Developing Trust and Reputation Taxonomy for a Dynamic Network Environment

Tanja Ažderska and Borka Jerman-Blažič
Jožef Stefan Institute
Ljubljana, Slovenia
e-mail: {atanja, borka}@e5.ijs.si

***Abstract*—Trust and reputation are the pillars of many social phenomena that shape the Internet socio-economic scene. The few existing taxonomies provide only initial insights into the ways trust benefits can be felt, but they are neither complete nor elaborated in a systemic manner. In this paper, we propose a multidimensional framework for designing and assessing the completeness and consistency of reputation mechanisms. Our framework is based on systemic principles; it identifies reputation system components, the factors that influence the system-design, defines the interrelations between the former and the dependencies on the later. By considering the human-centric, dynamic and context-dependent trust-establishment, we detect five major factors that guide reputation systems' design. The presented framework is applied to BarterCast, a reputation mechanism that extends the current P2P network protocol – BitTorrent, and is deployed in the BitTorrent-client Tribler.**

Keywords–trust; taxonomy; reputation mechanisms; system theory; context

I. INTRODUCTION

Catering the variety entities and interactions between them, the Internet is an environment where the pervasive risk and inherent uncertainty pose a requirement for new tools to support decision making in such circumstances. Apart from the commercial expansion of the Internet, traditional networking among people relies on unwritten social protocols, like gossiping and rumors, to judge about one's trustworthiness and reliability. A global consensus on person's reputation has neither been required nor needed, yet the social model has been successfully supporting legitimate interactions by identifying untrustworthy individuals. The advent of social networking and computational semantics opens up a myriad of opportunities for merging the social and dynamic character of trust with the technical possibilities offered by Information and Communication Technologies. The growth of user-generated content, the vast offer of service providers, and the wealth of collaborative and market-based platforms, have introduced additional levels of complexity in the processes of information filtering and decision making. They require systemic approaches for treating trust and reputation (T&R). Hence, the success of online trust-based methods depends largely: a) on the research aimed at identifying where these methods offer the most benefit and b) on the quality of the frameworks where the principles of system design reside. Our work is a contribution in both of these directions. The framework defined here is guided by the principles of system theory and taxonomical categorization. To present the outlined topics and the results, the paper is organized as follows: the following section briefly examines related work in T&R, defines the notions of T&R and the progress towards their formalization. The succeeding sections outline the methodology used and introduce the proposed framework based on the principles of General Systems Taxonomy. Practical observations, supplemented with insights from other trust taxonomies and proposals, are elaborated through the framework, enabling the addition of a new level of granularity to the existing research map on T&R. The next section illustrates the application of the newly designed approach for the specific case of distributed environments, mapping the BarterCast reputation mechanism across the dimensions of the framework. The paper concludes with a review of the presented topics and a constructive discussion, outlining our future research plans.

II. THE NOTION OF TRUST AND REPUTATION IN A NETWORK ENVIRONMENT

Trust is a social manifestation we face on a daily basis. However, its definition is hard to grasp. One reason for this is its strong contextual dependence. However, another reason that is crucial and that refers to the practical side of system design is the non-linear nature of the social phenomena ascribed to trust, such as belief, regret, forgiveness, subjective judgment, etc. These comprise the affective (emotional, and thus the human) side of trust, and do not allow the system to be designed according to the elegant principles of mathematical linearity and probabilistic averaging. Therefore, incorporating trust into online scenarios analogous to those in the traditional social networks has not been very fruitful. The literature on T&R in social sciences is exhaustive [1–3]. The common attitude supports the aspect of relying on others' willingness to perform beneficial actions for one's welfare. Based on Gambetta's attitude on trust [4], we give the following initial definition:

Definition 1. Trust is the belief, i.e., the subjective probability that an entity will perform in a way likely to bring the expected benefit, or not to do unexpected harm.

Despite the interchangeable use of the concepts of T&R, reputation deserves its own and more specific definition that would stress how it differs from trust.

 ISBN: 978-1-61208-183-0

Definition 2. Reputation is the empirical memory about an entity's past behaviour, performance, or quality of service, in a specific context, i.e., domain of interest.

Hence, reputation is the amount of context-aware trust that an entity has created for itself, i.e., a quantitative representation of trustworthiness bounded by the domain of interest. Reputation results from calculation and assessments and is based on facts rather than mere opinion and belief (e.g., I trust you because of your good reputation), unlike trust, which is a more subjective form of evaluating someone's performance (e.g., I trust you despite your bad reputation).

