Aug 10th, 12:00 AM

Trust Building and Risk Mitigation via Smart Contracts on Amazon Mechanical Turk

Moritz Tobias Bruckner
University of Augsburg, moritz.bruckner@wiwi.uni-augsburg.de

Adeline Frenzel
University of Augsburg, adeline.frenzel@wiwi.uni-augsburg.de

Daniel Veit
University of Augsburg, daniel.veit@wiwi.uni-augsburg.de

Trust Building and Risk Mitigation via Smart Contracts on Amazon Mechanical Turk

Emergent Research Forum (ERF)

Moritz Bruckner
University of Augsburg
moritz.bruckner@wiwi.uni-augsburg.de

Adeline Frenzel
University of Augsburg
adeline.frenzel@wiwi.uni-augsburg.de

Daniel Veit
University of Augsburg
daniel.veit@wiwi.uni-augsburg.de

Abstract

Amazon Mechanical Turk (MTurk) allows organizations and individuals to benefit from a collective source of intelligence, skills and insights from a global population, but MTurk withdraws from responsibilities and the obligation of overlooking payment transactions. Consequently, there is no contractual agreement between the crowd worker and the requester on when payments should be authorized. Requesters even obtain ownership of the work without having to pay for it. This situation of lock-up poses a serious issue for crowd workers. As a solution to this problem, the present study introduces smart contracts to transactions on crowd work platforms, arguing that smart contracts can mitigate risks from lock-up situations and support trust, through non-alterable terms and conditions imprinted into the code of a smart contract. This research conceptualizes an online experimental study to validate the trust building and risk mitigating effects of smart contracts in crowd work transactions on Amazon Mechanical Turk.

Keywords

Smart Contract, Crowd Work, Lock-Up, Trust, Risk, Amazon Mechanical Turk, Experiment

Introduction

Amazon Mechanical Turk (MTurk) is a marketplace for businesses and individuals to crowdsource processes and jobs online. Tasks include conducting simple data validation and research to survey participation and further. MTurk therefore allows its users to benefit from a collective source of intelligence, skills and insights from a global population (Amazon Mechanical Turk, Inc. 2020). On MTurk, complex problems are broken down into more manageable micro-tasks, called Human-Intelligence Tasks (HITs). HITs are published by requesters and crowd workers complete these tasks over the Internet. As requesters need to check the quality of the work before authorizing remuneration, crowd workers need to trust in receiving payment from the requester after a HIT is processed. In a traditional client-contractor-relationship, the client would give the job to one contractor after analyzing its trustworthiness. This trust management is not possible on crowd work platforms as requesters may give micro-tasks to thousands of crowd workers, which could behave dishonestly, i.e. by delivering low quality or wrong results (Yu et al. 2012). MTurk hereby withdraws from the obligation of overlooking the payment transaction and responsibilities, giving requesters the possibility to reject decent work (Amazon Mechanical Turk, Inc. 2020; Deng et al. 2016; Gol et al. 2019a). Moreover, requesters obtain the ownership of completed work, even if they did not pay for it, which may lead to unethical behavior of requesters. Crowd workers on the other hand, do not have any possibility to claim the payment (LaPlante and Silberman 2016). As a consequence, research shows that crowd workers allocate an average of 23.2% of their capacity on tasks without payment (Berg 2016). Consequently, crowd workers face inequality, are marginalized (Deng et al. 2016) and still have to trust the requesters that the agreed conditions of payment are being met. As there is no contractual agreement between the crowd worker and the requester on when payments should be approved by the requester, this situation is of undetermined length and may last from only hours up to 30 days (maximum time of the auto-approval setting on MTurk (Amazon Mechanical Turk, Inc. 2020)).

This phenomenon is commonly referred to as a lock-up situation. From a theoretical perspective, lock-up situations increase risk due to information asymmetry between the two parties on MTurk. The undetermined length of the lock-up period is hereby expected to be an amplifier to the risks, which result in blind trust being needed by the crowd worker on MTurk. Currently, the only indirect mitigation possibility for crowd workers are several forums (i.e. Turkopticon, Turker Nation, MTurk Forum, etc.) where workers can share information and experience regarding HITs and requesters (Gol et al. 2019b; Irani and Silberman 2013; LaPlante and Silberman 2016). One actual possibility as a countermeasure against lock-up risks would be smart contracts.

