IMPLEMENTING MIXED STRATEGIES ON THE BLOCKCHAIN

ABSTRACT. We explore innovations available using blockchain technologies which allow two or more parties with conflicting interests to come to cooperative agreements. In light of Rubinstein's strategic approach to bargaining, it is clear that a probabilistic negotiation device would be an effective tool toward reaching the Nash Bargaining Solution. We argue that the blockchain may provide players with such a commitment device. Rational players with access to such a device should, in actual practice, be able to come to an agreement very near the Nash Bargaining Solution, in a short amount of time.

1. Introduction

The bargaining problem is often given as follows [Rub82, pg 97]:

> Two individuals have before them several possible contractual agreements. Both have interests in reaching agreement but their interests are not entirely identical. What "will be" the agreed contract, assuming that both parties behave rationally?

This is a difficult problem. Without ways to enforce binding threats, negotiation can be unpredictable, and often the outcome is determined by factors not easy to quantify within the scope of classical economic discussions. Solutions to hard problems are by nature evasive, so academics usually restrict themselves to tractable models. In 1953, Nash [Nas53] studied a model demand game, and gave axiomatic characterizations of the so called Nash Bargaining Solution. Rubinstein's seminal paper [Rub82] in 1982 indicated a possible strategic approach towards inducing a solution. Rubinstein's game (developed further in [BRW86]) introduced two factors forcing the players to resolve the game: 1) A penalty for time spent negotiating and 2) exogenous probability of negotiation breakdown.

Game theoretical situations, in contrast to real world negotiations, usually allow players to choose from a finite-parameter space of moves. In the real world, there are an unlimited number of moves, and there are an unlimited number of games players can choose to play. If one player has the ability to fully commit to a threat, this player can change the nature of the game by limiting the rational options of his opponent.

We argue that the blockchain provides two important features that make a Rubinstein solution practical. First, genuine, publicly observable randomness (cf. [BCG15]). Second, smart contracts that allow for sums of money to be directed around, based on randomness or on the direction of neutral oracles. With smart contracts, it is now much easier to credibly make threats.

We refer the reader to T.C. Schelling's classic text, [Sch60] for a fascinating discussion of how game theory meets the real world. A more modern reference on the theoretical side is given in the monograph [Mut99], which includes a thorough discussion of Rubinstein type games.

2. Levetrage

When two parties are negotiating over a surplus, there is a well-defined idea in game theory literature of what the agreement "should" be. This is called the Nash Bargaining Solution (NBS). Assuming that the NBS is the result of an efficient market, any agreement reached other than the NBS should be considered a market inefficiency.

We begin by stating our main result here, and then explain its components in the sequel. This is essentially given by arguments in [Rub82].

Theorem 1. *Suppose that two players are negotiating in a symmetric game where they each have access to commitment devices, commitment release devices, and probabilistic commitment devices. Rational players should agree very soon to an agreement very near the Nash Bargaining Solution.*

The following corollary follows from the translation invariance assumption of the Nash problem.

Corollary 1. *Suppose A has a legal right and ability to cause an event T to happen. If the cost to A of event T is c_1 and the cost to B is c_2, and if all players are rational and have access to probabilistic commitment devices and a device committing to T, B should pay A a sum of $\frac{c_2 - c_1}{2}$ to agree to not cause T.*

3. COMMITMENT DEVICES

Paraphrasing Schelling's definition of commitment: [Sch60][pg 127], we say that commitment involves maneuvers that leave one in a position so that their only rational option is follow through with a threat. The object of commitment is the credibility of a threat. Nash nicely summarizes the issues involving threats as follows [Nas53, pg 130]:

> If one considers the process of making a threat, one sees that its elements are as follows: A threatens B by convincing B that if B does not act in compliance with A's demands, then A will follow a certain policy T. Suppose A and B to be rational beings, it is essential for the success of the threat that A be *compelled* to carry out his threat T if B fails to comply. Otherwise it will have little meaning. For, in general, to execute the threat will not be something A would want to do, just of itself. The point of this discussion is that we must assume there is an adequate mechanism for forcing players to stick to their threats and demands once made: and one to enforce the bargain, once agreed. Thus we need a sort of umpire, who will enforce contracts of commitments.

