Trust in Shapley: A Cooperative Quest for Global Trust in P2P Network

Arti Bandhana
Artificial Intelligence Center
Department of Computer Science
Faculty of Electrical Engineering
Czech Technical University in Prague
Prague, Czech Republic
bandhart@fel.cvut.cz

Tomáš Kroupa
Artificial Intelligence Center
Department of Computer Science
Faculty of Electrical Engineering
Czech Technical University in Prague
Prague, Czech Republic
tomas.kroupa@fel.cvut.cz

Sebastián García
Artificial Intelligence Center
Department of Computer Science
Faculty of Electrical Engineering
Czech Technical University in Prague
Prague, Czech Republic
garciseb@fel.cvut.cz

ABSTRACT

Modeling the trust of peers in peer-to-peer networks is pivotal in maintaining the security and functionality of the network. This trust is commonly perceived as a peer's reliability based on past interactions and is generally classified as local and global trust values. In a traditional client-server network, the responsibility of maintaining the integrity of the network falls on the central authority responsible for enforcing the security protocols and safeguarding the network against adversarial activities. In contrast, peer-to-peer networks may lack a central authority due to their decentralized nature, needing innovative mechanisms to maintain network trust. Incorporating a trust mechanism that considers peer interactions within peer groups becomes convenient in the absence of central authority. This paper introduces a novel approach to global trust computation. We propose a transferable utility coalitional game that pools local trust values between peers. The coalitions of peers aggregate the local trust values by considering internal and external trust. Internal trust is defined as the sum of the local trust values of the peers in the coalition, and external trust is constituted by the minimal trustworthiness of peers in the coalition to the peers outside. The resulting trust game is superadditive, monotone, and has a non-empty core. The global trust values of individual peers are the Shapley values in the trust game. Our numerical experiments in three different settings show that the resulting global trust captures the peer behavior faithfully, and we compared our method to Eigentrust.

KEYWORDS

Reputation management; peer-to-peer network; Global trust; Coalitional game; Shapley value

ACM Reference Format:
Arti Bandhana, Tomáš Kroupa, and Sebastián García. 2024. Trust in Shapley: A Cooperative Quest for Global Trust in P2P Network. In *Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), Auckland, New Zealand, May 6 – 10, 2024*, IFAAMAS, 9 pages.

Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), N. Alechina, V. Dignum, M. Dastani, J.S. Sichman (eds.), May 6 – 10, 2024, Auckland, New Zealand. © 2024 International Foundation for Autonomous Agents and Multiagent Systems (www.ifaamas.org).

1 INTRODUCTION

The domain of digital networking has witnessed a lot of advancements, one of which is peer-to-peer (P2P) networks for file sharing. These networks gained significant traction with the success of Napster, BitTorrent, Gnutella, and Kazaa [13]. P2P networks offer enhanced scalability and resilience by eliminating the need to go through a server [24]. While the P2P network has transformed the file-sharing landscape, the main challenge these networks face is the ability to determine their peers' trustworthiness accurately. Ensuring the reliability and authenticity of files being shared within the vast expanse of P2P networks is important, especially when there is no central authority to enforce security protocols.

Unlike traditional client-server architecture, P2P systems distribute responsibilities across all peers, meaning each peer acts as a client and a server [1]. These networks are categorized as pure P2P, hybrid, and super-peer networks based on the degree of decentralization [17]. Pure P2P network maintains a flat architecture where all their peers are equal in functionality. The hybrid P2P system combines the elements of both P2P and client-server models [27]. Striking a balance between the two, super-peer networks work on an intermediate layer [5]. While the P2P networks avoid a single point of failure, they become susceptible to security threats and malicious attacks [18]. The network also attracts adversarial peers who may deliberately disrupt the network operations.

To keep P2P networks secure, peers use their trust in other peers to protect themselves, block others, or tell others whom to block. Trust is a peer's belief in another peer's capabilities, honesty, and reliability based on their own direct experiences [22]. Trust models are pivotal in building any security solution because trust is an inherent concept of any security decision. Until now, most trust models are “I trust you or not” or better, “I trust you until I don't trust you and is too late”. These models propose a varying degree of trust that changes over time to improve security decisions. A trust model defines the method and procedure of trust modeling and evaluation by assigning a score to each peer [21]. The score is called a local trust if it is based on two peers' direct interaction, and global trust when it is a peer's overall standing in the P2P network [9]. There is a wide range of P2P trust models studied in the literature; see [3, 4, 12, 15, 19, 20, 23, 25]. While diverse in their methodologies, these trust models share a common objective: to control potential risks in peer interactions by establishing a robust trust framework. In particular, EigenTrust [11] stands out as one of the prominent methods in this domain.

However, none of these models consider the intricacies of "interaction groups" or, more formally, the coalitions between peers to compute trust. The coalitions are formed based on mutual benefit and peer interactions. Peers in the network can be seen as players forming coalitions to maximize their individual and collective benefits, i.e., trust. Through cooperation, peers can better determine the trustworthiness of other peers, pooling their collective experiences to derive a more accurate trust score. Motivated by the observation that trust dynamics in the network are not just a function of individual peers but rather influenced by the collective behavior of coalitions, this paper presents a novel approach to developing a trust model by combining the coalitional games and the Shapley value. Our approach emphasizes the significance of collaborative decision-making in trust evaluation. In particular, the experience of individual peers contributes to a broader collective computation of trust score in the network, making it challenging for adversarial peers to thrive. In this paper, we use the terms *trust* and *reputation* interchangeably, highlighting the intrinsic overlap of the two concepts within the context of peer-to-peer network evaluation.

The main contributions of this paper are as follows.

- The design of the trust model that offers a fresh perspective on trust computation in P2P networks based on cooperative game theory.
- The formulation of a coalitional game tailored to P2P networks, capturing trust relationships between peers within the coalition and peers outside the coalition.
- The application of Shapley value to compute a peer's global trust through collaborative trust computation.

The rest of the paper is structured as follows. Section 2 provides an overview of the related work from the literature regarding trust computation. The model design and theoretical results are presented in section 3. Numerical experiments are described in section 4 and the analysis of results is provided in section 5. Section 6 contains the conclusions and topics for future research.

2 RELATED WORK

The main objective of the trust models is to keep the network reliable, secure, and eliminate the distribution of inauthentic files and data by identifying potentially harmful peers in the network. This is mainly done through the computation of the *global trust* of each peer in the network.

