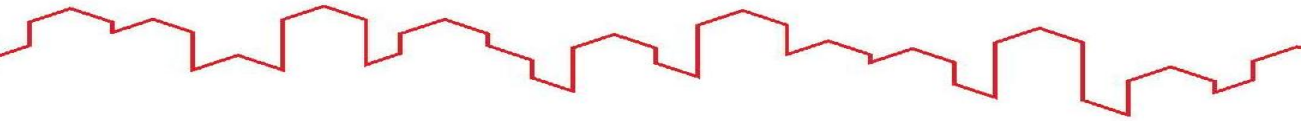


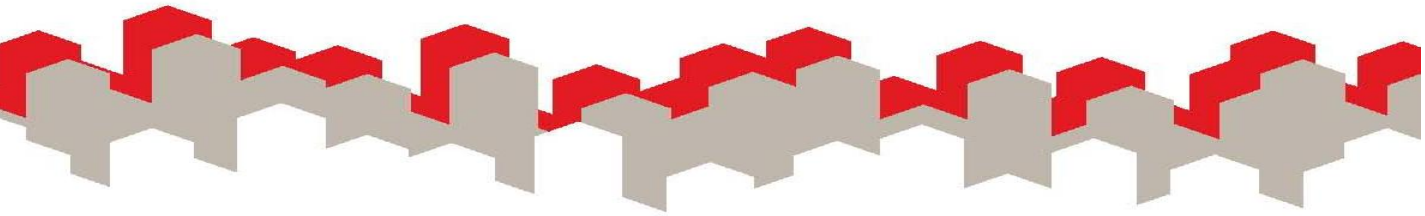
Department of Economics

Optimal Smart Contracts with Costly Verification

Akaki Mamageishvili[1]
ETH Zurich

Jan Christoph Schlegel
City, University of London

Department of Economics
Discussion Paper Series
No. 19/13



[1] Corresponding author: Akaki Mamageishvili, Department of Management, Technology and Economics, ETH Zurich, Main building, Rämistrasse 101, 8092 Zurich, Switzerland. Email: amamageishvili@ethz.ch

Optimal Smart Contracts with Costly Verification*

Akaki Mamageishvili[1] and Jan Christoph Schlegel[2]

[1]Department of Management, Technology and Economics, ETH Zurich
[2]Department of Economics, City, University of London

July 2019

Abstract

We study optimal smart contract design for monitoring an exchange of an item performed offline. There are two parties, a seller and a buyer. Exchange happens off-chain, but the status update takes place on-chain. The exchange can be verified but with a cost. To guarantee self-enforcement of the smart contract, both parties make a deposit and the deposits must cover payments made in all possible final states. Both parties have an (opportunity) cost of making deposits. We discuss two classes of contract: In the first, the contract only interacts with the seller, while in the second, the contract can also interact with the buyer. In both cases, we derive optimal contracts specifying optimal deposits and verification policies.

Keywords— Smart Contracts, Deposit Design, Costly State Verification

1 Introduction

Smart contracts offer a new way of implementing economic mechanisms.[1] A smart contract uses trust in distributed consensus as a substitute for a trustworthy mediator that is usually assumed in classical mechanism design. In a classical mechanism, a trustworthy mediator enforces the rules of the mechanism and calculates, based on the information provided by the participants, an allocation of resources. The mediator can be an auctioneer, an intermediary in a platform market, a court that enforces rules. In contrast to this, a mechanism encoded in a smart contract is hard-wired to perform the rules of the mechanism. The rules of the mechanism are self-enforcing. In particular, commitment can be encoded in the protocol. In the

*We thank Robert M. Townsend and Dan Cao for their valuable feedback.

[1]Smart contracts are programs written in a Turing complete language and executed in a blockchain environment. Buterin (2016) describes the first implementation of smart contracts in the Ethereum environment. Recent development allows smart contracts to be fed a trustworthy data from public databases, to make them more efficient for the usage, see Zhang et al. (2016).

case of an item exchange, a popular application of smart contracts, commitment is achieved by paying deposits in the contract.[2]

Smart contracts give rise to interesting design questions that have not usually been considered in the mechanism design literature. In classical mechanism design, information is elicited and allocation and transfers are implemented and enforced by the mechanism designer. Any necessary transfers are made immediately at zero transaction cost and are intermediated by the mechanism designer. In a smart contract, deposits are made before the contract is executed and all transfers made between the parties have to be taken from the initial deposits. This reflects the concern that agents can walk away from the contract at any time and commitment to participate after having agreed to do so cannot be enforced. On the downside, depositing involves an implicit cost for the participants in the smart contract: This can be the opportunity cost of not using the deposit while the contract is executed, borrowing costs of the agent, risk of loss of the deposit if the consensus protocol fails. In particular, mechanisms that use punishment through huge negative transfers in case of "miss-behavior" of agents would be impractical. Even though the punishments are only executed off the equilibrium path, huge deposits have to be made in order to make the threat of punishment credible. This would make such mechanisms very costly to implement as a smart contract.