In circumstances where one entity relies on another entity, trust choices include a certain level of risk. Josang defines two different types of trust – Reliability and Decision trust [5]. The former covers the aspect of trust as stated by Definition 1. The latter considers the risk brought about by the uncertainty of transactional outcomes and is used to extend the first definition, which now gains the following structure:

Definition 3. Trust is the extent to which one entity is willing to depend on others' decisions, accepting the unpredictable risk of a negative (undesired) outcome.

Much of the research on trust evaluation has its roots in Game Theory, where concepts like quality, cost and utility are more formally defined [6]. The most fundamental trust problems in game theory are captured by the Prisoner's Dilemma [7], a principle that demonstrates the trade-offs in people's decisions to maximize either their own profit or the overall outcome of the game. The Prisoner's Dilemma is also used in strategies for fostering contribution in some technical implementations online, such as BitTorrent's tit-for-tat policy [8]. Despite the early work on trust relations and conflict resolution in game theory, the notion of computational trust appears significantly later, when Marsh establishes the basis of formal trust in distributed artificial intelligence [9].

A work that relates quality and uncertainty within the framework of reputation is the Akerlof's study on the "market of lemons" [10]. Reputation mechanisms (henceforth denoted as RMs) are used to balance the information asymmetry, by helping buyers make better-informed decisions and incentivizing sellers to offer high-quality goods. Akerlof makes an instructive distinction between the *signaling* and the *sanctioning* role of RMs, which was only recently considered in computer science [11]. The computational formalization of T&R is mainly done by the use of a mathematical and formal logics apparatus. We restrain from presenting that body of work here, as this paper is part of the *identification* phase of a RM, rather than its *modeling* process.

III. TRUST TAXONOMIES AND THE NEW APPROACH

Several taxonomies of trust have been designed in the past decade [5], [12–14]. As a categorization of system entities, components and their interrelations, taxonomy is hardly a useful systemic approach if it only identifies the RM entities. Cohesive factor for all systems, which has not been tackled by any of the known taxonomies, is the identification of connections between the RM components. The framework presented in this paper not only specifies that, but it also provides analysis in several dimensions across the factors influencing RM's design. To entitle this work a systemic approach, we turn to the principles of General Systems Taxonomy and determine the position of RMs in the general systems space. Our taxonomy differs from the existing in the field in a few crucial aspects: 1) It follows a systemic approach of revealing the design issues in building RMs and relies on simple systemic principles; 2) It relates the RM subsystems in a way that allows understanding of their interrelations, but also of their connection to the environment where the overall system evolves; 3) It sets a common ground for the widespread, but scattered, research on computational T&R; 4) Most importantly, it determines the 'system' concept applicability of the defined taxonomy and detects the factors required for its completeness. The main content of this framework is outlined in the text that follows.

One of the most prominent works in General Systems Taxonomy is that of Nehemiah Jordan [15], according to which a system's taxonomy has three organizing principles: 1) Rate of change, 2) Purpose, and 3) Connectivity. Each principle defines two antitheses, resulting in the three pairs of properties shown in Table 1. Within this general framework, we also position the systemic properties of RMs, and use them later in developing the novel reputation taxonomy.

Dynamicity (D): Static systems are those that exhibit no change in a defined time-span. RMs are expected to provide long-term incentives and support decision-making in a dynamic manner. To do that, they consider the quality of experiences of the system entities and the history of transactions among them.

Environmental-orientation (E): The principle of purpose determines the direction of energy/information flow inside or outside the system. The two possibilities are a system-directed flow or environment-oriented. The former tends to maintain stable and constant conditions inside the system, whereas the latter modifies the system to obtain a desired state or bypass certain disturbances.

TABLE I. ORGANIZING PRINCIPLES OF JORDAN'S SYSTEMS TAXONOMY (the categories to which we assign RMs are bolded and italicized)

Rate-of-change	Purpose	Connectivity
Structural (static)	Purposive (system-directed)	Mechanistic (non-densely connected)
Functional (dynamic)	***Non-purposive (environment-directed)***	***Organismic (densely connected)***

Dense connectivity (C): The principle of system connectivity states two possibilities: systems are a) mechanistic, i.e., not densely connected and the removal of parts or connections produces no change in the remaining components; or b) organismic, i.e., densely connected and the change of a single connection affects all the others. RMs depends heavily on the interactions among system entities. They are of inherently non-linear nature, implying that the outcome of each interaction has no predictable impact on the overall RM.

