An Incentive-Compatible Smart Contract for Decentralized Commerce

Nikolaj I. Schwartzbach
Dept. of Computer Science
Aarhus University
Aarhus, Denmark

2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) | 978-1-6654-3578-9/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICBC51069.2021.9461077

***Abstract*—We propose a smart contract that allows two mutually distrusting parties to transact any non-digital goods or services on a blockchain. The contract acts as an escrow and settles disputes by letting parties wager that they can convince an arbiter they were the honest party. We prove that the contract is secure in a strong game-theoretic sense if and only if the arbiter is biased in favor of honest parties. The contract can be instantiated on any blockchain that supports smart contracts. In particular, it can be instantiated in a manner that complies with laws and regulations by using a blockchain with revocable anonymity.**

***Index Terms*—game theory, smart contract, e-commerce**

I. Introduction

A fundamental problem of electronic commerce is ensuring both ends of the trade are upheld: an honest seller should always receive payment, and an honest buyer should only pay if the seller was honest. Traditionally, this is ensured by introducing a trusted intermediary who holds the payment in escrow until the trade has completed, after which it releases the funds to the seller. In this work we propose replacing the intermediary with a smart contract that runs on a blockchain. The contract makes black-box use of an arbiter which is a protocol invoked in case of disputes. We assume parties are rational, meaning they act to maximize their utility with no concern for the intended behavior of the protocol designer. This is arguably a more realistic model in the context of electronic commerce, as parties can be presumed to have an economic incentive to engage in the transaction. We prove that the contract ensures honest behavior in rational agents only if the arbiter is better than random. By assuming parties are risk averse we can replace the arbiter with a random coin toss. Finally, we feature a discussion of how to instantiate the contract on a blockchain to comply with laws and regulations.

A. Related work

Our work is related to the classic problem of fair exchange. It is well-known there is no two-party protocol that achieves fairness in general [1] so the use of a trusted third party is necessary for fair exchange. Fair exchange with optimistic use of a trusted third party was studied in e.g. [2]–[4]. More recently, the trusted third party has been implemented as a smart contract on a blockchain, see [5], [6]. Common to all these protocols is that they only work for digital goods as they make use of cryptographic primitives on the goods. Escrow with physical goods was studied in [7], though its focus is on implementing the escrow cryptographically and does not feature a game-theoretic analysis. Outside academic circles, there are proposed solutions to electronic commerce of physical goods, of which the most promising are Kleros [8] and OpenBazaar [9], though they lack a formal game-theoretic analysis. In fact, we show both systems are insecure as game-theoretic security implies parties must be penalized for issuing a false dispute, proportional to the value of the item transacted.

This work was supported by the European Research Council (ERC) under the European Unions's Horizon 2020 research and innovation programme under grant agreement No 669255 (MPCPRO).

II. The contract

We consider a buyer B who wants to purchase an item it from a seller S. The item is sold for a price of x, and has a value to the buyer of $y > x$, and a value to the seller of $x' < x$. From a game-theoretic point of view, we have to assume $y > x > x'$; otherwise neither buyer nor seller has incentive to engage in the transaction. The item it is *non-digital* which means it has to be shipped through a physical channel "off-chain". By definition, no algorithm can determine whether or not it was physically delivered to the buyer. We assume both parties have access to a blockchain, which for our purposes is a shared data structure that allows both parties to deploy a smart contract π that can maintain state, respond to queries, and transfer funds. Unlike a human third party, the smart contract can be guaranteed to behave honestly due to the security of the underlying blockchain. For simplicity, we assume the blockchain is secure and incorruptible, and consider only attacks on the contract itself. We also assume transaction fees are negligible compared to the items being transacted, such that they can be disregarded entirely.

The contract makes use of an *arbiter* which is a protocol invoked in case of disputes: its purpose is to distinguish the honest party from the dishonest party. We denote by γ the error rate of the arbiter. In the case of digital goods, cryptography allows us to get $\gamma = 2^{-\kappa}$ for any κ which has been exploited in previous work [2]–[6]. We assume each party holds an estimate of $\gamma > 0$ that they provide as input to the contract. This value might be established empirically, though it likely depends on the nature of the goods transacted. As in [2]–[4], [8], to save resources we make *optimistic* use of the arbiter, meaning it is only invoked when necessary. The contract is parameterized

by a *wager constant* $\lambda > 0$ and a *repayment constant* $0 \leq \alpha \leq 2$. The contract proceeds as follows: both parties sign a contract committing to making the trade, and B places x money in escrow. S delivers it to B who then notifies the smart contract to transfer the funds in escrow to S, thus terminating the contract. To handle disputes, B can place a "wager" of size λ that they can convince the arbiter of their honesty. The seller can then counter this complaint by also placing a wager of size λ, after which the arbiter is invoked to choose a winner. The winner is repaid $x + \alpha\lambda$, while the loser receives nothing. We use the leftover $(2-\alpha)\lambda$ to compensate the arbiter for their time. We handle crashing by having timeouts in the contract in a way that favors the party that did not crash.