In this paper, we study the design of optimal smart contracts as a mechanism design problem. We study this question in a context motivated by a practical problem. A file exchange smart contract platform with deposits, such as FileBounty[3], or BitBay[4], mediates the exchange of a file between a seller and a buyer of a file, requiring deposits from both sides of the trade. Sending the file is costly and the contract has to incentivize the seller to send the file to the buyer. The smart contract uses (the threat of) a costly verification procedure to incentive the file exchange. Examples of such verification procedures include revealing some contents of the file on a publicly available web page, together with the magnet link to a file which can only be downloaded by the buyer, or some physical (video, photo) proof which is checked by some randomly chosen nodes of the blockchain network in exchange for financial payoff (an "oracle" in the blockchain parlance) to reach a consensus on its validity, in a similar manner as consensus is achieved in proof of stake blockchains.[5] We consider the size of the deposits as part of the design problem and analyze optimal smart contracts where the opportunity cost of deposits is taken into account when designing a contract.

We provide a rigorous analysis of the problem as a mechanisms design problem, social welfare is optimized subject to incentive and participation constraints, and

[2]We are not claiming that a smart contract is the only way for contracting parties to enforce actions. There might be other mechanisms to enforce the contract in case of misbehavior (account suspension, reputation damage if the identity is known, legal enforcement, etc.). However, smart contracts provide mechanisms for enforcement when these other mechanisms are not readily available or costly.

[3]`https://chainsolutions.com/filebounty-protocol/`

[4]`https://bitbay.market/double-deposit-escrow`

[5]Dziembowski et al. (2018) and Allen et al. (2019) study the practical design of such a protocol on the blockchain. The protocol in Dziembowski et al. (2018) includes deposits and a costly verification procedure and Allen et al. (2019) consider a dispute resolution procedure, an instance of what we call costly verification procedure. We abstract away of the specifics of the verification procedure and instead study the economic question of optimally designing deposits and monitoring policies.

characterize the optimal contracts. We consider two possible scenarios that differ in how much communication is feasible: in the first, the contract only interacts with the sender of the file [6]. In this case, the seller can be monitored and be asked to prove whether he has sent the file. Proving is costly. We derive an optimal monitoring policy and optimal deposits. In the optimal contract, the sender is monitored with a probability that is increasing in the opportunity cost of depositing and decreasing in the cost of monitoring. Payments to the sender can be conditioned on whether he is monitored or not. There are two focal contracts within the class of optimal contracts. In the seller optimal contract, the payments when monitored and when not monitored are the same. In the buyer optimal contract, the seller is only paid if he is monitored and otherwise receives no transfer.

In the second scenario, the contract can also interact with the buyer and the contract uses the signals from both players. If communication with the buyer is allowed, the threat of monitoring is sufficient to induce truthful behavior. First, we show that monitoring is required, at least with some positive probability, in order to be able to distinguish between two states. Otherwise, during the execution of the contract, multiple equilibria can arise some of which do not induce exchange of the file. In the monitoring equilibrium, the buyer reveals whether the file has been sent or not. If the cost of verification is low, the only deposit has to be made by the buyer, which would be taken away by the seller if he is monitored and he proves, or if he is not monitored. If the cost of verification is high, both the seller and the buyer need to deposit an amount such that the sum of deposits covers the cost of verification. Again there can be different optimal contracts that are more or less favorable for the seller or buyer. If the buyer deposits more, then the seller receives a) a higher price and b) can deposit less money, as the opportunity cost of forgoing the price provides incentives for him to prove if monitored. With a low cost of verification, though, there is just one optimal contract and favorable contracts for the seller and the buyer separately can not be designed.

1.1 Related Literature

Townsend (1979) initiated the study of optimal deterministic mechanisms with costly state verification. Gale and Hellwig (1985) apply the approach to the design of optimal debt contracts. Mookherjee and Png (1989) extended the class of available mechanisms by considering random mechanisms and studied optimal auditing contracts with costly verification. The authors show that in the case of finitely many hidden states of the insured person's income, an optimal auditing strategy randomizes between monitoring and not monitoring. One difference between our paper and their earlier work is that we consider the effect of deposits that lead to randomized monitoring, while risk aversion induced randomized monitoring in their case.

Witkowski et al. (2011) develop incentive compatible and individually rational mechanisms using intermediary and buyer acknowledgement. We can see smart contracts as such intermediary. Our mechanism two is somewhat similar to their

[6] There are a number of reasons why the participation of the buyer is not desirable. First, the buyer might be reluctant to send such a signal of item receipt for privacy reasons. Second, it requires the buyer to be online at some point during the execution time of the contract. Therefore, this procedure can not efficiently be automatized by the seller to sell a large number of items.

mechanism in respect of getting information from both parties. Depositing money from both the seller and the buyer in the file exchange setting, and its game-theoretical analysis is a topic of recent paper by Asgaonkar and Krishnamachari (2019).

Hartline and Roughgarden (2008) study optimal mechanism design under money burning and show that in certain settings it improves the objective function. Though the mechanisms developed in our paper do not burn money in equilibrium state(s), money burning occurs in the off-equilibria state(s). Ben-Porath et al. (2014) study the optimal allocation of one item among multiple agents with costly verification and show that randomization is required. Commitment is not needed in smart contracts, since deposits guarantee self-enforcement of such contracts. The role of commitment and evidence in mechanism design is the topic of Ben-Porath et al. (2019).

