




A Novel Serious Game for Trust-Related Data Collection in Supply Chains

Marco Niemann¹ , Frederik Elischberger¹, Pia Diedam¹,
Jorge Hopkins¹, Rewat Thapa¹, Diego de Siqueira Braga¹ ,
Bernd Hellingrath¹, Anthony Lins², Rennan Cavalcante Raffaele²,
and Fernando Buarque de L. Neto³ 

¹ Westfälische Wilhelms-Universität Münster, Münster, Germany
{marco.niemann,f_elis01,p_died04,j_hopk01,r_thap01,diego.siqueira,
bernd.hellingrath}@uni-muenster.de

² Catholic University of Pernambuco, Recife, Pernambuco, Brazil
anthony@unicap.br

³ University of Pernambuco, Recife, Pernambuco, Brazil
fbln@ecomp.poli.br

Abstract. Trust is considered an essential factor to develop and maintain business and supply chain relationships. However, it is hard to investigate its mechanisms due to the lack of supply chain trust-related datasets. This lack forces researchers to use artificially and often self-generated datasets which limit the validity of results and comparability with different approaches. Striving for the generation of less artificial trust datasets, this paper presents a novel serious game to gather trust information in a B2B supply chain setting.

Keywords: Serious games · Trust · Supply chains · Behavioral experiment · Data analytics · Docker · Online game · Multiplayer game

1 Introduction

This paper presents the finalized version of a new serious game aiming at the collection of data regarding the trust behavior of individuals in supply chains: the *Game of Trust*. Unlike a conventional simulation games for training or proof of concepts, serious games make it easier to collect, catalog and save the game data and other analysis without interrupting game flow.

2 The Game of Trust

2.1 Concept

The developed serious game was first introduced in [1]. Based on trust-related experiments like the Mango Chain Game [2], the Trust and Trace Game [3], and

the Beer Game [4], the game provide insight into supply chain’s trust relationships and interaction with neighboring tiers.

The *Game of Trust* followed the general guideline for designing serious games projects proposed by Lang et al. [5], adapting it in order to incorporate the requirement of a multi-player game. The game setting consists of a supply chain (SC) with multiple trading partners at each level. The research objective of the game is to collect data regarding the behavior of the players when they are exposed to the possibility of trusting or distrusting another player. The participants have to trade goods of two different qualities inside the supply chain with the possibility of hiding and revealing the mentioned quality. The game is composed of several rounds, each round divided in four phases: **Negotiation**,

Delivery, **Financial Closure** and **Questionnaire**.

The *Negotiation* phase is a three stepped sub-process in which the upper tier SC member can make an offer to one or multiple members of the next lower tier (e.g. $M \rightarrow W$). This entity can then adjust or confirm the received offer handing back the final acceptance or denial decision to the offer-issuing entity¹ (Fig. 1).