In this context, EigenTrust [11] computes global trust by aggregating local trust values based on past peer interactions. The local trust values are normalized to mitigate malicious interactions. EigenTrust is based on the Power Method applied to the trust matrix of normalized local trust values, which is guaranteed to converge to the dominant eigenvector under some conditions, thereby establishing a global trust value for each peer. However, EigenTrust may perform poorly in cases where convergence to the dominant eigenvector does not occur [2]. Another notable limitation of EigenTrust is its dependability on pre-trusted peers. The absence of such peers makes the algorithm vulnerable to collusion attacks.

To address the reliance on pre-trusted peers, the HonestPeer [12] algorithm, an enhanced version of EigenTrust, uses the concept of an "honest peer". The peer classified as an honest peer possesses the maximum reputation in the system at any given point and is influential in calculating the global trust of a peer. If the honest peer is among pre-trusted peers, these peers maintain significant influence on the global trust values; otherwise, the influence is marginalized. While HonestPeer adeptly addresses the disproportionate influence of pre-trusted peers, it does not completely eliminate the dependency on them. The algorithm still uses the concept of pre-trusted peers, adjusting their influence based on the presence or absence of the honest peer in the cohort.

In a similar way, the PowerTrust system [29] draws inspiration from the power law to dynamically select "power nodes" that are the most reputable using a distributed ranking. The PowerTrust system operates within a decentralized framework, relying on a structured overlay called the Trust Overlay Network to efficiently manage and retrieve trust data. This overlay, similar to Distributed Hash Tables, provides an organized storage and rapid retrieval of trust values. PowerTrust improves the accuracy of global trust value through a look-ahead random walk strategy. However, it relies on a selected group of peers, similar to the reliance on pre-trusted peers.

Global trust is typically calculated from the aggregation of local trust values, which reflects the quality of interactions between peers. Authors of PeerTrust [26] identify five factors essential for evaluating a peer's trustworthiness, one of which is peer interaction quality. The five factors are averaged according to a weighting for each factor to compute the general trust value of a peer.

One of the complexities to capture in peer interactions is the presence of deceptive users and malicious activities, which is addressed in AbsoluteTrust [3]. The authors use a weighted average approach to give greater significance to trust values stemming from authentic interactions, thereby minimizing the impact of potentially malicious peers. Another interesting approach towards capturing the activities of malicious nodes is presented in [28]. The authors use the concepts of proximity, familiarity, and similarity from human social psychology to calculate the trust value. The authors argue for a holistic view of trust encompassing local and global trust values. Bayesian networks have also been applied to model trust relationships probabilistically [22]. The Bayesian approach quantifies direct interactions, assimilates peer feedback, and forms a peer's global trust in the network.

3 MODEL DESIGN

In this section, we develop our model of global trust assessment in P2P networks. We assume that the set of peers and the connections between them are represented by a *trust graph*, which is a weighted directed graph $\mathcal{G} = (N, E)$, where $N = \{1, \dots, n\}$ is the set of peers and the *local trust* $a_{ij} \in [0, 1]$ of peer i towards j is assigned to each edge $(i, j) \in E$. The local trust value a_{ij} is the reputation of peer j from the viewpoint of peer i. The dependence of weighted graph $\mathcal{G}$ on values a_{ij} is tacitly understood. We assume that $\mathcal{G}$ is simple (no loops, $(i, i) \notin E$ for every $i \in N$). In other words, no peer is allowed to assign the reputation to itself. We don't require that $\mathcal{G}$ is a complete graph, but the local trust value a_{ij} must be defined for each edge $(i, j) \in E$.

We follow the standard terminology of cooperative game theory [7, 10, 16]. The players in our game are the peers. A subset of peers $S \subseteq N$ is called a *coalition*. Our goal is to define the trust (reputation) of each coalition based on the trust graph. This means that we seek the suitable definition of a *(coalitional) game*

$$v\colon \mathcal{P}(N) \to \mathbb{R},$$

a function mapping every coalition in the powerset $\mathcal{P}(N)$ to a real number, where $v(\emptyset) = 0$. We assume that the coalitional trust can be decomposed into internal and external trust. When coalition S is formed, its members generate the *internal trust*, which corresponds to the total intercoalitional trust among members of S, and the *external trust* representing the reputation of members in S from the perspective of peers outside S. We want to combine the internal and external trust into the coalitional trust for S.

Our approach is based on combining internal and external trust additively. The former is the sum of all local trust values between the peers in a coalition, whereas the latter reflects the trust between the peers inside and outside the coalition, and it is based on the conservative (pessimistic) assessment of the trust of peers in the coalition. This idea can be formalized as follows.

Definition 3.1. Let $\mathcal{G} = (N, E)$ be a trust graph. For every coalition of peers $S \subseteq N$, define

$$S^* = \{j \in S \mid \text{there exists } i \notin S \text{ such that } (i, j) \in E\}.$$

The *trust game* $v_{\mathcal{G}}$ is given by

$$v_{\mathcal{G}}(S) = \sum_{\substack{i,j\in S\\(i,j)\in E}} a_{ij} + \sum_{j\in S^*} \min_{\substack{i\notin S\\(i,j)\in E}} a_{ij}, \qquad S \subseteq N. \tag{1}$$

Observe that the second summand in (1) is zero whenever $S^* = \emptyset$ by the definition of empty sum. This ensures that $v_{\mathcal{G}}$ is a coalitional game. The first term sums up the weights of the edges between nodes within the coalition S, which represents the internal trust, and the second term calculates the aggregated weight of the edges external to the coalition S, which amounts to the minimal trust exerted on the coalition from external nodes. Summing up, the definition of the coalitional function (1) is based on two principles.

(1) Trust values between different pairs of peers in the coalition are aggregated *additively*.
(2) Trust values exerted on a single peer from peers external to the coalition are combined using *minimum*.

The second principle is a pessimistic way to assess the total trust exerted on a peer $j \in S$ since the peer j is trusted only to the minimal degree of trust a_{ij} among those $i \notin S$ with $(i, j) \in E$. The use of minimum instead of, say, multiplication, avoids paradoxical situations when the peer highly trusted by many other peers would have very low trust.

The meaning of formula (1) is straightforward in the situation when the trust graph captures only the relations of maximal trust between peers.

Example 3.2. Let $\mathcal{G} = (N, E)$ be the trust graph such that $a_{ij} = 1$ for all $(i, j) \in E$. Then the trust game is

$$v_{\mathcal{G}}(S) = |\{(i, j) \in E \mid i, j \in S\}| + |S^*|, \qquad S \subseteq N,$$

which is just the number of trust relations in S plus the number of peers in S that are trusted by at least one peer outside S. We note that the non-monotonicity of the operator * makes further analysis of this game somewhat complicated.