Smart contracts attracted some attention in the law and economics literature as well. Cong and He (2019) study the role of smart contracts and decentralized consensus in the market organization and asymmetric information environment. Holden and Malani (2017) study ways how smart contracts can be used into solving holdup problem.

On a high level our model is also related to mechanism design for bilateral trade Myerson and Satterthwaite (1983); Blumrosen and Dobzinski (2014). However, our model focuses on incentivizing exchange rather than the question to eliciting private information about valuations for the exchange.

2 Model

There are two agents: a risk-neutral seller, denoted by S, and a risk-neutral buyer, denoted by B. There is one item, denoted by I. There are two relevant dates, which we call "today" and "tomorrow". Today a contract is agreed upon, which specifies details about monitoring decisions, possible messages and transfers in the different states. Tomorrow the seller decides whether or not he sends the file, the contract is executed and transfers are paid out. The seller can verify the act of sending the item on the contract, yet at a cost of verification $c > 0$. The contract can monitor if the submission happened, by asking the seller to provide a proof of this event. It can also randomize this process.

The utility is quasi-linear in transfers. Seller's valuation for sending the item is $v^S(s)$ and his valuation for not sending the item is $v^S(\bar{s})$. Buyer's valuation (today) for receiving the item $v^B(s)$ and his valuation for not receiving the item is $v^B(\bar{s})$. We normalize valuations such that $v^B(s) - v^B(\bar{s}) = v$, and $v^S(\bar{s}) - v^S(s) = 1$. The time between today and tomorrow is discounted with $1 - \delta$ for $0 < \delta < 1$, so that if an agent deposits D today and gets paid out his entire deposit tomorrow, he has incurred an opportunity cost of δD. Alternatively, we can think of δ as other costs of depositing money (borrowing costs, the volatility of the currency in which deposits are made, etc.) We denote the deposit of the buyer by $D(B)$ and the deposit of the seller by $D(S)$.

In a terminal state w, the contract pays out transfers t_w^S to the seller and t_w^B to the buyer. For each final state w, it must hold that $t_w^S \geq 0$ and $t_w^B \geq 0$ and the following budget balance constraint: $t_w^S + t_w^B \leq D(B) + D(S)$. That is, the

smart contract can burn money, but it can not create money. We denote the pair of transfers (t_w^S, t_w^B) with t_w.

In the following, we are interested in contracts that maximize welfare (the sum of utilities), subject to incentive and participation constraints.

2.1 One-sided communication

We first consider the situation, where only the seller exchanges information with the contract. Since there are only two pay-off relevant states, we may assume without loss of generality (by the revelation principle) that there are two possible messages that the seller can send, which we denote by {"sent", "not sent"}. The seller is required to notify the smart contract about whether he has sent the item or not. There is some timeout, during which the seller has to respond. After having sent a message, the seller can be monitored. Without loss of generality, we may assume that monitoring only happens if the message "sent" has been received. Thus if the seller sends the message "not sent", the mechanism ends and transfer $t_{\bar{s}}$ are realized. If the seller sends the message "sent", the contract randomizes between monitoring and not monitoring. Monitoring happens with probability α. If monitoring does not happen, transfers $t_{s,\bar{M}}$ are realized. If monitoring happens, the seller is asked to provide the proof of sending. If the seller provides a proof, the transfers $t_{s,M,P}$ are realized, otherwise, transfers $t_{s,M,\bar{P}}$ are realized.

There are 4 final states, $w_1 = (s, M, P)$, $w_2 = (s, M, \bar{P})$, $w_3 = (s, \bar{M})$ and $w_4 = (\bar{s})$. Note that messages to the contract and actions are both part of a strategy set of a player.

Suppose we want to implement a contract where the seller always sends the file. Such an optimal contract minimizes the sum of the expected monitoring cost and the opportunity cost of depositing, subject to the relevant incentive and participation constraints. It is without loss of generality to assume that the mechanism is strongly budget balanced, because the buyer can get paid out any remaining deposits, after transfers to the seller have been realized. As only the seller interacts with the mechanism, this will not influence the incentive constraints, the participation constraint of the seller and will make satisfying the participation constraint of the buyer easier. In the following for each $1 \geq \alpha \geq 0$, we define by $E_\alpha[t_s^S] := \alpha t_{s,M,P}^S + (1-\alpha) t_{s,\bar{M}}^S$ the expected transfer to the seller, in case he has sent the file, assuming that he will always provide a proof if he is asked to (as he will optimally do) and analogously define $E_\alpha[t_s^B] := \alpha t_{s,M,P}^B + (1-\alpha) t_{s,\bar{M}}^B$. Then solving for the optimal contract such that the file is always sent, amounts to solving the following cost minimization problem.

$$
\begin{aligned}
\min \alpha(1-\delta)c + \delta(D(B) + D(S)) \\
\text{subject to } E_\alpha[t_s^S] - \alpha c \geq 1 + t_{\bar{s}}^S \\
t_{\bar{s}}^S \geq \alpha t_{s,M,\bar{P}}^S + (1-\alpha) t_{s,\bar{M}}^S \\
v + E_\alpha[t_s^B] \geq \frac{D(B)}{1-\delta} \\
E_\alpha[t_s^S] - \alpha c \geq 1 + \frac{D(S)}{1-\delta} \\
0 \leq t_w^S + t_w^B \leq D(B) + D(S) \text{ for each } w \\
t_w^S, t_w^B \geq 0 \text{ for each } w \\
D(B), D(S) \geq 0 \\
0 \leq \alpha \leq 1
\end{aligned}
$$