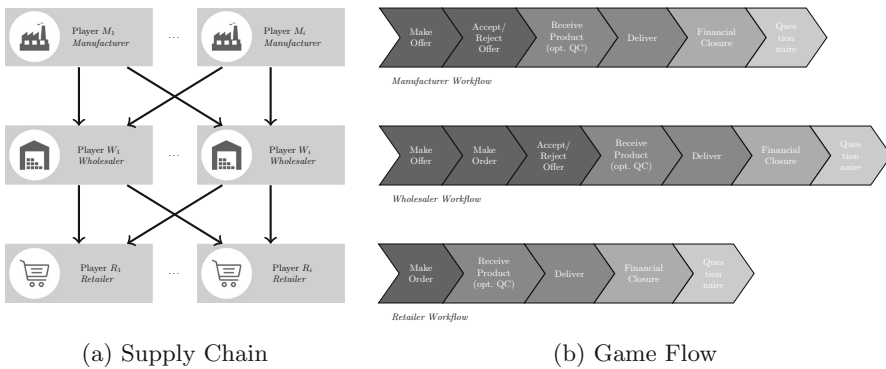


Fig. 1. Game of Trust - game structure and dynamics

After successful completion of the *Negotiation* the *Delivery* phase is initialized. Each entity receiving a valid order is required to deliver the promised product quantities within this step. An important feature at this step is the option to freely combine deliveries from the inventories of both product qualities (in the following HQ and LQ). This allows to deliver products of lower price and quality (LQ) as the higher priced HQ products - a strategy to fulfill orders otherwise not dispatchable or to optimize earnings. In case an order is unfulfillable anyways it will be added to a list of backorders - associated with a fine for the inability to deliver on time. Besides delivering on its own, each entity will also

¹ Note that the offering entity will only be able to reject orders when they have been adjusted by the ordering SC member. Otherwise acceptance is mandatory.

receive any products ordered in the prior *Negotiation* phase². To account for the ability of the delivering party to mislabel products, receivers have the option to perform a quality check on their received goods against a small fee. Finally, the inbound items will be added to the SC members warehouse - either according to the trusted or revealed label.

The actual interaction between the SC actors is then finalized by the *Financial Closure*. In this phase all delivery-based earnings will be offset against all costs resulting from inventory cost, backorder and lying penalties. As each players in-game success is evaluated based on the financial outcome, this phase will allow him/her to understand his/her current performance and potential opportunities for improvement.

Each round is then finally concluded by a short *Questionnaire*. To keep the time spent outside of the game flow minimal only a small set of closed-end questions will be asked. These help to assess each users subjective trust assessment of each interaction partner. While this has no further impact on the game, the obtained data helps to assess trust values computed from the transaction data for correctness/appropriateness (an overview of the computed values and used formulas can be found in [1]).

2.2 Implementation

To account for the experimental and educational purpose of the *Game of Trust*, a considerable amount of attention was paid to its design. Based on a fast, scalable and reproducible IT-architecture (see Fig. 2) the *Game of Trust* allows large multi-player experiments. These will not only help to advance trust related research in SC but also to explore yet underused application areas for serious games. The scalability and reproducibility is achieved by containerization via Docker [6–8]. It allows to create a runnable description of the whole required gaming infrastructure within a single, so-called `docker-compose` file [9]. This highly simplifies testing, deployment, scaling and hopefully also encourages other researchers to use and improve the *Game of Trust* given the low entry barrier.

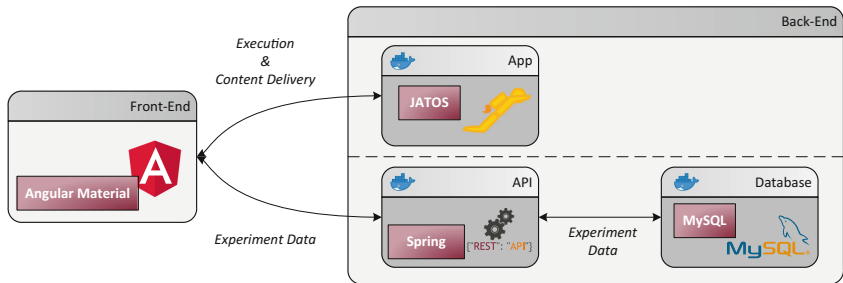


Fig. 2. *Game of Trust* - IT architecture

² Given the sequential nature of the *Game of Trust*, each entity will receive goods before having to deliver on its own.

The actual game was implemented based on the JATOS framework [10]. Developed to make online studies/surveys easier, JATOS already provides a lot of basic functionalities like user and session management as well as data exchange/synchronization. At the same time JATOS is completely based on web technologies like simple HTML and JavaScript (JS) and thus allows the creation of highly customizable 'studies'. The *Game of Trust* was then developed using the JS frameworks AngularJS [11] and AngularJS Material [12]. Using material design enabled the creation of a simplistic, yet visually appealing game with controls users are familiar with from their daily use of mobile devices and web applications.

