoun Alazab, Abdul Rehman Javed, Nancy Victor, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu.
Incentive mechanisms for smart grid: State of the art, challenges, open issues, future directions.
*Big Data and Cognitive Computing*, 6(2), 2022.

Ana Mikatadze.
A different approach to free riders problem.
https://medium.com/powershare/elinor-ostrom-on-tragedy-of-the-commons-a47bedcc4c2e.

Shreya.
Know about 'the tragedy of the commons'.
https://www.kidpid.com/know-about-the-tragedy-of-the-commons/.

# Referências II


Xiaoling Dai, Kaylash Chaudhary, and John Grundy.
Comparing and contrasting micro-payment models for content sharing in p2p networks.
In *2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*, pages 347–354, 2007.

Bagher Rahimpour Cami and Hamid Hassanpour.
A reputation-based trust model with fuzzy approach and dp,q-distance technique for peer-to-peer networks.
*International Journal of Computer Applications*, 37:41–44, 2012.

Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina.
The eigentrust algorithm for reputation management in p2p networks.
In *Proceedings of the 12th International Conference on World Wide Web*, WWW '03, page 640–651, New York, NY, USA, 2003. Association for Computing Machinery.

# Referências III

Andrew West, Sampath Kannan, Insup Lee, and Oleg Sokolsky.
An evaluation framework for reputation management systems.
05 2009.

# Seção 8 - INCENTIVE MECHANISMS AND ACCOUNTABILITY

Aluno: **Luiz Carlos**

Professor: Francisco Sant‘anna

Universidade do Estado do Rio de Janeiro – UERJ