III. Game-theoretic Security

In the following, we assume parties are *rational*, i.e. they maximize their own utility with no concern for the intended behavior of the protocol designer. We say the protocol is secure if maximal utility is achieved when a party behaves honestly. We assume familiarity with game theory and refer to [10] for details. Formally, we consider a two-party protocol π where each party P_i has a set $\mathcal{S}_i$ of possible (pure) strategies, of which there is a unique *honest strategy* $s_i^* \in \mathcal{S}_i$. We let $s^* = (s_1^*, s_2^*) \in \mathcal{S}_1 \times \mathcal{S}_2$ be the unique honest strategy profile. For our purposes, subgame perfection is likely not sufficient in itself: if the incentive to choose s^* is too small, there may be other reasons to deviate not captured by the utilities of the game, say for sport or for revenge. If the incentive is sufficiently large (say $\geq \varepsilon$) then we say the protocol is secure in a game-theoretic sense against ε-deviating rational adversaries. Our definition generalizes the notion from [11] of evolutionary stable equilibria by quantifying how much utility is lost by deviating from the equilibrium strategy profile.

Definition. *Let π be a two-party protocol with strategy space $\mathcal{S}$, where $s^* \in \mathcal{S}$ is the honest strategy profile. We say π has* ε-strong game-theoretic security *if the following is satisfied:*

- (Completeness) - *s^* is the unique SPE.*
- (Soundness) - *For every $s \neq s^*$, and every i with $s_i \neq s_i^*$, it holds that $u_i(s_i^*, s_{-i}) \geq u_i(s_i, s_{-i}) + \varepsilon$.* ◇

We now consider the contract as an extensive-form game and draw the corresponding game tree (seen in Fig. 1). The payoff for each party is defined as their expected change in funds. We only consider the case of *maximal security*, meaning we intentionally leave out some cases where ε is small.

Theorem. *The contract is only complete when $\gamma < \frac{1}{2}$, and it has (maximal) ε-strong game-theoretic security if and only if one of the following conditions are established:*

1) $\alpha = 2$*; and* $\lambda \geq \frac{x\gamma+\varepsilon}{1-2\gamma}$.
2) $\frac{1}{1-\gamma} < \alpha < 2$*; and* $\varepsilon \geq x\left(\frac{1-2\gamma}{2-\alpha}\right)$*; and* $\lambda \geq \frac{x\gamma+\varepsilon}{1-\alpha\gamma}$.
3) $\alpha = \frac{1}{1-\gamma}$*; and* $\varepsilon = x(1-\gamma)$*; and* $\lambda = x\left(\frac{1-\gamma}{1-2\gamma}\right)$.
4) $\alpha < \frac{1}{1-\gamma}$*; and* $\varepsilon = x\left(\frac{1-2\gamma}{2-\alpha}\right)$*; and* $\lambda = x\left(\frac{1}{2-\alpha}\right)$.

Proof. We proceed using backwards induction in the game tree, and require that honest actions yield ε more payoff than the dishonest ones. This can be seen to be true if and only if the following two inequalities are satisfied:

$$(x + \alpha\lambda)(1-\gamma) - \lambda \geq \varepsilon \tag{1}$$

$$0 \geq \varepsilon + (x + \alpha\lambda)\gamma - \lambda \tag{2}$$

For completeness, we have $\varepsilon = 0$ and strict inequalities which can only be true if $\frac{\gamma}{1-\gamma} < \frac{1-\gamma}{\gamma}$. This can easily be seen to only be true for $\gamma < \frac{1}{2}$. For the rest of the proof, we only show the case of $\alpha = \frac{1}{1-\gamma}$, as the other cases are similar. In this case, Eq. (1) gives an upper bound on the security parameter $\varepsilon \leq x(1-\gamma)$. Similarly, Eq. (2) gives a lower bound of $\lambda \geq \frac{(1-\gamma)(x\gamma+\varepsilon)}{1-2\gamma}$. Choosing the maximum $\varepsilon = x(1-\gamma)$ and substituting gives the desired result. □