Smart contracts were first formulated to conduct the full contractual procedure (agreement, monitoring and adjucation) without human or any third party intervention (Szabo 1997). After 2008 with the inception of Bitcoin and after 2013 with the success of Ethereum (Buterin 2014; Nakamoto 2008), smart contracts are commonly based on blockchain technology and are meant to link encoded contractual agreements, digital monitoring and real-world execution (Iansiti and Lakhani 2017; Werbach and Cornell 2017). In the context of transactions on MTurk, smart contracts are hypothesized to increase transparency by creating equal conditions in transactions between requester and crowd worker. Hence, we argue that smart contracts mitigate risks from lock-up periods and support trust through non-alterable terms and conditions, imprinted into the code of a smart contract. As a result, our research examines the following question:

Do smart contracts in lock-up situations of undetermined length shape trust and risk perceptions on Amazon Mechanical Turk?

In order to answer this question, we conceptualize an online experimental investigation into the interaction effects of smart contracts and lock-up situations employed for requester-crowd worker payment agreements on MTurk. By examining the influence of smart contracts on transaction risks and trust on MTurk, this study makes relevant contributions to crowd work literature in general and to literature on smart contracts and lock-ups in specific. Overall, we intend to lead the way for public contracting, and therefore to a smart-contract-augmented contract law regime (Halaburda et al. 2019).

Amazon Mechanical Turk, Risk, Trust and Lock-Up Situations

MTurk resembles an online platform, upon which third-party requesters broadcast HITs and external crowd workers complete these. From a requesters' perspective, MTurk provides value by giving access to a global, on-demand 24x7 workforce completing thousands of HITs in a short period of time (Amazon Mechanical Turk, Inc. 2020; Brawley and Pury 2016). From a crowd workers' perspective, MTurk offers a platform that enables its users to work from home and choose one's own work hours and to get paid (Deng and Joshi 2016). The governance structure of MTurk is manifested by the terms and conditions of use within the participation agreement. Within these terms and conditions, MTurk declines all responsibility related to the transactions between requesters and workers in terms of quality, safety or payment issues (Bergvall-Kåreborn and Howcroft 2014). MTurk additionally states that users' engagement on the platform is at their own risk, and all work "is made for hire", for the benefit of the requester (Bergvall-Kåreborn and Howcroft 2014). This means, that there is no legal protection and any ownership or intellectual property rights reside with the requester (Amazon Mechanical Turk, Inc. 2020; Felstiner 2011; Newman 2019). The situation is further aggravated by the fact that once the crowd worker has been accepted for a HIT, it must be completed in a given timeframe. However, there is no timely limit for requesters evaluating and reimbursing the work. The "mandatory satisfaction" clause even gives the requester the authority to reject a HIT without justification (Brawley and Pury 2016; Deng et al. 2016). At the same time, the requester is able to access the work without forfeiting ownership (Amazon Mechanical Turk, Inc. 2020; Bergvall-Kåreborn and Howcroft 2014). This lack of transparency raises exceptional ethical concerns and risks for crowd workers in ways that the crowd workers are unable to make judgements about the moral valence of their work (Zittrain 2008). In addition, the time-period for reimbursement of the conducted work is unknown, a situation for the crowd worker that is commonly referred to as a lock-up situation.

Little is known about lock-up situations in the relationship between requester and crowd worker on MTurk. Lock-ups have predominantly been studied in the context of contractually agreed lock-up periods of Initial Public Offerings, where the investor is restricted from selling her/his shares for a fixed period of time (Field and Hanka 2001; Garfinkle et al. 2002; Keasler 2001). The difference to lock-ups in the environment on MTurk is that the length of a lock-up is voluntarily set by requesters in the auto-approval settings, and may be extended up to 30 days. However, within this time-period, the requester may manually approve or reject

payments and hence decides whether the crowd worker will receive remuneration or not. This includes substantial risks as the crowd worker must trust in the benevolence of the requester.