The first two constraints are incentive constraints of the seller. He should send the file rather than not send the file and truthfully reveal that he has not sent the file if he has not done so. The other incentive constraints are implied by these two, i.e. the seller will always reveal that he has sent the file if he has done so, and he will prove that he has sent the file if he is monitored and has sent the file. The third and fourth constraints are individual rationality constraints of the buyer and the seller. Note that they include the opportunity cost of depositing.

We first derive optimal deposits, given a particular monitoring policy.

Proposition 1. *If the seller is monitored with probability $0 < \alpha \leq 1$, then the problem is feasible if and only if*

$$v - 1 \geq \alpha c + \frac{\delta}{1-\delta}(\frac{1}{\alpha} + c).$$

In that case, optimal deposits are

$$D(S) = x \quad \textit{and} \quad D(B) = \frac{1}{\alpha} + c - x \textit{ for any } 0 \leq x \leq (1-\delta)(1-\alpha)(\frac{1}{\alpha} + c).$$

Proof. First, we show that in any feasible contract for a given monitoring probability α we have $D(B) + D(S) \geq \frac{1}{\alpha} + c$. We show that this holds for an optimal contract, and hence for any feasible contract. First observe that it is without loss of generality to assume that in an optimal contract $t_{s,M,\bar{P}}^S = 0$ (for each feasible solution, decreasing $t_{s,M,\bar{P}}^S$ will not change the objective value of the problem and will not change the feasibility of the problem). Next observe that it is also without loss of generality to assume that in optimal contract $t_{\bar{s}}^S = (1-\alpha) t_{s,\bar{M}}^S$ (as $t_{s,M,\bar{P}}^S = 0$, for each feasible solution with $t_{\bar{s}}^S > (1-\alpha) t_{s,\bar{M}}^S$, decreasing $t_{\bar{s}}^S$ without violating the constraint will not change the objective value of the problem and will not change the feasibility of the problem). Combining $t_{\bar{s}}^S = (1-\alpha) t_{s_{\bar{M}}}^S$ with the first constraint, we obtain

$$E_\alpha[t_s^S] - \alpha c \geq 1 + (1-\alpha) t_{s,\bar{M}}^S$$

or equivalently

$$\alpha t^S_{s,M,P} - \alpha c \geq 1.$$

Thus

$$D(B) + D(S) \geq t^S_{s,M,P} \geq \frac{1}{\alpha} + c.$$

An immediate consequence is that the condition $v - 1 \geq \alpha c + \frac{\delta}{1-\delta}(\frac{1}{\alpha} + c)$ is necessary for a feasible solution, as otherwise, the gains from trade do not exceed the monitoring and deposit costs (which are at least $\delta(\frac{1}{\alpha} + c)$ in each feasible solution). The condition is also sufficient, since following class of contracts is feasible and satisfies $D(B) + D(S) = \frac{1}{\alpha} + c$: Let $0 \leq x \leq (1-\delta)(1-\alpha)(\frac{1}{\alpha} + c)$. Let $D(B) = \frac{1}{\alpha} + c - x, D(S) = x, t^S_{s,M,P} = \frac{1}{\alpha} + c, t^S_{s,\bar{M}} = \frac{x}{(1-\alpha)(1-\delta)}, t^S_{\bar{s}} = \frac{x}{1-\delta}, t^S_{s,M,\bar{P}} = 0$. Note that the IC constraints and IR constraint for the seller hold (with equality). Moreover, if $(1-\delta)(v-1) \geq (1-\delta)\alpha c + \delta D(B)$, then the IR constraint of the seller holds, as:

$$v + (1-\alpha)D(B) = v + D(B) - 1 - \alpha c \geq \frac{D(B)}{1-\delta}.$$

Finally, we show that the optimal deposits have to be chosen such that $D(S) \leq (1-\delta)(1-\alpha)(\frac{1}{\alpha} + c)$. As we have shown, in an optimal contract, we have $D(B) + D(S) = \frac{1}{\alpha} + c$. Thus $t^S_{s,M,P} \leq \frac{1}{\alpha} + c$ and $t^S_{s,\bar{M}} \leq \frac{1}{\alpha} + c$. Therefore, by the IR constraint of the seller, $\frac{1}{\alpha} + c - \alpha c = 1 + (1-\alpha)(\frac{1}{\alpha} + c) \geq 1 + \frac{D(s)}{1-\delta}$, and therefore $(1-\delta)(1-\alpha)(\frac{1}{\alpha} + c) \geq D(S)$.

