CAN BLOCKCHAIN SOLVE THE HOLD-UP PROBLEM?

RICHARD HOLDEN AND ANUP MALANI

UNSW AND UNIVERSITY OF CHICAGO

OVERVIEW

1. Holdup is an important problem in contracts. Reduces gains from trade, output. Alters firm boundaries.
2. Contract theorists have devised mechanisms to address problem. But they require commitment (as would the original contract).
3. This commitment is hard to achieve with present contracting techniques.
4. Blockchain is a database technology that verifies transactions in a decentralized manner, makes transactions public, and – importantly – makes transactions very hard to reverse. Smart contracts are contracts written as computer scripts.
5. Smart contracts on blockchain enables commitment that either contract theory mechanisms, or the original contact, need to function.

A PHILOSOPHICAL NOTE

- This paper is not a piece of “blockchain advocacy”.
- Our goal is to press on what blockchain + smart contracts might be able to achieve in contracting
  - Our focus is on the classic bilateral setting (e.g. Buyer-Seller relationships) often studied in contract theory.
  - Interested in the implications are for the boundary of the firm.
- Lots of pros and cons to BC+SC—need to compare to status quo/existing contracting technology.
- We don’t think blockchain/smart contracts will change contract law.
  - But could be useful contracting technology.

1. THE HOLD-UP PROBLEM

- Buyer B agrees to buy quantity q widgets at price p from seller S.
- The buyer's valuation is v, seller's cost is c.
- B can make a relationship-specific investment to raise v to $v' > v$.
- S can make a relationship-specific investment to lower c to $c' < c$.
- Example of holdup: After B invests, S asks for a higher price $p' \in [p, p + (v' - v)]$.
- Ex ante, this reduces B's return to relationship-specific investment to $(v' - v) - (p' - p)$. Thus investment will fall.
- Obviously trade may decline if trade is only valuable with investment. Transaction may move from market to firm.

EXAMPLE: *ALASKA PACKER ASS'N V. DEMENICO*

- APA (buyer) hires fishermen (seller), including Demenico, from San Francisco to fish for salmon in Alaska and delivery fish to B's cannery near Haines. B agrees to pay each fisherman $50 + 2 cents/fish.

- After B charters boat to take S from San Francisco to Alaska, but before delivery of fish, S decides to ask for $100 + 2 cents/fish. B agrees.

- When boat with S returns to San Francisco, B pays $50 rather than $100 and S sues.

EXAMPLE: *ALASKA PACKER ASS'N V. DEMENICO*

- N.D. Cal. sides with S: B would not have agreed to the new contract unless it made sense to.
- CA9 sides with B: B gave S no consideration, hence this is a holdup.
- Commentators think the case stands for the proposition that renegotiation under duress invalidates the modified contract.
- We think the problem is not the rule, but the non-verifiability. Courts cannot verify the facts.
  - This case could have gone either way despite a good rule. DCt and App Ct. disagreed. Prof. Threedy notes other facts that courts missed.
  - Uncertainty of outcome for even the correct rule can deter investment.

2. CONTRACT THEORY'S SOLUTIONS TO HOLD-UP

1. Renegotiation design mechanisms. E.g., Chung (1991), Aghion, Dewatripont & Rey (1994), Noldeke & Schmidt (1995), Edlin & Reichelstein 1996.
   - Holdup stems from renegotiation of price
   - If we can structure renegotiation to ensure p' gives B enough incentive to make efficient investments, then we solve the harm from hold-up
2. Revelation mechanisms. E.g., Maskin (1977), Moore & Repullo (1988).

If these require too much information, then parties can try to bar any renegotiation in the original contract, e.g., have a no renegotiation clause (if de jure or de facto enforceable). But then the choice is between holdup and inflexibility.

Alternatively, parties can use asset ownership to address the problem. Hart & Grossman (1986), Hart & Moore (1990). See also, Williamson (1975), Klein, Crawford & Alchian (1978).