3.1. **Commitment Using the Blockchain.** Smart contracts on the blockchain can provide a simple mechanism for commitment, by using an oracle. Suppose that A makes a threat. A can can always borrow a large amount of money, and tie the funds up in a smart contract on the blockchain. If a trusted oracle determines that the threat has not been followed through, the funds are "burned". So if two players are bargaining over \$100, A can declare that he will lose \$100 if he accepts less than \$95. Now B has no rational choice but to agree to \$95. We assume that the oracle can only see the outcome of the final agreement, and is not corruptible. (In practice, the perceived corruptibility is potentially an issue.)

3.2. **Commitment Release.** Taken at face value, the above commitment device leads to a "draw first" game. However, we argue that if one can create a commitment, one should also be able to create a way to release the other side from commitment. For example, if A ties up \$100 in a contract, B can counter with a slightly more complex contract: B also ties up \$100, and loses his \$100 if he makes any agreement, unless, \$50 is deposited into a third account that is directly controlled by B. Now A is released from his commitment: He can create a contract that controls \$50, sending it to the account controlled by B, if and only if

B agrees to the original 95/5 split. The oracle governing A's original contract can only see that an acceptable 95/5 split has been agreed to, but cannot see that A is contemporaneously giving \$50 back to B.

It does not take much imagination to see, that with trustworthy but scope-limited oracles, this game can can go on ad infinitum.

3.3. Advantages of the Blockchain for this type of commitment.

Implementing a legal contract accomplishing the above would be more problematic, we imagine.[1] The code that receives a broadcast signal and either refunds or distributes A's money is not a legal contract. It's a piece of code, and does not require considerations from multiple parties. Importantly, while a court can rule that a legal contract is not enforceable, courts cannot rule code executable, nor can they reverse the execution of the code once it is executed.

4. Mixed Strategies

If players are always able to make and release commitments as in the previous section, the game is essentially the same as without these devices. What is needed, then, is a threat to make the negotiations fail completely. Provided that a player has a mechanism for causing the negotiation to fail, this player can turn a messy game into a much tidier Rubinstein type game.

In particular, suppose that A knows that commencing irrevocable event T will cause the negotiation to fail, to both players' detriment. A can make an offer on some block of the blockchain, and then attach to it a probability p. If, after so many blocks, the offer is not accepted, then T happens with probability $(1 - p)$. Now B must not dilly-dally. If the offer is acceptable, it should be accepted. It will not be accepted, only in the situation that B believes that B can achieve a better outcome by continuing negotiation.

At this point, we claim the game is almost symmetric: B could immediately make a counter offer of the same nature, so provided p is near 1 there is little difference in who goes first. Now A should not make p too low: B can always immediately return the same offer the instant (or the next block) that B receives the offer. So little is gained by making p too low. However, there is always a probability that B will not receive the the threat. The only situation in which a low p would give advantage to A would be if A catches B in a situation where B has the ability to immediately accept the offer the instant it is offered, but not the ability to immediately return a counter offer.

4.1. Proof of Theorem 1.

We prove our theorem by arguing that p should be very close to 1 and the offer should be the Nash Bargaining Solution. (Recall that in the simplest symmetric case, the NBS simply splits the pot). We argue by contradiction: First we suppose that there is a strategy for A that has an expectation of larger than 1/2. A makes the offer determined by this strategy. Now the instant that the offer is received, by symmetry, B believes they can maximize their expectations going forward by making the same counter offer. Since this move by B (who is assumed rational) is determined, the expectation to A is still the expectation that remains. But B's expectation is at least that of A's, so both are larger than 1/2, a contradiction. So 1/2 is an upper bound for expectations to A. Thus, if A can achieve 1/2 via strategy S, A should implement S. One such strategy is to begin by offering 1/2. B also knows that the best B can hope for is 1/2, so B will accept it if offered. So A should make an offer, but attach with it some probability $p < 1$.

[1] The author is not trained as a lawyer and makes no representations of any sort of legal qualifications.

By choosing p slightly less than 1, B should accept as soon as possible, so as to minimize the probability that the game will end in failure.

5. Disagreement Device

In order to implement the game described in the previous section, we needed a credible disagreement device. In the literature, this problem is nontrivial: For example, we quote from a 2011 discussion of Rubinstein's game [AB11]:

> The presence of Nature's choice in that procedure is very appealing. It points out the possibility that a relationship may end after a failure to reach an agreement with some probability. But the fact that this probability is determined by one of the players may not be deemed very realistic.

With the randomness present in the blockchain, the probability can be determined by one of the players realistically. What is left is for us to show is that the blockchain can trigger a disagreement event. This means the contract should take an action that the player who created the contract cannot take back, and should be damaging to the other party.