We will establish the basic properties of trust games from the viewpoint of cooperative game theory. A coalitional game v is called *monotone* if

$$v(S) \le v(T)$$

for all $S, T \in \mathcal{P}(N)$ with $S \subseteq T$, and *superadditive* if

$$v(S) + v(T) \le v(S \cup T)$$

for all $S, T \in \mathcal{P}(N)$ with $S \cap T = \emptyset$.

Proposition 3.3. *Let $\mathcal{G} = (N, E)$ be any trust graph. Then the trust game $v_{\mathcal{G}}$ is monotone and superadditive.*

Proof. Let $S \subseteq T$ for $S, T \in \mathcal{P}(N)$. For each $j \in S^*$ we denote

$$M_{T\setminus S}(j) = \{i \in T \setminus S \mid a_{ij} = \min_{k\notin S} a_{kj}\}$$

and

$$M_{N\setminus T}(j) = \{i \notin T \mid a_{ij} = \min_{k\notin S} a_{kj} \neq \min_{k\in T\setminus S} a_{kj}\}.$$

Then

$$v_{\mathcal{G}}(S) = \sum_{\substack{i,j\in S\\(i,j)\in E}} a_{ij} + \sum_{j\in S^*} \min_{\substack{i\notin S\\(i,j)\in E}} a_{ij},$$

where

$$\begin{aligned} \sum_{j\in S^*} \min_{\substack{i\notin S\\(i,j)\in E}} a_{ij} &= \sum_{\substack{j\in S^*\\ i\in M_{T\setminus S}(j)\\ (i,j)\in E}} a_{ij} + \sum_{\substack{j\in S^*\\ i\in M_{N\setminus T}(j)\\ (i,j)\in E}} a_{ij} \\ &\le \sum_{\substack{i\in T\setminus S, j\in S\\ (i,j)\in E}} a_{ij} + \sum_{j\in T^*} \min_{\substack{i\notin T\\(i,j)\in E}} a_{ij}. \end{aligned} \tag{2}$$

Now, the monotonicity follows from the decomposition

$$\begin{aligned} v_{\mathcal{G}}(T) = {} & \sum_{\substack{i,j\in S\\(i,j)\in E}} a_{ij} + \sum_{\substack{i,j\in T\setminus S\\(i,j)\in E}} a_{ij} + \sum_{\substack{i\in S, j\in T\setminus S\\(i,j)\in E}} a_{ij} + {} \\ & \sum_{\substack{j\in S, i\in T\setminus S\\(i,j)\in E}} a_{ij} + \sum_{j\in T^*} \min_{i\notin T, (i,j)\in E} a_{ij}. \end{aligned}$$

and from (2) applied to the last two summands above.

As for superadditivity, let $S, T \subseteq N$ and $S \cap T = \emptyset$. Then

$$\begin{aligned} & v_{\mathcal{G}}(S) + v_{\mathcal{G}}(T) \\ & = \sum_{\substack{i,j\in S\\(i,j)\in E}} a_{ij} + \sum_{\substack{i,j\in T\\(i,j)\in E}} a_{ij} + \sum_{j\in S^*} \min_{\substack{i\notin S\\(i,j)\in E}} a_{ij} + \sum_{j\in T^*} \min_{\substack{i\notin T\\(i,j)\in E}} a_{ij}. \end{aligned}$$

Using (2) we get

$$\begin{aligned} & \sum_{j\in S^*} \min_{\substack{i\notin S\\(i,j)\in E}} a_{ij} + \sum_{j\in T^*} \min_{\substack{i\notin T\\(i,j)\in E}} a_{ij} \le \\ & \underbrace{\sum_{\substack{i\in S, j\in T\\(i,j)\in E}} a_{ij} + \sum_{j\in S^*} \min_{\substack{i\notin S\cup T\\(i,j)\in E}} a_{ij} + \sum_{\substack{i\in T, j\in S\\(i,j)\in E}} a_{ij} + \sum_{j\in T^*} \min_{\substack{i\notin S\cup T\\(i,j)\in E}} a_{ij}}_{b:=}. \end{aligned}$$

Since

$$v_{\mathcal{G}}(S \cup T) = b + \sum_{\substack{i,j\in S\\(i,j)\in E}} a_{ij} + \sum_{\substack{i,j\in T\\(i,j)\in E}} a_{ij}$$

we obtain

$$v_{\mathcal{G}}(S) + v_{\mathcal{G}}(T) \leq v_{\mathcal{G}}(S \cup T),$$

which concludes the proof. □

There are many solution concepts for coalitional games. Any such concept maps a coalitional game to the set of plausible *allocations*, which are just vectors

$$\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n.$$

Interestingly enough, every trust game has at least one allocation $\mathbf{x}^*$ in the core. This allocation is defined for each peer $j \in N$ simply as the sum of incoming local trust values:

$$x_j^* = \sum_{\substack{i \in N \\ (i,j) \in E}} a_{ij}. \tag{3}$$

Recall that the *core* of a coalitional game v is the convex polytope of efficient and coalitionally rational allocations,

$$C(v) = \left\{ \mathbf{x} \in \mathbb{R}^n \mid \sum_{i \in N} x_i = v(N), \ \sum_{i \in S} x_i \geq v(S), \text{for each } S \subseteq N \right\}.$$

Proposition 3.4. *For every trust game,* $\mathbf{x}^* \in C(v_{\mathcal{G}})$.

Proof. The allocation $\mathbf{x}^* = (x_1^*, \dots, x_n^*)$ defined by (3) is efficient since

$$\sum_{j \in N} x_j^* = \sum_{j \in N} \sum_{\substack{i \in N \\ (i,j) \in E}} a_{ij} = v_{\mathcal{G}}(N).$$

It is also coalitionally rational since, for every $S \subseteq N$, we get

$$\sum_{j \in S} x_j^* = \sum_{j \in S} \sum_{\substack{i \in N \\ (i,j) \in E}} a_{ij} = \sum_{\substack{j,i \in S \\ (i,j) \in E}} a_{ij} + \sum_{\substack{j \in S, i \notin S \\ (i,j) \in E}} a_{ij},$$

where the right-hand side above is greater or equal than $v_{\mathcal{G}}(S)$ by the definition of trust game. □

Important classes of coalitional games are the families of exact games and supermodular games [10]. Recall that a game v is called *exact* if, for each coalition $S \subseteq N$, there is an allocation

$$\mathbf{x} \in C(v) \text{ such that } v(S) = \sum_{i \in S} x_i.$$

A game v is *supermodular* if the inequality

$$v(S) + v(T) \leq v(S \cup T) + v(S \cap T)$$

holds for every $S, T \subseteq N$. It is well-known that every supermodular game is exact, but the converse generally fails. The following example shows that $v_{\mathcal{G}}$ may not be an exact game and, consequently, not supermodular.