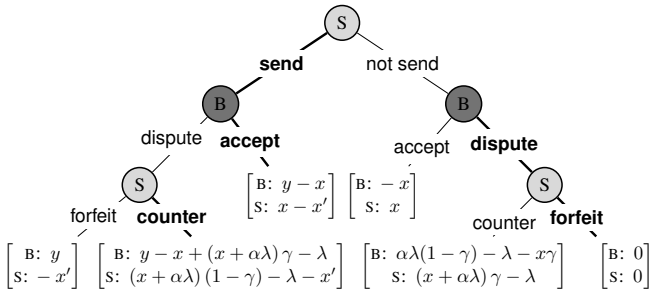

Fig. 1. Game tree of the smart contract after both parties have accepted the transaction. The first coordinate is the buyer payoff and the second is seller payoff. Light nodes are seller actions; dark nodes are buyer actions. The heavy edges denote honest actions.

Corollary. *When the winning party exactly receives back their wager, i.e. $\alpha = 1$, the contract has $x(1-2\gamma)$-strong game-theoretic security whenever $\gamma < \frac{1}{2}$ and $\lambda = x$.* □

IV. Discussion

Strong game-theoretic security necessitates the use of an arbiter which is strictly better than chance. This assumption must hold independently of B and S, meaning the arbiter must not collude with either party. It is difficult if not impossible to prove the existence of such an arbiter in the context of physical goods. One option is to use a decentralized court system like Kleros [12], though in absence of an empirical study it remains conjecture whether this is in fact better than chance. We can also replace the arbiter with a random coin toss [13]. This results in a contract with weak game-theoretic security, in the sense that the honest strategy is a non-unique SPE, though it remains secure in a strong sense against risk averse players.

The contract can be run on any blockchain that supports smart contracts (such as Ethereum). As a result, many properties of the contract are inherited from the corresponding blockchain. The contract can be used in a manner that complies with current laws and regulations by using a blockchain with revocable anonymity [14], [15]: a party who takes part in distributing illicit goods can be deanonymized by the courts, while all other parties remain anonymous. This would allow for a certification or blueprint of marketplaces based on smart contracts even if they are essentially anonymous, so long as the underlying blockchain uses revocable anonymity.

REFERENCES

[1] R. Cleve, "Limits on the security of coin flips when half the processors are faulty," in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, ser. STOC '86. New York, NY, USA: Association for Computing Machinery, 1986, p. 364–369. [Online]. Available: https://doi.org/10.1145/12130.12168

[2] N. Asokan, V. Shoup, and M. Waidner, "Asynchronous protocols for optimistic fair exchange," in *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No.98CB36186)*, 1998, pp. 86–99.

[3] A. Küpçü and A. Lysyanskaya, "Usable optimistic fair exchange," in *Topics in Cryptology - CT-RSA 2010*, J. Pieprzyk, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 252–267.

[4] ——, "Optimistic fair exchange with multiple arbiters," in *Computer Security – ESORICS 2010*, D. Gritzalis, B. Preneel, and M. Theoharidou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 488–507.

[5] S. Dziembowski, L. Eckey, and S. Faust, "Fairswap: How to fairly exchange digital goods," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 967–984.

[6] A. Asgaonkar and B. Krishnamachari, "Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator," *CoRR*, vol. abs/1806.08379, 2018.

[7] S. Goldfeder, J. Bonneau, R. Gennaro, and A. Narayanan, "Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin," in *Financial Cryptography and Data Security*, A. Kiayias, Ed. Cham: Springer International Publishing, 2017, pp. 321–339.

[8] "Kleros escrow explainer - secure your blockchain transactions today," accessed on 10/10/2020. [Online]. Available: https://blog.kleros.io/kleros-escrow-secure-your-blockchain-transactions-today/

[9] "How moderators and dispute resolution work in openbazaar," accessed on 16/10/2020. [Online]. Available: https://openbazaar.org/blog/how-moderators-and-dispute-resolution-work-in-openbazaar/

[10] M. J. Osborne and A. Rubinstein, *A course in game theory*. Cambridge, USA: The MIT Press, 1994, electronic edition.

[11] B. Thomas, "On evolutionarily stable sets," *Journal of Mathematical Biology*, vol. 22, no. 1, pp. 105–115, Jun 1985.

[12] C. Lesaege, F. Ast, and W. George, "Kleros Short Paper v1.0.7," Tech. Rep., 09 2019.

[13] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *SIGACT News*, vol. 15, no. 1, p. 23–27, Jan. 1983.

[14] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology — EUROCRYPT 2001*, B. Pfitzmann, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 93–118.

[15] I. Damgård, H. Gersbash, U. Maurer, J. B. Nielsen, C. Orlandi, and T. P. Pedersen, "Concordium White Paper, vol. 1.0," Tech. Rep., 04 2020.