In conclusion, ethical considerations on crowd working platforms, are about the borderless nature which results in the fact, that crowd employment platforms are largely hidden from legislation or regulation (Felstiner 2011). As a result, lock-up periods cause increased risk and trust discrepancies in requester-crowd worker transactions.

Smart Contracts

Smart contracts were first formulated by Szabo in 1997. At the time, the author envisioned the full cycle of a contract, including the search, performance and adjucation to be handled by hardware and software without human interaction. Smart contracts are defined as "(…) automatically executable agreements between parties based on predefined codified criteria" - (Halaburda et al. 2019, p.2).

In 2008, blockchain technology became popular through the BitCoin white paper, written by Nakamoto (2008). Leveraging the benefits of blockchain technology, users were encouraged to develop contracting platforms for automatic execution of digitally encoded contractual terms outside the BitCoin system (Werbach and Cornell 2017). Inspired by the shortcomings of BitCoin, Vitalik Buterin developed the Ethereum blockchain platform in 2013 (Buterin 2014). Ethereum was the first platform to allow the development of diverse blockchain applications like for example smart contracts (Iansiti and Lakhani 2017). From the moment of inception of the Ethereum platform, increased use of digital data inputs to monitor contracts took place (Iansiti and Lakhani 2017). In addition, monitoring can be directly tied to contractual terms and execution without dispute. In smart contracts, once the agreements are made, contractual terms are inalterable and transactions will be executed automatically if all prerequisites are met (Halaburda et al. 2019). Therefore, the adoption of well-designed smart contracts yields improvements in terms of reduced contract monitoring costs such as costs of renegotiation of contractual terms (Halaburda et al. 2019).

In the context of crowd work platforms, which do not offer a contractual agreement between requester and crowd worker (i.e. MTurk), smart contracts represent a platform-independent solution for both parties to define the expected work quality as well as a resulting payment security. Therefore, smart contracts close the trust discrepancy between both parties and ensure that the requester will get exactly the work outcome s/he expects and the crowd worker will get the payment if s/he delivers the work as required. These automatically executable agreements build trust/reduce risk for both sides of the exchange by making them equal partners and reduce the effort for requesters to manually check the works' quality.

Hypotheses Development and Research Model

Lock-up periods force crowd workers to advance their labor with non-regulated and insecure remuneration practices, enforced by the terms and conditions of the MTurk platform (Amazon Mechanical Turk, Inc. 2020; Bergvall-Kåreborn and Howcroft 2014).

Trust is defined by the function of the degree of risk inherent in a situation (Koller 1988). Because crowd workers are forced to fulfill their duty within a certain time frame and requesters are not, trust is being compromised by the discrepancy of regulatory and timely strictness between requesters and crowd workers. Trust is further aggravated by the fact that requesters are allowed to reject work on MTurk and still remain ownership of intellectual property rights (Amazon Mechanical Turk, Inc. 2020; Bergvall-Kåreborn and Howcroft 2014; Brawley and Pury 2016; Deng et al. 2016).

Summarized, under such conditions, the crowd workers' trust in the transaction is expected to decrease and perceived risk is expected to increase. Therefore, hypothesis 1 states the following:

H1: *Lock-up situations will decrease perceived trust and increase perceived risk compared to the situation without a lock-up.*

Smart contracts represent encoded terms and conditions that two parties agree on. Once implied, these terms and conditions are non-alterable and execution will take place automatically (Halaburda et al. 2019). Implying these inalterable self-executing contracts to transactions on MTurk that are characterized by lock-up periods, risk perceptions of crowd workers are expected to decrease and trust is hypothesized to increase. For this reason, hypotheses 2 a and 2 b state the following:

H2-a: *Smart contracts will shape trust perceptions from lock-up situations, leading to increased perceptions of trust, when a lock-up is present.*

H2-b: *Smart contracts will moderate risks from lock-up situations, leading to decreased perceptions of risk, when a lock-up is present.*