Example 3.5. Let $N = \{1, 2, 3\}$ and $\mathcal{G} = (N, E)$ be the trust graph in Figure 1. The resulting trust game $v_{\mathcal{G}}$ is defined by $v_{\mathcal{G}}(\{1\}) = 0.1$, $v_{\mathcal{G}}(\{2\}) = 0.2$, $v_{\mathcal{G}}(\{3\}) = 0.3$, $v_{\mathcal{G}}(\{1, 2\}) = 1.5$, $v_{\mathcal{G}}(\{1, 3\}) = 1.3$, $v_{\mathcal{G}}(\{2, 3\}) = 1.6$, and $v_{\mathcal{G}}(N) = 2.2$. The typical core allocation (3) is $\mathbf{x}^* = (0.6, 0.9, 0.7)$.

The game is not exact. By contradiction, assume that for $S = \{1\}$ there exists a core allocation $\mathbf{x}$ such that

$$v_{\mathcal{G}}(\{1\}) = 0.1 = x_1.$$

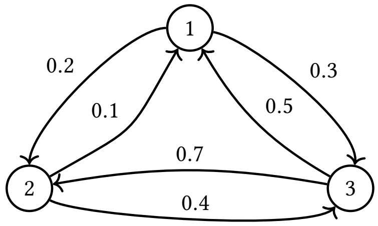

Figure 1: The trust graph from Example 3.5

This implies that

$$\begin{aligned} x_1 + x_2 &\geq v_{\mathcal{G}}(\{1, 2\}) = 1.5, \\ x_1 + x_3 &\geq v_{\mathcal{G}}(\{1, 3\}) = 1.3, \end{aligned}$$

therefore

$$\begin{aligned} x_2 &\geq 1.4, \\ x_3 &\geq 1.2. \end{aligned}$$

In conclusion,

$$x_1 + x_2 + x_3 = 2.7 > 2.2 = v_{\mathcal{G}}(N),$$

a contradiction.

3.1 Shapley Value

We identify the global trust values of peers with the Shapley values of peers in the associated trust game. The vector of Shapley values can be viewed as a fair allocation of trust to individual peers. Specifically, the *Shapley value* of a coalitional game v is the allocation $\phi(v) \in \mathbb{R}^n$ with coordinates

$$\phi_i(v) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(n - |S| - 1)!}{n!} \cdot \Delta_i v(S), \qquad i \in N, \tag{4}$$

where

$$\Delta_i v(S) = v(S \cup \{i\}) - v(S)$$

is the *marginal contribution* of player $i \notin S$ to coalition S in game v. The Shapley value is a solution concept that has the null player property, it is symmetric, efficient, and linear. By the last property, we can split the trust game into two coalitional games $u_{\mathcal{G}}$ and $w_{\mathcal{G}}$ each of which corresponds to one summand in (1), so that the Shapley value of

$$v_{\mathcal{G}} = u_{\mathcal{G}} + w_{\mathcal{G}}$$

becomes

$$\phi(v_{\mathcal{G}}) = \phi(u_{\mathcal{G}}) + \phi(w_{\mathcal{G}}).$$

To this end, we define the *internal trust game* as

$$u_{\mathcal{G}}(S) = \sum_{\substack{i,j \in S \\ (i,j) \in E}} a_{ij}, \qquad S \subseteq N,$$

and the *external trust game* as

$$w_{\mathcal{G}}(S) = \sum_{j \in S^*} \min_{\substack{i \notin S \\ (i,j) \in E}} a_{ij}, \qquad S \subseteq N.$$

Observe that the internal trust game is analogous to an induced-subgraph game studied in the case of undirected graphs [8].

PROPOSITION 3.6. *Internal trust game $u_{\mathcal{G}}$ is monotone, supermodular, and the Shapley value of peer $i \in N$ is*

$$\phi_i(u_{\mathcal{G}}) = \frac{1}{2}\left(\sum_{\substack{j\in N \\ (i,j)\in E}} a_{ij} + \sum_{\substack{j\in N \\ (j,i)\in E}} a_{ji} \right).$$

PROOF. Let $S \subseteq T$ for $S, T \in \mathcal{P}(N)$. Then

$$u_{\mathcal{G}}(S) = \sum_{\substack{i,j\in S \\ (i,j)\in E}} a_{ij} \leq \sum_{\substack{i,j\in T \\ (i,j)\in E}} a_{ij} = u_{\mathcal{G}}(T)$$

since each $a_{ij} \geq 0$ and

$$\{(i,j) \in E \mid i,j \in S\} \subseteq \{(i,j) \in E \mid i,j \in T\}.$$

Assume now that $S, T \in \mathcal{P}(N)$ are arbitrary. Then

$$u_{\mathcal{G}}(S) + u_{\mathcal{G}}(T) \leq u_{\mathcal{G}}(S \cup T) + u_{\mathcal{G}}(S \cap T)$$

since the two terms on the right-hand side contain the same terms as those on the left-hand side, and in addition also the sum of local trust values a_{ij} with $i \in S \setminus T, j \in T \setminus S$ or $j \in S \setminus T, i \in T \setminus S$.

The formula for Shapley value can be derived by following the proof of [8, Theorem 1] for undirected graphs. □

The Shapley value in the internal trust game has a simple interpretation — each peer is assigned the average of its "outgoing" and "incoming" local trust values.

The analysis of external trust game is more complicated. This is due to the fact that a nonzero coalitional game $w_{\mathcal{G}}$ is neither monotone nor superadditive. Indeed, it follows from the definition that $w_{\mathcal{G}}(N) = 0$ and $w_{\mathcal{G}}(S) > 0$ for some coalition $S \neq \emptyset$. Moreover, a nonzero game $w_{\mathcal{G}}$ is not balanced since any allocation $\mathbf{x} \in C(w_{\mathcal{G}})$ must have nonnegative coordinates, which means that the efficiency $\sum_{i\in N} x_i = w_{\mathcal{G}}(N) = 0$ yields $x_i = 0$ for each $i \in N$. By a similar argument, the Shapley value of a peer in $w_{\mathcal{G}}$ may be negative. The closed-form formula for $\phi(w_{\mathcal{G}})$ would not be as directly interpretable as the one for $\phi(u_{\mathcal{G}})$, since the definition of $w_{\mathcal{G}}$ involves non-monotonic operator *.