□

The proposition implies the following proposition:

Proposition 2. *If the problem is feasible, in each optimal solution the buyer is monitored with probability*

$$\alpha = \min\{\sqrt{\frac{\delta}{(1-\delta)c}}, 1\}.$$

Proof. By Proposition 1, we may assume that the sum of the monitoring cost and deposit cost is

$$\alpha(1-\delta)c + \delta(\frac{1}{\alpha} + c).$$

Minimizing this expression over all $0 < \alpha \leq 1$ yields the desired α. □

In general, there is a continuum of optimal contracts available that distribute the surplus differently between the seller and buyer. The payments in the non-monitoring case and the size of the seller's deposit determine the surplus distribution. We can characterize the seller optimal contract and the buyer optimal contract among the optimal contracts.

Proposition 3. *Let* $\alpha = \min\{\sqrt{\frac{\delta}{(1-\delta)c}}, 1\}$ *and* $(1-\delta)(v-1) \geq (1-\delta)\alpha c + \delta(\frac{1}{\alpha} + c)$.

1. *There is an optimal contract that is most preferred among optimal contracts by the seller: The seller deposits* $D(S) = 0$ *and the buyer deposits* $D(B) = \frac{1}{\alpha} + c$. *The seller receives the full deposit* $D(B)$*, if he messages "sent" and he is not monitored or monitored and provides a proof. He receives* $t^S_{\bar{s}} = (1-\alpha)D(B)$ *if he messages "not sent" and nothing if he does not prove if monitored.*

2. *There is an optimal contract that is most preferred among optimal contracts by the buyer: The seller deposits* $D(S) = 0$ *and the buyer deposits* $D(B) = \frac{1}{\alpha} + c$. *The seller receives the full deposit, if he is monitored and provides a proof, and nothing in all other states.*

Proof. By Proposition 2, in each optimal contract, the seller is monitored with probability α. Moreover, for the given α, in both contracts, all constraints are satisfied. In the first contract the IR constraint of the seller binds, as $\alpha D(B) - \alpha c = \alpha(\frac{1}{\alpha} + c) - \alpha c = 1$. Thus the contract is buyer optimal. In the second contract, the buyer obtains the whole deposit in all states that are reached with positive probability. Hence the contract is optimal for him. □

In both contracts, the seller does not make a deposit. However, there also exist optimal contracts where he deposits a positive amount. In these contracts, the payment in case of non-monitoring to the seller cover his depositing cost.

If the seller is completely risk-neutral, as we have assumed, the contract that pays him the deposit, if monitored, and nothing if not monitored, appears focal. It yields the highest pay-off for the seller, and only involves side-payments to the seller if the file has been sent. If we would relax the assumption of risk neutrality, an interior contract where payments in the monitoring and non-monitoring case are more equal, becomes more sensible.

Hidden Cost

Our previous discussion assumed that the monitoring cost is known. The analysis can be extended to the case where the monitoring cost is private information of the seller. As in a standard screening model, a menu of contracts can be offered where different type sellers choose different contracts. We briefly sketch the extension to the case with two cost types. Suppose there are two possible costs $0 < c_L < c_H$ and a fraction π of high-cost types and a fraction $1 - \pi$ of low-cost types. Similarly as in the proof of Proposition 1 for the full information case, one can show that there is an optimal menu where contracts are offered such that only the buyer makes a deposit, the seller receives the full deposit if monitored and nothing in all other states. However, the deposits (and thus the payment to the seller) is different than in the full information case. The (expected) cost minimization problem becomes

$$\begin{aligned}
\min \pi((1-\delta)\alpha_L c_L + \delta D_L(B)) + (1-\pi)((1-\delta)\alpha_H c_H + \delta D_H(B)) \\
\text{subject to } \alpha_L D_L(B) - \alpha_L c_L \geq \alpha_H D_H(B) - \alpha_H c_L \\
\alpha_H D_H(B) - \alpha_H c_H \geq \alpha_L D_L(B) - \alpha_L c_H \\
\alpha_L D_L(B) - \alpha_L c_L - 1 \geq 0 \\
\alpha_H D_H(B) - \alpha_H c_H - 1 \geq 0 \\
(1-\delta)(v - \alpha_H D_H(B)) \geq D_H(B) \\
(1-\delta)(v - \alpha_L D_L(B)) \geq D_L(B) \\
0 \leq \alpha_H \leq \alpha_L \leq 1, \quad D_H(B), D_L(B) \geq 0
\end{aligned}$$

α_X is the probability of monitoring, $D_X(B)$ and $D_X(S)$ are deposits of the buyer and the seller, respectively, for each type contract $X \in \{L, H\}$. It is straightforward to see that the IR constraint of the high type binds and that the IC constraint that

the low-cost type should take up the low-cost contract binds. Thus we obtain the conditions that

$$D_H(B) = \frac{1}{\alpha_H} + c_H$$
$$D_L(B) = \frac{1}{\alpha_L} + c_L + \frac{\alpha_H}{\alpha_L}(c_H - c_L)$$

Note that in comparison to the full information case, a larger deposit and corresponding larger payments to the seller have to be made in the low-cost contract. The optimal deposits lead to the following expression for the cost function:

$$\pi((1-\delta)\alpha_L c_L + \delta(\frac{1}{\alpha_L} + c_L + \frac{\alpha_H}{\alpha_L}(c_H - c_L))) + (1-\pi)((1-\delta)\alpha_H c_H + \delta(\frac{1}{\alpha_H} + c_H)).$$