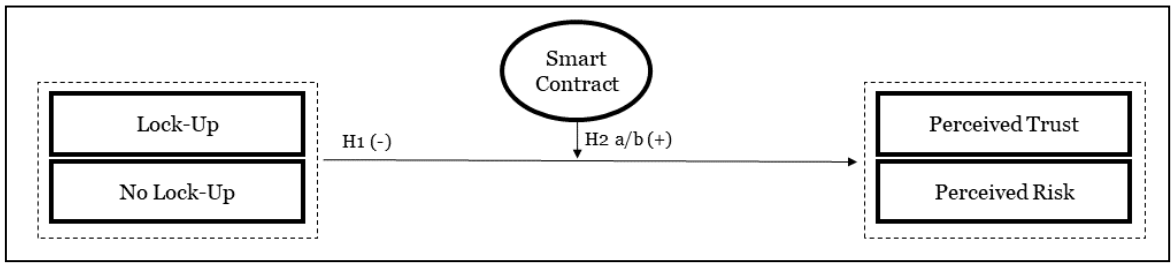

Figure 1. Conceptual research model

Methodology

Procedure: The four groups of the online experiment include two varying versions of lock-ups. Scenario one will present the crowd workers with a lock-up situation, in which the crowd worker has to finish a task within a set time period but the requester will not have a deadline for reviewing and remunerating the work. The no lock-up situation on the other hand, is created by a short deadline for both (e.g. 24-48 hours), the crowd worker and the requester. The crowd workers have to finish their task and the requesters need to review and remunerate the work in time. Scenario three and four will also include a lock-up and no lock-up situation but will additionally present a smart contract for the crowd worker and the requester, including its terms and conditions. The dependent variables of trust (McKnight et al. 2002) and risk (Keil et al. 2000) perceptions will be measured via established multi-item constructs. The complexity of the task will be controlled.

Data Collection: Data will be collected with crowd workers from the MTurk platform. We will ensure validity of the experimental design by conducting manipulation checks. Attention checks throughout the experimental procedure will assure that participants respond to the questions thoughtfully.

Expected Findings, Discussion and Future Research

Based on the results of the online experiment, we expect to find that lock-ups yield a negative effect on the dependent variables due to trust asymmetries and risk perceptions of crowd workers.

Smart contracts on the other hand, are expected to mitigate risk perceptions through creation of equally applicable terms and conditions for the requester and the crowd worker. The smart contract is hereby expected to take on the role of a reliable, third party regulating instance. With this technical attribute, crowd workers are receiving their funds if the work has been conducted to the agreed level of quality. This will be the case independent of any fraudulent intentions of requesters. To receive work without paying will not be possible anymore, which in turn increases trust and reduces risk for both parties through increased transparency and comprehensible execution of terms and conditions via a smart contract.

Our work illustrates the relevance of exploring technical lock-up situations and their interactions with smart contracts. Specifically, we demonstrate how smart contracts as a regulatory technology, shape risk perceptions and trust from lock-up situations on MTurk, where crowd workers find themselves dependent on the goodwill of a requester and do not seldomly miss out major parts of their income. This highlights the need for research on solutions to this problem. Smart contracts serving as self-regulating and executing instance in crowd work transactions could embody a regulatory third party to increase transparency, trust and to reduce risks. Future research is therefore clearly recommended to investigate the trust building and risk mitigating effects of smart contracts in combination with lock-up situations.

REFERENCES

Amazon Mechanical Turk, Inc. 2020. Retrieved 12. February, 2020, from https://www.mturk.com/.

Berg, J. 2016. "Income Security in the On-Demand Economy: Findings and Policy Lessons from a Survey of Crowdworkers," *Comparative Labor Law & Policy Journal* (37), pp. 543–576.

Bergvall-Kåreborn, B., and Howcroft, D. 2014. "Amazon Mechanical Turk and the commodification of labour: Amazon Mechanical Turk," *New Technology, Work and Employment* (29:3), pp. 213–223.