We will briefly comment on the Shapley value-based global trust from the perspective of two properties of EigenTrust, transitivity and conflation [2, 11]. *Transitivity* asserts that i's trust in k can be computed from i's level of trust in j, and j's trust in k. In our setting, we cannot formulate transitivity directly since our model does not require computing i's trust in k; see the following example with $i = 1$, $j = 2$, and $k = 3$.

Example 3.7. Let the set of peers be $N = \{1, 2, 3\}$ and the trust graph $\mathcal{G}$ be as in Figure 2. The corresponding trust game $v_{\mathcal{G}}$ is given by $v_{\mathcal{G}}(\{1\}) = 0$, $v_{\mathcal{G}}(\{2\}) = a_{12}$, $v_{\mathcal{G}}(\{3\}) = a_{23}$, $v_{\mathcal{G}}(\{1,2\}) = a_{12}$, $v_{\mathcal{G}}(\{2,3\}) = a_{12} + a_{23}$, $v_{\mathcal{G}}(\{1,3\}) = a_{23}$, and $v_{\mathcal{G}}(N) = a_{12} + a_{23}$. The Shapley value determines the global trust value of each peer, $\phi_1(v_{\mathcal{G}}) = 0$, $\phi_2(v_{\mathcal{G}}) = a_{12}$, and $\phi_3(v_{\mathcal{G}}) = a_{23}$. Note that neither the coalitional trust value $v_{\mathcal{G}}(\{1,3\}) = a_{23}$ nor the Shapley value $\phi_3(v_{\mathcal{G}}) = a_{23}$ indicates the influence of peer 1 on the trust in peer 3.

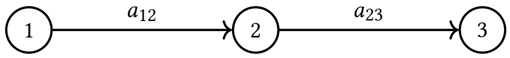

Figure 2: The trust graph from Example 3.7

It may seem from the global trust value $\phi_1(v_{\mathcal{G}}) = 0$ in Example 3.7 that our method exhibits the *conflation* of zero local trust and non-existing evaluation of a peer, which is one of the features of EigenTrust. However, this is not always the case, as Example 3.8 demonstrates.

Example 3.8. Consider the setting of Example 3.5 with (a) local trust $a_{32} = 0$ and (b) with no edge from peer 3 to peer 2. Then (a) and (b) yield different ratios of the Shapley values, cca 5:3:7 and 5:4:7, respectively.

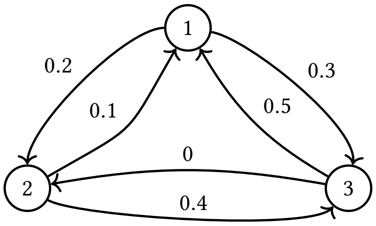

Figure 3: The trust graph from Example 3.8 (a)

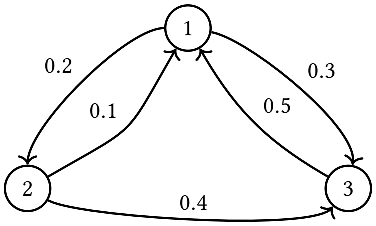

Figure 4: The trust graph from Example 3.8 (b)

3.2 Local Trust Estimation

The computation of coalitional trust according to Definition 3.1 is based on the trust graph with local trust values along its edges. It is common for peers to rate each other post-transaction in decentralized environments. A *transaction* [14] refers to a query posed by peer i to peer j. Adopting the rating mechanism [11], our transaction rating is set to 1 if the information provided by peer j in response to the query posed by i is authentic (*satisfactory*). Conversely, a -1 rating is assigned to inauthentic (*unsatisfactory*) information. Let sat_{ij} and $unsat_{ij}$ represent the total number of satisfactory and unsatisfactory transactions from peer i to j, respectively. We consider the non-normalized local trust defined by

$$s_{ij} = sat_{ij} - unsat_{ij}.$$

The quantity s_{ij} is further normalized to limit the variability in trust values resulting from disparate transaction frequencies. Normalization ensures that no peer disproportionately influences the trust values and that it lies within a consistent range eliminating the risk of skewed representation of trustworthiness in the network, especially in the presence of adversarial peers. We apply the

EigenTrust normalization methodology to obtain the normalized local trust value

$$c_{ij} = \frac{\max\{s_{ij}, 0\}}{\sum\limits_{k \in N} \max\{s_{ik}, 0\}}.$$

In case that

$$\sum_{k \in N} \max\{s_{ik}, 0\} = 0,$$

we set $c_{ij} = 0$. This convention not only guarantees that the definition of c_{ij} is mathematically sound, but also acknowledges that the concerning peer had no satisfactory transactions, thereby being conservatively allocated the lowest trust value. These normalized trust values form the edge weights of our trust graph and are used to compute the worth of each coalition. By leveraging these edge weights, we compute the Shapley value, which represents the global trust of each peer under different scenarios in our numerical experiments.

4 DESCRIPTION OF EXPERIMENTS

The following experiments were conducted, each designed to capture peer behavior under a distinct range of satisfactory and unsatisfactory transactions. The key focus of these experiments is to evaluate how accurately the Shapely-based trust computation captures the peer interactions in the network. We are testing the model's ability to grasp the true dynamics of peer interactions within a peer-to-peer network. In all the experimental scenarios the data were generated in such a way that every peer had at least one interaction with any other peer, which implies that the trust graph is a complete directed graph.

In the first scenario, the *Ideal Scenario*, we evaluate the model's performance under optimal conditions. Here, each peer's behavior is characterized by a uniform presence of satisfactory transactions. All the peers are benign and do not generate any unsatisfactory transactions. As an ideal setting, this scenario assesses the behavior of the model in global trust allocation when all the peers generate the same number of transactions. It serves as a reference point and provides a benchmark for analyzing peer behavior in subsequent scenarios.

The second scenario provides a more practical view of the network operations regarding transaction generation. Termed as the *Baseline Scenario*, the network generates a mix of satisfactory and unsatisfactory transactions. It simulates a more realistic network environment reflecting the irregularities and fluctuations in transactional interactions, depicting a setting where the existence of any adversarial peer within the network is unknown. Evaluating the model's performance in an uncertain environment with mixed transactional interaction offers a perspective on the model's responses to varying levels of discrepancies in transactions. This allows for a detailed analysis of the model's reliability and precision in differentiating between the nature of transactions. It is a preliminary step in evaluating the model's adaptability before introducing explicit adversarial peers in the next scenario.