The cost function is convex in the probabilities. Thus an optimum can be characterized by the first order conditions:

$$\frac{\delta}{\alpha_L^2} + \frac{\delta\alpha_H(c_H - c_L)}{\alpha_L^2} = (1-\delta)c_L,$$
$$\frac{\delta}{\alpha_H^2} = \frac{\pi}{(1-\pi)\alpha_L}(c_H - c_L) + (1-\delta)c_H.$$

2.2 Communication with both parties

Next, we consider the case where also the buyer exchanges information with the contract. the contract requires the buyer to confirm that he has received the item. As before, it is without loss of generality to consider two messages, as there are only two payoff-relevant states. We denote the two possible messages by: {"received","didn't receive"}. It is without loss of generality, to only use messages by the buyer, since a mechanism that also interacts with the seller cannot be more efficient, as both of the players hold the same bit of information.

The buyer is required to notify the smart contract about whether he has received the item or not. There is some timeout, during which the buyer has to respond. After having sent a message, the seller can be monitored. Without loss of generality, we may assume that monitoring only happens if the message "didn't receive" has been received. Thus, if the buyer sends the message "received", the mechanism ends and transfers t_r are realized. If the buyer sends the message "didn't receive", the mechanism randomizes with certain probability between monitoring and not monitoring. If monitoring does not happen, the mechanism ends and the transfers $t_{\bar{r},\bar{M}}$ are realized. Monitoring happens with probability α, in which case the seller is asked to provide a proof of sending. If the seller provides a proof, the transfers $t_{\bar{r},M,P}$ are realized. If the seller does not provide a proof, the transfers $t_{\bar{r},M,\bar{P}}$ are realized.

2.2.1 No Monitoring

There is a contract that achieves the first-best outcome and does not monitor at all. Note that if the mechanism does not monitor, the buyer will always choose the message which has the higher transfer for him (this is a form of cheap talk). Note

that there are only two final states in this case, (r) and $(\bar{r})$. If the buyer plays the truthful response in both cases, the seller can be incentivized to send the file by receiving a sufficiently large positive transfer in the state "received" and zero in the state "didn't receive". Optimally, the transfer in the state "received" will exactly compensate the seller for sending the file.[7] This mechanism satisfies all incentive compatibility and individual rationality constraints.

The contract without monitoring relies on the seller believing that the buyer will be truthful. He will only sign the contract if subsequently an equilibrium move, where the buyer chooses the truthful strategy, is played. Similarly, the buyer will only sign the contract if subsequently an equilibrium move, where the seller sends the file, is played. Thus the contract is only implemented if both parties believe that subsequently an efficient equilibrium move is played. If the players believe that an inefficient equilibrium is played, if the contract is implemented, they might not want to sign it. Monitoring allows to eliminate the inefficient equilibria and hence guarantees implementation, but at a cost. Next, we will discuss optimal contracts with a positive probability of monitoring.

2.2.2 Monitoring

In this section, we consider the case, where monitoring happens with probability $0 < \alpha \leq 1$. Suppose we want to implement a contract where monitoring happens with probability α, the seller always sends the file and the buyer always truthfully reveals whether the file has been sent.

As the buyer truthfully reveals the state, monitoring is off-equilibrium, and such optimal contract minimizes opportunity cost of depositing, subject to the relevant incentive and participation constraints. Appropriate deposits have to be made in order to make the threat of monitoring credible, even though monitoring will not happen in equilibrium. Similarly, now money burning can happen, but only off equilibrium. The cost minimization problem is:

$$
\begin{aligned}
\min \delta(D(B) + D(S)) \\
t^S_{\bar{r},M,P} - c \geq t^S_{\bar{r},M,\bar{P}} \\
t^S_r \geq 1 + \alpha t^S_{\bar{r},M,\bar{P}} + (1-\alpha) t^S_{\bar{r},\bar{M}} \\
t^B_r \geq \alpha t^B_{\bar{r},M,P} + (1-\alpha) t^B_{\bar{r},\bar{M}} \\
t^B_r \leq \alpha t^B_{\bar{r},M,\bar{P}} + (1-\alpha) t^B_{\bar{r},\bar{M}} \\
(1-\delta)(v + t^B_r) \geq D(B) \\
(1-\delta)(t^S_r - 1) \geq D(S) \\
t^S_w + t^B_w \leq D(S) + D(B) \text{ for each } w \\
t^S_w, t^B_w \geq 0 \text{ for each } w \\
D(B), D(S) \geq 0
\end{aligned}
$$

[7] If a larger transfer would be selected, inefficiently large deposits would have to be made. Since the buyer is indifferent between sending two different signals to the contract, the equilibrium is not "trembling-hand" perfect. However, there is a close to an optimal contract, where t^S_r is slightly above the seller's indifference value.

The first and second conditions are IC constraints for the seller to provide a proof if monitored and to send the file in the beginning. The third and fourth constraints are IC constraints of the buyer to truthfully reveal whether the file has been sent. The fifth and sixth constraints are the individual rationality constraints of the buyer and seller.

We first derive optimal contracts, given a particular monitoring policy.