The significance of considering General Systems Taxonomy is in the clarification and simplification of the often-misused concept of a system. Our work establishes RMs as real systems, and by using sufficient generality and simplicity, categorizes them as dynamic (D), densely connected (C) and environment-oriented (E). In the next section we move to identification of the RM components, and determine their interrelations.

IV THE TAXONOMY FRAMEWORK

The new taxonomy proposed here covers more aspects of the issue and applies to the trust taxonomies and to the RM design: 1) It categorizes common and important concepts in the research on RMs, establishing a common systemic vocabulary; 2) It represents a novel approach to multi-dimensional mapping and assessment of the completeness and consistency of a RM; 3) It introduces additional granularity in the current taxonomic map of RMs, considering the notion of reputation and its application to the RM components; 4) It employs the D-C-E nature of RMs to detect additional factors that influence RMs design, providing better completeness of the taxonomy.

As a skeleton, we take Stanford's taxonomy [12], shown in Table II. The framework resulting from our work that was imposed on the skeleton allows a direct mapping of the models across the factors-dimension and subsystems-dimension in a consistent manner. This enables an immediate establishment of the interdependence between: a) the various RM subsystems; b) the subsystems and the RM as a whole; c) the RM and the general system where the RM is deployed; d) the RM and the environment where the overall system resides.

TABLE II. BREAKDOWN OF THE REPUTATION SYSTEM COMPONENTS (Marti *et al.*)

Reputation Systems		
Information Gathering	***Scoring and Ranking***	***Response***
Identity Scheme Information Sources Information Aggregation Stranger-Policy	Good vs. Bad Behavior Quantity vs. Quality Time-dependence Selection Threshold Peer Selection	Incentives Punishments

In order to specify the requirements and the implications of designing an efficient reputation mechanism, Marti et al. considered the following factors of impact: a) The limitations and opportunities imposed by the system architecture where the RM is deployed; b) The expected user behaviour; c) The goals of adversaries. As stated in Section III, RMs are of a D-C-E nature. Table III contains an assessment of the factors of impact on a D-C-E scale. It demonstrates which of these factors do not consider one or more system properties (D, C or E).

TABLE III. EVALUATING THE FACTORS OF IMPACT ON D-C-E SCALE (Y denotes "Yes" – does consider; N denotes "No" – does not consider)

Factor / Property	User behavior	System Architecture	Goals of adversaries
Dynamicity *(D)*	Y: through churn	***N:needed to capture environment evolution***	Y: accounted for in the adversarial strategies
Densely connected *(C)*	***N: very small number of users can have a large impact on the system***	***N: the reputation mechanism as a subsystem of the overall system has a huge impact***	***N: necessary to take into consideration for providing the resilience of the system***
Environment-oriented *(E)*	***N: so far only as system-oriented, neglecting the influence of the environment on user behavior***	Y: by considering the various properties of a centralized, distributed, hybrid	Y: few types of attacks (Sybil attack, collusion) resemble this nature of the reputation system

The content of Table III shows that the C-nature of the RMs is not considered at all. The interactions and relations between entities and the environment presented are not captured by any of the known trust taxonomies, and consequently, by none of the computational trust models.

Active Entity behaviour. As a first distinctive element from Stanford's taxonomy, we introduce the more general concept of reputation entity and recognize "users" as only one type of these entities. Entity refers to a party who participates in the process of reputation evaluation, either as an evaluator or as an evaluated side. We distinguish two types of reputation entities, active and passive. The former are enrolled actively in the reputation process: aggregating and disseminating information, acting upon certain triggers, and evaluating each other's and the trustworthiness of the passive entities. Examples are agents, users, peers in P2P networks, etc. In contrast, passive entities are those whose trustworthiness is evaluated by the active entities; they do not provide any feedback, and do not participate in the aggregation of reputation scores. Examples are items, comments, video/audio content, etc.

RMs must exhibit a high adaptive capability to address the issues outlined above. An important part of the solution is both the hard-technical and the soft-usability aspects of the system. The former may include availability and connectivity checking to form an overlay of reliable entities, while the latter will require bootstrapping techniques for the new-coming entities, and incentive policies for those who have already established some history of experiences.

Resilience and evolutionism. The circular, interlocking and time-dependent relationships among RM components

 ISBN: 978-1-61208-183-0

are also important in determining entities' behaviour. There often are properties of the overall solution that might not be found among the properties of its building components, leaving the behaviour of the whole system impossible to be explained in terms of the behaviour of its parts. In fact, this is a common property of complex systems that depend on social dynamics.