In the third scenario, *Adversarial Scenario*, adversarial peers are intentionally incorporated into the network. Peers classified as adversarial generate more unsatisfactory transactions than non-adversarial peers. The influx of unsatisfactory transactions from adversarial peers necessitates evaluating the model's precision in trust value calculations. This scenario is important because it lets us test how well the trust computation can hold under extreme adversarial conditions.

In addition to our primary experiments, we also compared our model's trust computation with the basic variant of EigenTrust. In this variant, there are no pre-trusted peers. The comparison was conducted within our model's context of *Adversarial Scenario*. Comparing this scenario, in particular, underscores the model's capability to compute global trust values accurately in the presence of adversarial peers. This comparison was not only for identifying the same good and adversarial peers but also for exploring how our model aligns with or diverges from EigenTrust.

In summary, our goal is to show how our model performs in different scenarios—from the ideal to the challenging—and, in particular, how it measures against established methods like EigenTrust.

5 RESULTS OF EXPERIMENTS

The results of our experiments highlight the fairness and accuracy of computing the global trust values in different scenarios. Without unsatisfactory transactions, the Shapley value in the *Ideal Scenario* is equal for all the peers, which follows from the symmetry of Shapley value and Definition 3.1. This states that the global trust is uniform across the network in the presence of balanced transaction counts per peer. We conducted the experiments with three different peer groups, and the results were identical across each group, as illustrated in Table 1. This uniformity across the network reflects the model's fairness in trust allocation, showing that no peer receives undue advantage or disadvantage. It emphasizes that when the number of transactions is equal among peers, the quality of interactions takes precedence. The results establish a baseline for the model's ability to represent peer behavior in a uniformly positive transactional environment accurately.

Table 1: Results for the *Ideal Scenario*

Peers	*Transactions*	*Global Trust*
5	10	1
10	100	1
20	1000	1

The objective of the *Baseline Scenario* was to provide a practical viewpoint of the transaction generation in a network by incorporating unsatisfactory transactions. In this scenario, each peer generated satisfactory and unsatisfactory transactions within a given range uniformly at random. We experimented with three different peer groups in this scenario, and the transaction generation range per peer group is shown in Table 2. The randomness in transaction generation introduced an element of unpredictability, similar to interactions in a real-world P2P network, thereby highlighting the model's ability to adapt to varied transactional behavior.

As anticipated, the Shapley values in this scenario showed variations due to the randomness in the transaction generation. Moreover, the subsequent ranking of the peers based on their global trust values correlates with the number and nature of the transactions. For a 5-peer network, peer 5 is the most trusted and has the highest Shapley value of 1.32 while peer 4 is deemed least trusted

Table 2: The ranges for random generation of satisfactory and unsatisfactory transactions in the *Baseline Scenario*

Peers	*Transactions*
5	range(100,500)
10	range(500,1000)
20	range(500,1000)

as illustrated in Figure 5. For the 10-peer and 20-peer networks, a similar pattern was observed in the results based on the nature and number of transactions. The results in this scenario depict the model's ability to adapt and calculate global trust across transactions of varied numbers and nature. This difference in the global trust values can be seen in Figure 5, which compares trust values for a 5-peer network in the *Ideal Scenario* and *Baseline Scenario*.

Another noteworthy observation in this scenario was that the ranking of Shapley values of the peers and their typical core allocation (3) are identical. Therefore, peers with a higher number of satisfactory interactions receive a higher local trust value, leading to a higher Shapley value and, thereby, a higher global trust value.

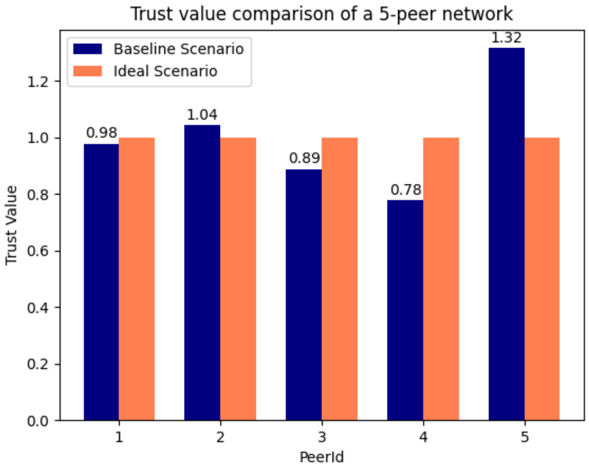

Figure 5: The comparison of global trust values between *Ideal Scenario* and *Baseline Scenario* in a 5-peer network

In the third scenario, *Adversarial Scenario*, we introduced adversarial peers into the network. These peers are characterized by generating a higher number of unsatisfactory transactions when compared to normal peers, challenging the model's ability to compute the global trust values accurately. *Normal peers* here refer to those not explicitly categorized as adversarial even though they generate unsatisfactory transactions. The process of transaction generation for normal peers in this scenario mirrored the approach of *Baseline Scenario*. As for adversarial peers, unsatisfactory transactions were generated within the notably high range of 1000 − 10000. This range was set exceptionally high to see the model's response in extreme adversarial conditions. As in the previous scenarios, we experimented with three different peer groups, and the number of adversarial peers differed in each group. The number of adversarial peers for each group is represented in Table 3.

Table 3: Adversarial peers in the *Adversarial Scenario*

Peers	*Adversarial*
5	1
10	2
20	5

The peers classified as adversarial received lower global trust values than their normal counterparts. In the 5-peer network, peer 2 was deemed as the adversarial peer, generating a high number of unsatisfactory transactions, and as evident from the line graph in Figure 6, it had the lowest global trust value underlining the impact of its adversarial behavior. This observation was similar for the larger peer groups. The 10-peer network, where peers 2 and 5 were categorized as adversarial, also received lower trust values. This pattern was consistent with the 20-peer network where peers 1,2,5,7,11 were marked as adversarial. The high variance in the global trust values is due to the randomness in the transaction generation.