We suggest a very simple form of such a device: The contract takes funds that previously belonged to a player, and deposits these into an account held by a third party. The third party has invoiced the player for services to be delivered as soon as funds are transfered. The player and the third party have signed an agreement making any payments non-refundable.

While there are a number a services that can legally be contracted for, we suggest one in particular: negative publicity.

For example, a player may make an arrangement with a PR firm for $2500 worth of negative publicity against his negotiating adversary. The PR agrees to perform this, pending a non-refundable payment. In many legal disputes, one litigant may have damning information on the adversary that will cause more damage to the adversary than the cost of spreading it. This works in particular if the litigant has a clear legal right to speak loudly and freely. [2] This can even be further automated: A freeway billboard company or internet advertising agency can sell negative advertising, and publish the advertising the instant the payment is received.

5.1. **Example.** Suppose a customer is sold a defective product, and the seller refuses to refund the product. The customer can threaten to spend several hundred dollars with a marketing firm publicizing just how horrible the defective product was. If the business stands to lose more in future sales than the cost of the marketing, the business is wise to offer the customer a refund, up to an amount determined by Theorem 1.

6. Randomness on the blockchain

Publicly observable randomness is an interesting open problem. Due to the decentralized nature of blockchains, future blocks are extremely hard to predict, and we think, the uncertainty is enough for the success of a mixed strategy. The question of whether the hash of a future block can be manipulated has been studied in [BCG15] and [PW16] where it is shown that some small influence may be bought for a very high price, but this must be done by bribing some portion of the mining pool. We feel such an attack would be extremely impractical. When designing a contract, it should be easy to require enough randomness to financially disincentivize any such attack. By simply hashing a future block, we should be able convince any observer that the hash will be impossible to predict, at least enough to create

[2] Again, the author is not a lawyer, this is merely armchair speculation

the effect of mixed strategies. Another option is to use an oracle that hashes an externally generated (and generally trusted) beacon such as NIST Randomness Beacon [NIS11]. Again, the only real objective is to refer to a beacon that any adversary will believe is unmalleable.

7. Concept Summary

The typical use case is as follows. An individual finds herself in a dispute initiated by another party, who is somewhat of a bully. Both parties have much to lose if the dispute escalates, however, the adversary might have more to lose, in particular because the adversary is in the wrong. Unfortunately for the individual, escalating the dispute comes with costs, so she is averse to that. The bully knows this, and uses this fact against her, continuing to extract concessions, and ignoring all threats. So instead of making a vacuous threat, our protagonist makes a probabilistic threat to expose the bully far and wide, and follows through with the threat, *probabilistically.* The first act of commitment is to simply let the random contract be executed. By doing this once, she has demonstrated that she can stomach the low probability of a bad outcome, knowing that the bully has considerably more exposure. When she makes the threat again, the bully can no longer rely on her self-interest and must think about his own. If the bully is rational, he will agree to end the dispute on equitable terms.

References

[AB11] Nejat Anbarci and John Boyd, *Nash demand game and the kalai-smorodinsky solution*, Games and Economic Behavior **71** (2011), no. 1, 14–22.

[BCG15] Joseph Bonneau, Jeremy Clark, and Steven Goldfeder, *On bitcoin as a public randomness source*, IACR Cryptology ePrint Archive **2015** (2015), 1015.

[BRW86] Ken Binmore, Ariel Rubinstein, and Asher Wolinsky, *The nash bargaining solution in economic modelling*, RAND Journal of Economics **17** (1986), no. 2, 176–188.

[Mut99] Abhinay Muthoo, *Bargaining theory with applications*, Cambridge University Press, New York, NY, USA, 1999.

[Nas53] John Nash, *Two-person cooperative games*, Econometrica **21** (1953), no. 1, 128–140.

[NIS11] *Nist randomness beacon*, https://beacon.nist.gov (2011).

[PW16] Cécile Pierrot and Benjamin Wesolowski, *Malleability of the blockchain's entropy*, IACR Cryptology ePrint Archive **2016** (2016), 370.

[Rub82] Ariel Rubinstein, *Perfect equilibrium in a bargaining model*, Econometrica **50** (1982), no. 1, 97–109.

[Sch60] T. C. Schelling, *The strategy of conflict*, Oxford University Press, 1960.

E-mail address: `mw@levetrage.com`

Mixed Metrics, LLC