Context. Reputation information becomes significant only after it is put into a relevant context. Context is the set of circumstances or facts that surround a particular event or situation. Despite the various types of trust defined in the literature, only a few definitions consider its context-dependency. However, none of the known approaches considers the impact of context on the separate RM components [16]. Most of the current proposals employ it for content-filtering purposes. By including context information in the reputation evaluation, not only can the level of the entities' expertise be obtained, but also the domain of interest where this expertise is relevant.

Time. The time as well is an insufficiently considered factor that influences many of the design choices. Some relations between reputation and time have been studied extensively; however, many important time-properties have not received the expected attention. Each subsystem of the RM is influenced by decisions that should consider the permanency of the identifiers, the recentness of information, the time-stamp of feedback actions, the convergence of the reputation value, synchronization of time-driven actions, updates of the reputation values, etc. The time-issues in a RM depend on the given subsystem where they appear. Some of the ways to approach these issues include: introduction of a sliding window over which the reputation information gains certain importance; time-discounting of the various (meta) results obtained at a certain point in time or a combination of the discounting factors together with the entities' reputation in a certain context.

Privacy. The interest in information is accompanied by privacy requirements. Although privacy is a research field on its own, some design points of RMs directly face privacy challenges. RMs are expected to keep balance between the heterogeneity of users and their interest in information. As the main purpose of RMs is the embodiment of trust on the Internet, it would be useful to investigate where the offline forms of regulation-by-law fit in the online world and whether they can be incorporated to help the establishment of trust.

On the Internet, people tend to tolerate worse experiences, acknowledge lower competences, exhibit lower privacy requirements, accept greater risks and act under higher uncertainty. The fast convergence of the reputation effects degrades reputation as soon as the information propagates the network. By limiting this effect to the relevant context, RMs will exhibit better adaptability and flexibility to user demands. It is multidimensional as it is based on the factors identified to capture the RM's D-C-E nature and defines their relation to the RM subsystems.

V. THE EXAMPLE OF BART CAST

The reason we have chosen BarterCast (BC) [17] for taxonomical mapping is that it is fully distributed, but also a deployed RM in the BitTorrent content-sharing client Tribler [18]. Its design premise is that social phenomena (friendship, trust and sense of community) affect positively the system usability and performance. We briefly introduce BC, and then map it across the framework dimensions.

Information Gathering: For peers (client software), BC uses permanent IDs (*PermIDs*) based on a public key scheme, validated by a challenge-response mechanism to prevent spoofing. Users are referred to by *pseudonyms*. The social network creation is facilitated by the ability to import contacts from other networks (MSN, Gmail). Context information is stored in *MegaCaches* to support trust-based social groups. For content discovery, a *semantic overlay* of *taste buddies* (peers with similar taste) is maintained and discovered by a *gossiping protocol*. Exchanging data is done by 1) *exploitation*, with the buddies, or 2) *exploration*, with a random new peer. Only *direct experience* (for aggregated amount of service) is exchanged during the gossip. Peers maintain *private* (based on an entity's interactions with a single entity) and *shared history* (about interactions with all entities) and *subjectively* calculate the reputation. BC considers paths of two hops, due to the small-world effect in P2P file-sharing networks.

Scoring and Ranking: The network of interacting entities in BC is represented as a graph. As input statistics, both the quantity (upload in MB) and the quality (the positive contribution) of the service are considered in the scoring algorithm. The private and the shared history form the peer's local graph, which is used as an input for the maxflow algorithm. It computes the maximum flow over all possible paths, from a source node to a sink (target) node. The result is the highest reputation that a source node can give to a target node, and it is a scalar value in the [-1, 1] interval.

Response: BC introduces a few types of incentives. First, a *cooperative download* is used to improve the download performance of group members. Second, in addition to the BitTorrent's tit-for-tat (which gives peers only a short-term incentive to upload), BC incorporates long-term incentives by implementing a ranking policy, which allows interested peers an initial cooperation in the order of their reputation. Third, it cherishes the peers' sense of community, which on the long run acts as a social norm for contributive behavior. Finally, by introducing costly procedures for using system resources, BC discourages malice, providing an additional incentive for contributive peers. In order to select interacting partners, BC introduces a banning policy. The choice of whom to allow the use of resources is made according to the peers' reputation, where a reputation is required to be

 ISBN: 978-1-61208-183-0

above a negative threshold (to differ strangers from disreputable peers).