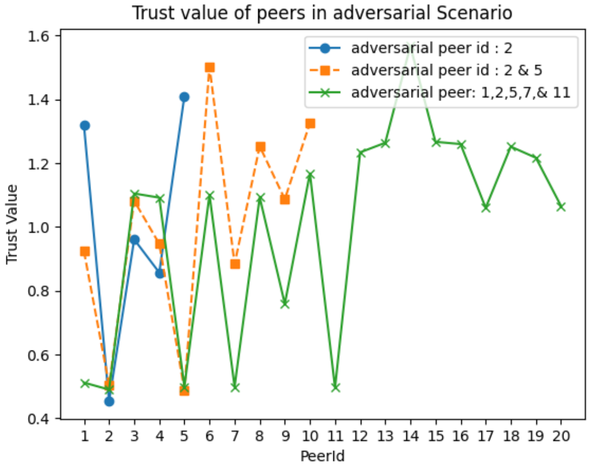

Figure 6: Trust values of peers in the *Adversarial Scenario*, where blue represents the 5-peer network with 1 adversarial peer, orange represents the 10-peer network with 2 adversarial peers, and green represents the 20-peer network with 5 adversarial peers

The global trust values from *Adversarial Scenario* were further compared with the basic variant of EigenTrust, which does not depend on pre-trusted peers. It initiates the iterative process with uniform initial trust values for all peers. The comparative analysis of the global trust values for a 10-peer network from our model with the EigenTrust variant is presented in Figure 7. Peers 2 and 5 were predefined as adversarial, and the global trust values assigned to these peers were in relative concordance with both models. We note the difference in the magnitude of the global trust values provided by both models, especially in the case of EigenTrust where the global trust values of the adversarial peers are zero. This difference in global trust values is attributed to the inherent variations in the methodologies of the two models. This comparative analysis with EigenTrust was instrumental in validating our model's accuracy in computing global trust values, particularly in scenarios involving adversarial peers. The consistency in ranking these adversarial peers between our model and EigenTrust underscores its effectiveness in accurately identifying and appropriately assigning lower trust values to such peers. Importantly, this comparison highlights our model's alignment with established trust computation methods, emphasizing its capability to distinguish and reflect the nuanced differences in peer behaviors within the network.

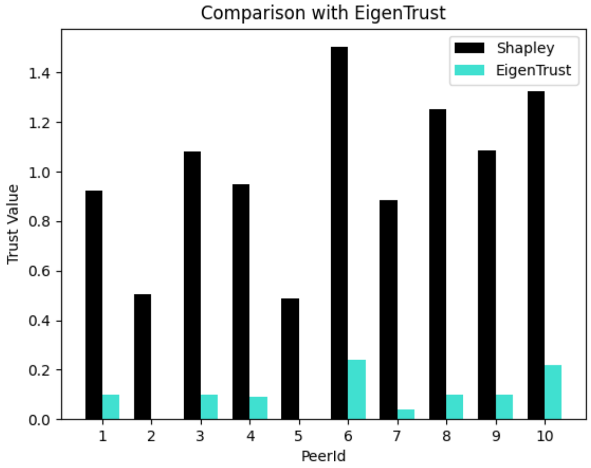

Figure 7: The comparison with basic variant of EigenTrust, where peers 2 and 5 were marked as adversarial

Our approach can also be extended to bigger peer groups. We note that for bigger peer groups computing the Shapely value efficiently will become challenging due to its exponential nature, nevertheless, this complexity can be solved with sampling algorithms which give a close approximation. While many sampling algorithms are available, we opted to experiment with the algorithm from [6], which samples over different permutations of the coalitions. We compared the global trust values computed in a 10-peer network from the *Baseline Scenario* with the sampling algorithm, and the results are displayed in Figure 8. The global trust values obtained from the sampling method using 1000 randomly generated permutations closely align with the actual global trust values. This suggests that the sampling method is effective in approximating the global trust values in the case of a bigger peer network.

6 CONCLUSIONS AND FUTURE RESEARCH

This paper presents a transferable utility coalitional game for modeling trust in a P2P network. Our concept of coalitional trust hinges on evaluating trust through the direct experience of peers within and outside coalitions rather than on transitive relationships, as in EigenTrust. We proved the resulting trust game is monotone, superadditive, and balanced. Further, we derived a peer's global trust value from the Shapley value of trust game. Our experimental results confirmed that this approach to calculating global trust captures peer behavior in the simulated network based on the generated transactions. We experimented with three peer groups, the largest group being the 20-peer network. Our approach can also be applied to bigger peer groups using sampling algorithms for approximating the Shapley value. Future research could beneficially extend beyond the scope of our investigation in several ways.

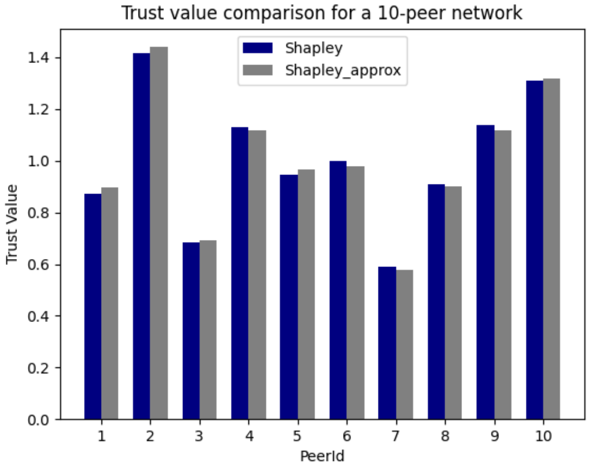

Figure 8: The comparison of global trust values in a 10-peer network with the sampling algorithm

- Many important families of coalitional games are *totally balanced* [16]. The open question is if every trust game is totally balanced. Note that a two-player subgame of a trust game is typically not a trust game since there may be no trust graph associated with the subgame.
- The related problem is whether there are core allocations of trust games other than those given by formula (3). Specifically, the goal is to *characterize the core* of the trust game in terms of vertices. This seems to be a nontrivial question since trust games are not supermodular by Example 3.5.
- *The effects of manipulation.* Our future work also entails analyzing the effects of the presence of peers whose local trust values may not faithfully capture their reputation and their subsequent impact on the coalition they are part of.

ACKNOWLEDGMENTS

The research of A. Bandhana and T. Kroupa was supported by the GAČR project GA21-17211S and partly funded by the AFOSR award FA9550-18-1-0097. The research of S. García was supported by the Strategic Support for the Development of Security Research in the Czech Republic 2019–2025 (IMPAKT 1) program granted by the Ministry of the Interior of the Czech Republic under No. VJ02010020 – AI-Dojo: Multiagent Testbed for Research and Testing of AI-driven Cybersecurity Technologies.