Proposition 4. *If the seller is monitored with probability* $0 < \alpha \leq 1$*, then the problem is feasible if and only if*

$$v - 1 \geq \frac{\delta}{1-\delta} \max\{1, c\}.$$

In that case optimal deposits for $c \leq 1$ *are*

$$D(B) = 1, \quad D(S) = 0,$$

and for $c > 1$ *are*

$$D(B) = x, \quad D(S) = c - x, \quad \text{for any } \delta c + (1-\delta) \leq x \leq c.$$

Proof. The following transfers incentivize sending in equilibrium:

$$t_r^S = \max\{1, c\}, t_{\bar{r},M,P}^S = c, t_{\bar{r},\bar{M}}^S = t_{\bar{r},M,\bar{P}}^S = 0,$$
$$t_r^B = t_{\bar{r},\bar{M}}^B = t_{\bar{r},M,P}^B = t_{\bar{r},M,\bar{P}}^B = 0,$$

One readily checks that the IC constraints are satisfied.

For the IR constraints, we distinguish the case that $c \geq 1$ and $c \leq 1$. For $c \geq 1$, the IR constraint for the buyer becomes: $(1-\delta)(v + t_r^B) \geq x$ and the IR constraint of the seller becomes: $(1-\delta)(c-1) \geq c - x$ or equivalently $x \geq \delta c + (1-\delta)$. Since $t_r^B \leq c - t_r^S = c - 1$, we get that $(1-\delta)(v + c - 1) \geq x$, which implies that $x \leq c$, from the feasibility condition. Thus, the two IR constraints are satisfied by construction.

For $c \leq 1$ we let $D(B) = 1$ and $D(S) = 0$. Seller's individual rationality constraint is satisfied by construction. Buyer's individual rationality constraint is $(1-\delta)v \geq 1$ or equivalently $(1-\delta)(v-1) \geq \delta$. Thus, by our feasibility assumption it is satisfied.

Budget balance constraints are satisfied by construction.

Note that the objective function can not be improved: Deposits need to cover at least the monitoring cost. Thus we need total deposits of at least c. Furthermore, in the state r, the seller needs to receive at least 1, to satisfy his individual rationality constraint. Finally note that the feasibility condition is necessary, as otherwise the gains of trade do not exceed the depositing cost.

□

Remark 1. *With deposits of exactly* $\max\{1, c\}$*, we theoretically have the same problem as in our discussion of the no monitoring case: Incentive constraints only hold with weak inequality, and in particular the buyer is indifferent between telling the truth and lying. However, this is a boundary case and with deposits slightly greater than* $\max\{1, c\}$*, we can strictly incentivize truth-telling by the buyer, and sending and proving by the seller.*

Similarly, as in the previous section, there exist a continuum of optimal contracts (for high cost) that distribute the surplus differently between the buyer and the seller.

Proposition 5. *Let* $0 < \alpha \leq 1$.

1. *For* $c \leq 1$*, there is a unique surplus distribution in the optimal contract with monitoring probability* α *where the buyer extracts the whole surplus.*
2. *For* $c \geq 1$*, there is an optimal contract that is most preferred among optimal contracts with monitoring probability* α *by the seller: The buyer deposits* $D(B) = c$*, the seller deposits* $D(S) = 0$*. If the buyer confirms, the seller receives the full deposit* $t_r^S = c$*, if the buyer does not confirm, the seller receives the full deposit if he proves and nothing if he does not prove. The buyer receives no transfer in any state.*
3. *For* $c \geq 1$*, there is an optimal contract that is most preferred among optimal contracts with monitoring probability* α *by the buyer: In the contract deposits are* $D(B) = c$ *and* $D(S) = 0$*. If the buyer confirms, the seller receives* $t_r^S = 1$*, if the buyer does not confirm, the seller receives the full deposit if he proves and nothing if he does not prove. The buyer receives* $t_r^B = t^B_{\bar{r},\bar{M}} = t^B_{\bar{r},M,\bar{P}} = c-1$ *and* $t^B_{\bar{r},M,P} = 0$.

The result of Proposition 4 holds for any $\alpha \in (0, 1]$ and for each such α the contract achieves optimal welfare among contracts that monitor with positive probability. Note however that in the constructed optimal contract, money is burned in 3 states $(\bar{r}, \bar{M})$, $(\bar{r}, M, P)$ and $(\bar{r}, \bar{M})$. If we require strong budget balancedness (money is not burned in any state, even off equilibrium), that is, $t_w^S + t_w^B = D(S) + D(B)$ for each state w, then we need to require $\alpha \in [\alpha^*, 1]$ for some α^* to achieve the same optimal objective.

Proposition 6. *Let* $\alpha^* := \frac{1}{\max\{1,c\}}$*. Then for any* $\alpha \geq \alpha^*$*, there are deposits and transfers that achieve the optimal welfare without burning money and for* $\alpha < \alpha^*$*, there are no deposits and transfers that achieve the optimal welfare without burning money.*

Proof. First, we show that for $\alpha < \alpha^*$, the optimal objective can not be achieved. Combine the IC constraint of the seller to send with the truth-telling constraint of the seller to confirm sending if the buyer has sent the file with the strong budget balancedness, we get the following chain of (in)equalities

$$D(S) + D(B) = t_r^S + t_r^B \geq 1 + \alpha t^S_{\bar{r},M,\bar{P}} + \alpha t^S_{\bar{r},M,P} + (1-\alpha)(t^S_{\bar{r},\bar{M}} + t^B_{\bar{r},\bar{M}}) =$$
$$1 + (1-\alpha)(D(S) + D(B)).$$

Therefore, $\alpha \geq \frac{1}{D(S)+D(B)}$. By Proposition 4, for an optimal contract we have $D(S) + D(B) = \max\{1, c\}$. Thus, $\alpha \geq \frac{1}{\max\{1,c\}}$ in an optimum.