Stranger Policy: Strangers are tackled by the bootstrapping process in Tribler, in two ways. To obtain an initial list of neighbors, peers use a set of pre-known super-peers to bootstrap into the network. Then, there is also an overlay swarm with no central component that can also be used for initial bootstrapping, content discovery, and other information exchange.

Discussion. The way BC maps to the framework is presented in Table IV. The results suggest a space for substantial improvements. BC does not implement any type of integrity check of reputation entities and their relations across any of the defined factors. This can be achieved by introducing witnessing scheme, similar to that in [19]. Furthermore, coping with the dynamics is mainly handled on a network level through availability and connectivity check, considering only the node-churn in the network. Thus, many time-properties important for achieving consistency among the components are not taken into account. Although the validity of the reputation information is based on the 10 most recent transactions, this choice is made in a fixed manner rather than according to the system or interaction dynamics. One way to include the timeliness of reputation information in this RM is by introducing a time-discounting factor that will give different weights to the information according to its recentness. Another thing that BC lacks is a policy for penalizing malice. In an open, anonymous and dynamic environment, providing mechanisms that hold community members responsible for their actions is of crucial importance. Despite accounting for *taste similarity*, *taste* is much more subtle than preference. Results from Behavioral Economy show that users are often unaware of their taste, even for experiences from previously felt outcomes [20]. The possibility of importing contacts in Tribler from other social networks requires well-defined privacy policies, assurance for the system interoperability, and context-switching awareness. None of this is elaborated enough to justify the design choice for this kind of property. Although there is an *erase from profile* option, the download history for each peer is publicly visible for exploration and discovery. BC is based on the premise that, although non-resistant to cheating, real-world communities work well with millions of users. However, this does not speak about the impact these entities can have on the overall system welfare. For instance, only a small percentage of peers in a file-sharing community contribute the largest amount of resources in the network. False self-representation, as well as collusion, can have an impact on the cost that largely outweighs the benefit of designing and maintaining a RM. Finally, despite exploiting the small-world phenomenon for better gossiping in BC, this phenomenon is not an indication of any organizing principle of the nodes in the network. There is a certain structure a network should have in order for the small-world concept to be applied in the first place [21], [22]. In addition to applying re-organizing principles of the nodes' positions for satisfying the necessary structure, the BC reputation mechanism would benefit a great deal (with respect to both performance and accuracy of the result) from performing a full gossiping, instead of the current two-hop message exchange.

VI. Concluding remarks and Future work

Building reputation is primarily a social process. Online environments can largely benefit from trustworthy choices. Handling numerous online experiences in a short time-span requires highly scalable solutions for trust establishment. In such a dynamic environment, having no RM to capture interaction trends is equal to being equipped for a world that no longer exists. The presented framework is a systemic approach to designing dynamic, densely connected and environment oriented RMs. As major factors that influence RM design we included *context, time, privacy, active entity behavior, resilience and evolutionism*, in addition to *system architecture*. The insights were incorporated into a multidimensional framework, together with the RM subsystems, to establish their interconnections and dependencies. The result is a more granular categorization of design choices/decisions. Finally, we mapped BC as a representative distributed and socially inspired RM onto our framework, revealing some weaknesses and proposing improvements of its design.

Future step in our work will be a system-modeling approach for resolving the design issues for a novel RM. According to the principles outlined in this work, the model will be premised on dynamicity, adaptability and evolutionism. We will employ System theory methods, allowing the use of sophisticated tools for evaluation and verification, something that has not been proposed so far by any of the approaches in the field. Moreover, it is a step towards the standardization of the design process of RMs. A multi-disciplinary approach is thus essential for limiting or extending the possibilities offered by ICT for preserving practicality, but adding innovation as well.

References

[1] J. H. Fowler and N. A. Christakis, “Cooperative behavior cascades in human social networks,” *Proceedings of the National Academy of Sciences*, vol. 107, no. 12, pp. 5334-5338, Mar. 2010.

[2] John Conlisk, “Why Bounded Rationality?,” *Journal of Economic Literature*, vol. 34, no. 2, pp. 669-700, 1996.

[3] C. Castelfranchi and R. Falcone, “Trust is much more than subjective probability: Mental components and sources of trust,” *32nd Hawaii International Conference on System Sciences - Mini-Track On Software Agents, Maui*, vol. 6, 2000.

[4] D. Gambetta, “Can We Trust Trust?,” *TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS*, p. 213--237, 1988.

[5] A. Josang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decision Support Systems*, vol. 43, no. 2, pp. 618-644, Mar. 2007.