REFERENCES

[1] Karl Aberer and Manfred Hauswirth. 2002. An Overview of Peer-to-Peer Information Systems.. In *WDAS*, Vol. 14. Carleton Scientific, Paris, France, March 20-23, 2002, 171–188.

[2] Juan Afanador, Nir Oren, Murilo Baptista, and Maria Araujo. 2020. From eigentrust to a trust-measuring algorithm in the max-plus algebra. In *Proceedings of 24th European Conference on Artificial Intelligence - ECAI 2020*. IOS Press, Santiago de Compostela, Spain, 3–10.

[3] Sateesh Kumar Awasthi and Yatindra Nath Singh. 2020. Absolutetrust: algorithm for aggregation of trust in peer-to-peer networks. *IEEE transactions on dependable and secure computing* 19, 1 (2020), 176–189.

[4] Erman Ayday, Hanseung Lee, and Faramarz Fekri. 2009. An iterative algorithm for trust and reputation management. In *2009 IEEE International Symposium on Information Theory*. IEEE, Seoul, Korea, 2051–2055. https://doi.org/10.1109/ISIT.2009.5205441

[5] B. Beverly Yang and H. Garcia-Molina. 2003. Designing a super-peer network. In *Proceedings 19th International Conference on Data Engineering (Cat. No.03CH37405)*. IEEE, Bangalore, India, Mar. 5 2003 to Mar. 8 2003, 49–60. https://doi.org/10.1109/ICDE.2003.1260781

[6] Javier Castro, Daniel Gómez, and Juan Tejada. 2009. Polynomial calculation of the Shapley value based on sampling. *Computers & Operations Research* 36, 5 (2009), 1726–1730.

[7] Georgios Chalkiadakis, Edith Elkind, and Michael Wooldridge. 2022. *Computational aspects of cooperative game theory*. Springer Nature, Springer Nature Switzerland.

[8] Xiaotie Deng and Christos H Papadimitriou. 1994. On the complexity of cooperative solution concepts. *Mathematics of operations research* 19, 2 (1994), 257–266.

[9] Faezeh Sadat Gohari, Fereidoon Shams Aliee, and Hassan Haghighi. 2019. A dynamic local–global trust-aware recommendation approach. *Electronic Commerce Research and Applications* 34 (2019), 100838.

[10] Michel Grabisch et al. 2016. *Set functions, games and capacities in decision making*. Vol. 46. Springer, Springer International Publishing Switzerland.

[11] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. 2003. The Eigentrust Algorithm for Reputation Management in P2P Networks. In *Proceedings of the 12th International Conference on World Wide Web* (Budapest, Hungary) *(WWW '03)*. Association for Computing Machinery, New York, NY, USA, 640–651. https://doi.org/10.1145/775152.775242

[12] Heba A Kurdi. 2015. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems. *Journal of King Saud University-Computer and Information Sciences* 27, 3 (2015), 315–322.

[13] Lu Liu and Nick Antonopoulos. 2009. From client-server to p2p networking. In *Handbook of peer-to-peer networking*. Springer, Boston, MA, 71–89.

[14] Sergio Marti and Hector Garcia-Molina. 2006. Taxonomy of trust: Categorizing P2P reputation systems. *Computer Networks* 50, 4 (2006), 472–484.

[15] Xianfu Meng and Ge Zhang. 2020. TrueTrust: a feedback-based trust management model without filtering feedbacks in P2P networks. *Peer-to-Peer Networking and Applications* 13 (2020), 175–189.

[16] Bezalel Peleg and Peter Sudhölter. 2007. *Introduction to the theory of cooperative games*. Vol. 34. Springer Science & Business Media, Springer-Verlag Berlin Heidelberg.

[17] B Pourebrahimi, K Bertels, and S Vassiliadis. 2005. A survey of peer-to-peer networks. In *Proceedings of the 16th annual workshop on Circuits, Systems and Signal Processing*. Dutch Technology Foundation, Veldhoven, the Netherlands, 570–577.

[18] Chithra Selvaraj and Sheila Anand. 2012. A survey on security issues of reputation management systems for peer-to-peer networks. *Computer science review* 6, 4 (2012), 145–160.

[19] Zhenhua Tan, Xingwei Wang, Xueyi Wang, et al. 2016. A novel iterative and dynamic trust computing model for large scaled P2P networks. *Mobile Information Systems* 2016 (2016), 1–12.

[20] Chunqi Tian and Baijian Yang. 2014. A DS evidence theory based fuzzy trust model in file-sharing P2P networks. *Peer-to-peer Networking and Applications* 7 (2014), 332–345.

[21] Jingpei Wang, Jie Liu, et al. 2016. The comparison of distributed P2P trust models based on quantitative parameters in the file downloading scenarios. *Journal of Electrical and Computer Engineering* 2016 (2016), 6.

[22] Yao Wang and Julita Vassileva. 2003. Trust and reputation model in peer-to-peer networks. In *Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003)*. IEEE, Linköping, Sweden, 150–157.

[23] Yao Wang and Julita Vassileva. 2005. Bayesian network trust model in peer-to-peer networks. In *Agents and Peer-to-Peer Computing: Second International Workshop, AP2PC 2003, Melbourne, Australia, July 14, 2003, Revised and Invited Papers 2*. Springer, Springer, Berlin Heidelberg, 23–34.

[24] Yijing Xiao, Lian Zhu, and Xiang Li. 2021. A Review on Trust and Reputation Management Systems in e-commerce and P2P Network. In *2021 2nd International Conference on E-Commerce and Internet Technology (ECIT)*. IEEE, IEEE Computer Society, Hangzhou, China, 58–62.

[25] Li Xiong and Ling Liu. 2004. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering* 16, 7 (2004), 843–857.

[26] Li Xiong and Ling Liu. 2004. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering* 16, 7 (2004), 843–857. https://doi.org/10.1109/TKDE.2004.1318566

[27] Beverly Yang, Hector Garcia-Molina, et al. 2001. Comparing hybrid peer-to-peer systems. In *VLDB*, Vol. 1. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 561–570.

[28] Xingeng Zeng and Xuejun Yu. 2023. P2P based on network behavior analysis trust value calculation method. In *International Conference on Computer Network Security and Software Engineering (CNSSE 2023)*, Xiaohao Cai and Badrul Hisham bin Ahmad (Eds.), Vol. 12714. International Society for Optics and Photonics, SPIE, Harbin, China, 127140E. https://doi.org/10.1117/12.2683177

[29] Runfang Zhou and Kai Hwang. 2007. Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Transactions on parallel and distributed systems* 18, 4 (2007), 460–473.