RENEGOTIATION-DESIGN MECHANISMS

- Example: Aghion-Dewatripont-Rey mechanism.
- Two components:
  - (i) A default trade--(price,quantity) pair, that can be triggered by one party (say the Seller)
  - (ii)The right to make a take-it-or-leave-it offer than is assigned to the other party (say the Buyer)
- TIOLIO gives Buyer full bargaining power and makes her residual claimant.
- Default option makes Seller residual claimant on her investment.
- Second instrument solves moral-hazard-in-teams problem.

REVELATION MECHANISMS

- E.g., Maskin and Moore-Repullo mechanisms.
- Maskin (1977)
  - If state of the world (e.g. investments, costs) common knowledge among parties then can induce truthful revelation to a third party
  - Both parties simultaneously announce:
    - if agree then implement
    - If disagree then punish
  - Truth-telling is a Nash equilm, but so is lying
  - Can only implement Maskin-monotonic Social Choice Functions—rules out distributional considerations
- Moore-Repullo (1988)
  - Use a three-stage mechanism to achieve truthful revelation as unique subgame-perfect equilm for *any* SCF

MOORE-REPULLO MECHANISMS

- A(pple) announces either 40 or 32. If the announcement is 40 then A pays C(orning) a price equal to 40 and the mechanism stops.
- If A announces “32” and C does not challenge A’s announcement then A pays a price of 32 and the mechanism stops.
- If C challenges A’s announcement then
  - A pays a fine of 30 to a T(hird party)
  - A is offered the glass for 22
  - If A accepts then C gets 30 from T (and 22 from A for the glass)
  - If A rejects the glass then C pays 30 to T
  - A and C Nash bargain over the glass

LIMITATIONS TO MECHANISMS

- Limited information: Parties do not know enough to write mechanisms.
- Information asymmetry (the common knowledge problem): Parties do not agree on v, c, and costs of investment.
- Aghion et al (2012): an arbitrarily small perturbation away from common knowledge destroys the truthful equilm in Moore-Repullo mechanisms
  - Indeed, *any* dynamic mechanism admits a non-truthful equilm

3. HARD TO ADDRESS HOLDUP WITH CURRENT TECH

- Example: Apple (B) wants to buy “gorilla glass” from Corning (S).
- Complete contract not feasible with non-verifiability.
- Repeat play and reputation: unravelling, uneven bargaining power degrades investment incentives.
- Integration not always feasible. If S sells to multiple B’s, merger with one S increases problems with other buyers.

3. HARD TO ADDRESS HOLDUP WITH CURRENT TECH

- Bar renegotiation altogether or use a mechanism. But these require commitment.
  - E.g., ADR requires a party to make 1 (TIOLI) offer and no more. But you need to commit not to make a second offer.
- Natural solution is penalty clauses.
  - But courts may not enforce those
  - Penalty clauses must be paid to a third party otherwise they distort investment incentives (overreliance). But parties have an incentive to not-report violations* or otherwise enjoin payments to third parties, as they can split payments.
- Solution is automatic penalty mechanisms. E.g., machine that burns cash. But the more effective they are, the more they look like smart contracts on blockchain.

4. WHAT ARE BLOCKCHAIN AND SMART CONTRACTS?

- Blockchain is a database technology that verifies transactions in a decentralized manner, makes transactions public, and – importantly – makes transactions very hard to reverse

- Smart contracts are contracts written as computer scripts

MOTIVATION FOR BLOCKCHAIN

- Introduced by Nakamoto (2008) as a payments solution
- Problem: Digital payments from A to B raise a double-spending problem: A can send the same digital cash to B and to C (like an MP3 file).
- Old solution: Have a central authority verify payments, stop double spending. But central figures often untrustworthy (LICs) or charge high transactions costs (HICs).
  - Trust was an acute concern during financial crisis.