[6] S. H. Chin, “On application of game theory for understanding trust in networks,” in *2009 International Symposium on Collaborative Technologies and Systems*, Baltimore, MD, USA, 2009, pp. 106-110.

[7] D. Fudenberg and J. Tirole, *Game Theory*. The MIT Press, 1991.

[8] B. Cohen, “Incentives Build Robustness in BitTorrent,” 2003.

[9] S. P. Marsh, “Formalising trust as a computational concept,” 1994.

[10] G. A. Akerlof, “The Market for ‘Lemons’: Quality Uncertainty and the Market Mechanism,” *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488-500, 1970.

[11] C. Dellarocas, “The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms,” *Management Science*, vol. 49, no. 10, pp. 1407-1424, Oct. 2003.

[12] S. Marti and H. Garciamolina, “Taxonomy of trust: Categorizing P2P reputation systems☆,” *Computer Networks*, vol. 50, no. 4, pp. 472-484, Mar. 2006.

[13] H. Alani, Y. Kalfoglou, and N. Shadbolt, “Trust strategies for the semantic web,” *PROCEEDINGS OF THE TRUST, SECURITY AND REPUTATION WORKSHOP AT THE ISWC04*, vol. 7, p. 78--85, 2004.

[14] T. D. Huynh, “Trust and Reputation in Open Multi-Agent Systems,” Jun-2006.

[15] N. Jordan, *Themes in Speculative Psychology*. Routledge, 2003.

[16] T. Heath, E. Motta, and M. Petre, “Computing Word-of-Mouth Trust Relationships in Social Networks from Semantic Web and Web2.0 Data Sources.”

[17] M. Meulpolder, J. A. Pouwelse, D. H. J. Epema, and H. J. Sips, “Bartercast: A Practical Approach to Prevent Lazy Freeriding in P2P Networks.”

[18] J. A. Pouwelse et al., “TRIBLER: a social-based peer-to-peer system,” *Concurrency and Computation: Practice and Experience*, vol. 20, no. 2, pp. 127-138, Feb. 2008.

[19] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The Eigentrust algorithm for reputation management in P2P networks,” in *Proceedings of the twelfth international conference on World Wide Web - WWW ’03*, Budapest, Hungary, 2003, p. 640.

[20] D. Ariely, G. Loewenstein, and D. Prelec, “Tom Sawyer and the construction of value,” *Journal of Economic Behavior & Organization*, vol. 60, no. 1, pp. 1-10, May 2006.

[21] J. Kleinberg, “The Small-World Phenomenon: An Algorithmic Perspective,” *IN PROCEEDINGS OF THE 32ND ACM SYMPOSIUM ON THEORY OF COMPUTING*, p. 163--170, 2000.

[22] O. Sandberg, “Searching in a Small World,” p. 39--57, 2005.

TABLE IV. MAPPING BARTERCAST ONTO THE NEW FRAMEWORK

Subsystem		Factor	Context	Time	Privacy	RE	AEB
Information gathering		**ID Scheme**	Non-linkable; Verifiable	permanent ID (PermID)	pseudonyms	N (machine-dependent ID)	challenge-response; combats free-riding; Sybil-vulnerable
Information gathering		**Info Sources**	taste-buddies; subj. Reputations	10 most recent interactions	N	semantic overlay	considers 2 hops; employs small-world concept
Information gathering		**Info. Aggregation**	MegaCaches for context-info; private and shared history	N	gossiping only about direct experience	exploitation & exploration	false feedback restricted by the information capacity of edges; collusion possible
Information gathering		**Integrity check**	N	N	N	N	N
Scoring and ranking		**Inputs**	Quantity (Upload in MB); Only positive contribution;	N	N	N	History of transactions
Scoring and ranking		**Comp. engine**	Maximum-flow algorithm based on *arctan* function	N	Privacy as a metric	cooperative downloading protocol	No learning; Depends on system vulnerability
Scoring and ranking		**Outputs**	Single value in the interval [-1, 1]	N	N	optimistic un-choking	GUI for browsing peers
Response		**Threshold**	negative reputation threshold	Sliding window over 10 transactions	Preference similarity	N	Reputation-based peer selection
Response	Incentives	**Reward**	Improved service; Rank policy; tit-for-tat	N	N	Cooperation driven	relies on social altruism of taste-buddies; does not take risk into account
Response	Incentives	**Punish**	N	N	*Erase from profile* option	N	N
Stranger policy			N	N	N	N	bootstrapping; connectivity & availability check