On the other hand, for $\alpha \geq \alpha^*$ we can design deposits and transfers, that induce sending at minimal deposit costs. We consider deposits as in Proposition 4. For

$c \geq 1$ we take transfers as follows:

$$t_r^S = t_{\bar{r},M,P}^S = t_{\bar{r},\bar{M}}^S = c, t_{\bar{r},M,\bar{P}}^S = 0,$$
$$t_r^B = t_{\bar{r},\bar{M}}^B = t_{\bar{r},M,P}^B = 0, t_{\bar{r},M,\bar{P}}^B = c,$$

The proof that these transfers work is analogous to the proof of Proposition 4.

For $c \leq 1$, we take transfers as follows:

$$t_r^S = 1, t_{\bar{r},M,P}^S = 1, t_{\bar{r},M,\bar{P}}^S = 0, t_{\bar{r},\bar{M}}^S = 0,$$
$$t_r^B = 0, t_{\bar{r},M,P}^B = 0, t_{\bar{r},M,\bar{P}}^B = 1, t_{\bar{r},\bar{M}}^B = 1.$$

The proof that these transfers work is analogous to the proof of Proposition 4.

□

Hidden cost

In contrast to the case of one-sided communication with the seller, with hidden cost, there is an optimal menu of contracts that achieves the first best and the seller cannot extract any informational rent. Note that for each cost $c > 0$, there exists a contract (see part c of Proposition 5) where the buyer deposits $D(B) = c$ and the seller is paid 1 independently of cost. In these contracts, the depositing cost which is a function of the monitoring cost is entirely borne by the buyer. Thus we can ask the seller for the monitoring cost and the seller has no incentive to report a different cost.

3 Conclusion

We initiate the study of smart contracts through the classical mechanism design perspective. In particular, we model the self-enforcing nature of smart contracts by taking deposits as a design parameter into account. We discuss the optimal design of contracts for file exchange. We identify the ranges of parameters and compare the effects of having only the sender communicating with the contract versus both players doing so. As a future agenda of research, we aim to study optimal smart contract mechanisms under uncertainty, which may include the valuations of both players. A similar approach developed in this paper can also be applied to insurance contracts, with costly state verification and risk-averse players, if they are run as smart contracts. It may suggest modification of existing contracts by adding deposits for all possible state realizations.

References

Allen, D. W. E., Lane, A., and Poblet, M. (2019). The governance of blockchain dispute resolution. *SSRN*.

Asgaonkar, A. and Krishnamachari, B. (2019). 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. In *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2019, Seoul, Korea (South), May 14-17, 2019*, pages 262–267.

Ben-Porath, E., Dekel, E., and Lipman, B. L. (2014). Optimal allocation with costly verification. *American Economic Review*, 104(12):3779–3813.

Ben-Porath, E., Dekel, E., and Lipman, B. L. (2019). Mechanisms with evidence: Commitment and robustness. *Econometrica*, 87(2):529–566.

Blumrosen, L. and Dobzinski, S. (2014). Reallocation mechanisms. In *Proceedings of the Fifteenth ACM Conference on Economics and Computation, EC 14*, pages 617–617.

Buterin, V. (2016). Ethereum whitepaper.

Cong, L. W. and He, Z. (2019). Blockchain disruption and smart contracts. *Forthcoming in Review of Financial Studies*.

Dziembowski, S., Eckey, L., and Faust, S. (2018). Fairswap: How to fairly exchange digital goods. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 967–984.

Gale, D. and Hellwig, M. (1985). Incentive-compatible debt contracts: The one-period problem. *The Review of Economic Studies*, 52(4):647–663.

Hartline, J. D. and Roughgarden, T. (2008). Optimal mechanism design and money burning. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 75–84.

Holden, R. and Malani, A. (2017). Can blockchain solve the holdup problem in contracts? *SSRN*.

Mookherjee, D. and Png, I. (1989). Optimal auditing, insurance and redistribution. *Quarterly Journal of Economics*, 104(2):399–415.

Myerson, R. B. and Satterthwaite, M. A. (1983). Efficient mechanisms for bilateral trading. *Journal of economic theory*, 29(2):265–281.

Townsend, R. M. (1979). Optimal contracts and competitive markets with costly state verification. *Journal of Economic Theory*, 21:265–293.

Witkowski, J., Seuken, S., and Parkes, D. C. (2011). Incentive-compatible escrow mechanisms. In *Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence, AAAI 2011, San Francisco, California, USA, August 7-11, 2011*.

Zhang, F., Cecchetti, E., Croman, K., Juels, A., and Shi, E. (2016). Town crier: An authenticated data feed for smart contracts. In *ACM CCS*, pages 270–282.