NAKAMOTO'S SOLUTION: THE BITCOIN BLOCKCHAIN

- Suppose A has 10 in account and wants to send 10 to B and also to C
- Have A announce payments to network. Denominated in currency created by network (bitcoins) which are exchangeable elsewhere for USD, etc.
- Have others on network (nodes) race to record that they have seen the payment in a way that cannot be fabricated. i.e., if a node say A paid B, then it produces evidence that it could not unless in fact A said it paid B. Use hash functions, a type of one-way function.
    - Node's incentive to race is that they get a commission (in bitcoin).
- First transaction is recorded on public ledger (the blockchain).
    - If A sends 2 announcements (A pays B and A pays C), then the first to be validated is recorded and the second will be barred because A does not have enough money.
- By construction, you cannot go back and change the ledger (i.e., A cannot take money form other people to get more than 10 to give away) without re-validating all prior transactions, which Nakamoto (2008) shows would require a majority of the CPU power on the network.

MORE GENERALLY

- Accounts can mark ownership of all sorts of things (actions, goods, services) that are or you want to be rivalrous, not just digital payments. So blockchain can validate and record broad array of transactions.

- Being used for apps, real property, charitable contributions, produce, etc. (Though not clear it is needed for all these things.)

THE VALUE BLOCKCHAIN ADDS

Qualitatively new contributions:

- Decentralized “witnessing” of transactions

Incremental contributions:

1. Irreversible transactions
2. Public ledger of transactions (not entirely unique)
3. Anonymous transactions (transaction known, but ID is not)

Note: Blockchain doesn’t replace the need for certain standard enforcement mechanisms, but does provide incontrovertible evidence.

ASIDE: VALIDATION ON BLOCKCHAIN

- How do people “prove” they heard A announce “I send 10 to B”?
- Proof of work:
  - People on the network (nodes) race to run statement through a hash function that shows that they actually heard the statement. Running the hash function requires using CPU time (electricity).
- Proof of stake:
  - People on network in possession of the tokens/coins of the network can bet those on the statement that is correct. The transaction with more bets on it are real and are allowed to be hashed. To get something added you need enough tokens on the network.
- There are other methods of voting allowed to achieve consensus.

VALUE FROM SMART CONTRACTS

- Contracts written (in part) as computer scripts.
- They can be executed on blockchain using, e.g., Ethereum network.
- Value independent of blockchain: eliminate interpretation risk.
  - Scripts are interpreted by a compiler, which leaves no ambiguity.
  - Scripts may crash, but that can be tested in a sandbox/simulation.
- Blockchain-dependent value: eliminate counterparty risk.
  - Bind people to future transactions through irreversibility of blockchain.
  - E.g., A rents apt to B for $600/mo. In real world, if B has $600 on Sept. 30, can buy a dinner that evening for $25 and fall short on rent on Oct. 1. But with smart contract, the $600 is committed, so blockchain would stop B from buying dinner on Sept. 30.

5. HOW CAN BLOCKCHAIN ADDRESS HOLDUP?

- We need to implement a penalty clause triggered by deviation from original contract or mechanism. Penalty must be paid to third parties and must not be vulnerable to renegotiation by parties or injunction by courts.

1. Have contract use APIs to monitor all the contractual parties' accounts.
    - All parties have an incentive to provide access and APIs ex ante.

2. Write a penalty clause that pays third parties into the smart contract
    - A good way to do this is to make payments to public addresses and then announce the private keys to those addresses. Like putting a pile of cash on the corner of the room.

5. HOW CAN BLOCKCHAIN ADDRESS HOLD-UP?

- The parties cannot renegotiate as long as parties cannot make side payments that are verifiable by the code.

- The court cannot reverse the penalty payment. To do that, it needs to change the blockchain, which is what people use to record ownership of things. But to change the blockchain it needs, e.g., majority of CPUs on blockchain. (Analogy: court can award damages but cannot change stock price in a securities fraud case.)

- Penalty clause can be keyed to damages so that court cannot reverse penalty with damages.

IMPLICATIONS

- Half of all economic activity happens in markets, half in firms.
- Property-Rights Theory (Grossman-Hart-Moore) highlights the value and importance of asset ownership.
- Renegotiation-design and revelation mechanisms highlight what is possible *in theory* with contracts
  - But former require strong commitment power.
- Blockchain is a new technology which might make contractual solutions more feasible
- If so, would shift economic activity from firms to markets


END