All transaction data (*negotiations, orders, questionnaire results, ...*) generated during game play is stored within an adjunct MySQL [13] database located behind a REST API. While e.g. JATOS would have had an own data store, only this approach guaranteed the maximum flexibility in data collection as well as distribution for analytical purposes (see next section).

3 Trust Profiling with R-supported Data Analysis

While the *Game of Trust* allows researchers to generate lots of experimental data, the raw data alone provides little insight into the game and the underlying concepts. To get value out of the data careful analysis is required. In order to facilitate the execution of profiling and analysis tasks, the *Trust Profiling in R package* (`tp rp`) was developed. It wraps functions to access the database, create (trust-related) statistics as well as appropriate plotting capabilities. Providing this well-defined and simple analytical API allows researchers to execute and analyze the experiment without in-depth statistical and programming knowledge.

4 Conclusion and Future Work

This paper presents an original serious game to collect data regarding the trust behavior of individuals in SCs. Its easy, fast, scalable and reproducible IT-architecture enables researchers a straightforward set-up and execution of experiments. The provided statistical toolkit allows for an immediate careful analysis of the collected data.

A first large-scale behavioral experiment using the *Game of Trust* is scheduled for October 2017. It is expected that the analysis of the trust dataset uncovers different relevant decision-making profiles, exposing how the participants subjectively perform trust assessments of possible interacting partners. The findings may also help to evaluate the Trust Support Mechanism suggested in [14] and its impact on the SC-related decisions (e.g. procurement, partner selection, information sharing, etc.).

References

1. de Siqueira Braga, D., Niemann, M., Hellingrath, B., de Lima Neto, F.B.: The game of trust: using behavioral experiment as a tool to assess and collect trust-related data. In: Steghöfer, J.-P., Esfandiari, B. (eds.) IFIPTM 2017. IAICT, vol. 505, pp. 41–48. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59171-1_4
2. Meijer, S., Zuniga-Arias, G., Sterrenburg, S.: Experiences with the mango chain game. In: Smeds, R., Riis, J., Haho, P., Jaatinen, M. (eds.) Proceedings of the 9th International workshop of the IFIP, Espoo, Finland, pp. 123–132 (2005)
3. Meijer, S., Hofstede, G.: The trust and tracing game. In: Proceedings of 7th International Workshop of the IFIP, Aalborg, Denmark, May 2003
4. Sterman, J.D.: Instructions for Running the Production-Distribution Game “The Beer Game” (1998)
5. Lang, F., Pueschel, T., Neumann, D.: Serious Gaming for the Evaluation of Market Mechanisms. In: ICIS 2009 Proceedings, AIS, Phoenix, Arizona, USA, p. 97 (2009)
6. Docker Inc.: Docker - Build, Ship, and Run Any App, Anywhere (2017). <https://www.docker.com/>
7. Docker Inc.: What is a Container—Docker (2017). <https://www.docker.com/what-container>
8. Boettiger, C.: An introduction to Docker for reproducible research. *ACM SIGOPS Oper. Syst. Rev.* **49**(1), 71–79 (2015)
9. Docker Inc.: Docker Compose - Docker Documentation (2017). <https://docs.docker.com/compose/>
10. Lange, K., Kühn, S., Filevich, E.: Just another tool for online studies (JATOS): an easy solution for setup and management of web servers supporting online studies. *PLoS ONE* **10**(6), 1–14 (2015)
11. Google: AngularJS - Superheroic JavaScript MVW Framework (2017). <https://angularjs.org/>
12. Google: AngularJS Material - Introduction (2017). <https://material.angularjs.org/latest/>
13. Oracle Corporation: MySQL (2017). <https://www.mysql.com/>
14. De Siqueira Braga, D., Hellingrath, B., Buarque De L. Neto, F.: Trust-aware decision support mechanism for supply chains. In: Proceedings of the 28th EURO Conference - European conference for Operational Research and Management Science, Behavioural Operations Management. Poznan, Poland (2016)