Brawley, A. M., and Pury, C. L. S. 2016. "Work experiences on MTurk: Job satisfaction, turnover, and information sharing," *Computers in Human Behavior* (54), pp. 531–546.

Buterin, V. 2014. *A Next Generation Smart Contract & Decentralized Application Platform*. in *White Paper* Retrieved 23. January, 2020, from https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf/.

Deng, X., and Joshi, K. D. 2016. "Why Individuals Participate in Micro-task Crowdsourcing Work Environment: Revealing Crowdworkers' Perceptions," *Journal of the Association for Information Systems* (17:10), pp. 648–673.

Deng, X., Joshi, K. D., and Galliers, R. D. 2016. "The Duality of Empowerment and Marginalization in Microtask Crowdsourcing: Giving Voice to the Less Powerful Through Value Sensitive Design," *MIS Quarterly* (40:2), pp. 279–302.

Felstiner, A. 2011. *Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry*, Berkeley Journal of Employment and Labor Law.

Field, L. C., and Hanka, G. 2001. "The Expiration of IPO Share Lockups," *The Journal of Finance* (56:2), pp. 471–500.

Garfinkle, N., Malkiel, B. G., and Bontas, C. 2002. "Effect of Underpricing and Lock-Up Provisions in IPOs," *The Journal of Portfolio Management* (28:3), pp. 50–58.

Gol, E. S., Avital, M., and Stein, M.-K. 2019a. "Crowdwork Platforms: Juxtaposing Centralized and Decentralized Governance," in *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm, Sweden, pp. 1–16.

Gol, E. S., Stein, M.-K., and Avital, M. 2019b. "Crowdwork platform governance toward organizational value creation," *Journal of Strategic Information Systems* (28:2), pp. 175–195.

Halaburda, H., Levina, N., and Min, S. 2019. "Understanding Smart Contracts as a New Option in Transaction Cost Economics," in *Proceedings of the 40th International Conference on Information Systems (ICIS)*, Munich, Germany, pp. 1–17.

Iansiti, M., and Lakhani, K. R. 2017. "The truth about blockchain.," *Harvard Business Review* (95:1), pp. 118–127.

Irani, L. C., and Silberman, M. S. 2013. "Turkopticon: interrupting worker invisibility in amazon mechanical turk," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, Paris, France: ACM Press, p. 611.

Keasler, T. R. 2001. "The Underwriter's Early Lock-up Release: Empirical Evidence," *Journal of Economics and Finance* (25:2), pp. 214–228.

Keil, M., Tan, B. C., Wei, K.-K., Saarinen, T., Tuunainen, V., and Wassenaar, A. 2000. "A cross-cultural study on escalation of commitment behavior in software projects," *MIS Quarterly* (24:2), pp. 299–325.

Koller, M. 1988. "Risk as a Determinant of Trust," *Basic and Applied Social Psychology* (9:4), pp. 265–276.

LaPlante, R., and Silberman, M. S. 2016. "Building Trust in Crowd Worker Forums: Worker Ownership, Governance, and Work Outcomes," in *Weaving Relations of Trust in Crowd Work: Transparency and Reputation Across Platforms, workshop colocated withWebSci '16*, Hannover, Germany.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334–359.

Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. in *White Paper* Retrieved 15. October, 2018, from https://bitcoin.org/bitcoin.pdf.

Newman, A. 2019. *I Found Work on an Amazon Website. I Made 97 Cents an Hour.* in *The New York Times*from https://www.nytimes.com/interactive/2019/11/15/nyregion/amazon-mechanical-turk.html.

Szabo, N. 1997. "Formalizing and Securing Relationships on Public Networks," *First Monday* (2:9).

Werbach, K., and Cornell, N. 2017. "Contracts Ex-Machina," *Duke Law Journal* (67:2), pp. 313–382.

Yu, H., Shen, Z., Miao, C., and An, B. 2012. "Challenges and Opportunities for Trust Management in Crowdsourcing," in *2012 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, pp. 486–493.

Zittrain, J. 2008. "Ubiquitous human computing," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* (366:1881), pp. 3813–3821.