Corruption is a Path to Security

Tymofiy Mylovanov

joint work with

Rakesh Vohra

March 28, 2019

Synopsis

- Model of blockchain
- High mining rewards are not needed to attract ‘honest’ miners
- High entry costs are unable to deter ‘dishonest’ miners
- Lowering costs encourages entrance of corrupt miners but gives incentives to honest miners to do the same
- Optimal to set zero entry costs and zero rewards for mining

What is?

- A database which anyone can read

- Purpose: ensure agreement among users about an underlying state that changes over time
  - e.g., property records

- The resources needed to support a (property) database are provided via taxes

- The novelty: no trusted entity to manage the database

What is wrong with a trusted party approach?

- Exclusion to sell access
- Corruption to further political (or private) ends
- Privacy abuse
- Absence of trusted parties

Blockchain is an alternative to trusted party

- Relies on competition between intermediaries

- Users of the blockchain platform coordinate on common software
  - allows anyone access to the database as well as copy it
  - enables users to participate using pseudonyms if they wish
  - while identities are private, transactions are not

Conflicts on blockchain

- Multiple copies of the database ensure access and reliability

- Maintaining consistency between independent copies when records are added to the database is a problem

- Conflicts (called **forks**) can arise because:
  - latency in the network
  - as a way to exploit counterparties via what is called a **double spend** attack

Blockchain secuirty

- Blockchain limits conflicts by restricting the right to update the database

- Proof of work (PoW) - the most popular protocol
  - assigns the right to augment the database via a costly ‘electricity burning’ contest
  - contest participants are called **miners** and the probability of winning is proportional to the amount of computational power held
  - the winner of the contest is rewarded with ‘tokens’ whose value is linked to the integrity of the database

Blockchain security

- As long as no miner holds more than 51% of all computational power, the probability of the double spending problem arising is vanishingly small (Lamport, Shostak and Pease (1982))

- The blockchain also bars deletions from the database so as to allow anyone to verify the consistency of a new entry with previous entries in the database

Blockchain security

- The central question is whether the blockchain protocol provides sufficient incentives to prevent conflicts arising in the database
  - Biais et. al (2018) model the blockchain protocol as a stochastic game with multiple Markov perfect equilibria, some with no conflicts among the databases
  - Abadi and Brunnermeier (2018) argue that the fees paid to miners as well as the money burnt to secure the right to update the database are essential to maintaining validity of the database, and limits the value of transactions that will be executed on the blockchain
  - Budish (2018) argues that the flow payments to miners for running the blockchain must be large relative to the one-off, benefit from attacking it

Our results

- In this paper we propose a simple model that generates conclusions that run counter to those just summarized:
  - Optimal reward for mining is equal to zero, contradicting the intuition that high mining rewards are needed to attract ‘honest’ miners
  - Social welfare is *independent* of the level of mining and entry costs
    - high entry costs don’t decrease social welfare because of wastefulness of the proof of work
    - high entry costs are unable to increase social welfare by deterring fraudulent miners.

Why the difference?

- Prior work has focused on the competition needed to make the database secure rather than the competition to ‘capture the platform’

Literature

- implications for intermediaries (GPT)
- incentives created by protocols (51%)
- optimal fees

Model

- $2n$ honest agents
- $2k$ dishonest agents
- Dishonest seek to engage in double spending
- Randomly pair up all the agents to trade ($n+k$ pairs)

Model

- if a match does not trade, zero payoff

- Should they choose to trade, the payoffs earned are as follows:

  1. If both parties are dishonest, each earns zero.

  2. If both parties are honest, each earns w.

  3. If one is honest and the other not, the honest agent earns $-v$ while the dishonest agent earns u with $v > u$.

Model

- The matched pair can choose to trade without verifying each others endowments or they can trade contingent upon verification of their respective endowments

- Verification is performed by agents called miners

- Any agent can choose to be a miner

- A miner is expected to check the endowment claims of the counter-parties and, if the trade is executed, update the database

- To avoid conflicts, only one miner is permitted to update the database

Model

- The costs of maintaining a single database (account) of prior transactions is C

- Any agent, honest or otherwise, can establish multiple accounts

- Verification is offered for a fee $2p^*$ that will be divided equally between the counter-parties

- An agent not a counter-party to the trade that is selected as miner, will correctly determine if the counter-parties are honest or not

- In the event that at least one counter-party is discovered to be dishonest, the trade is not executed

Payoffs

- Each agent, honest or otherwise, may act as a miner

- They have an incentive to establish multiple accounts so as to increase the chance that they will be selected

- Let μ_D be the number of miner accounts held by a dishonest agent and μ_H the number of miner accounts held by an honest agent

- We are assuming two agents of the same type will choose the same number of miner accounts

Payoffs

- If $\alpha = \frac{2n}{2(n+k)}$, the proportion of honest agents, the expected payoff to an honest agent, denoted V_H is:

$$\alpha w - (1-\alpha)\frac{\mu_D v}{2n\mu_H + 2k\mu_D} - p^* + \frac{(n+k)\mu_H}{2n\mu_H + 2k\mu_D} 2p^* - \mu_H C \quad (1)$$

- The expected payoff to a dishonest agent, denoted V_D, is

$$\frac{\alpha u \mu_D}{2n\mu_H + 2k\mu_D} - p^* + \frac{(n+k)\mu_D}{2n\mu_H + 2k\mu_D} 2p^* - \mu_D C \quad (2)$$

Dominance of honest miners

- Our first is result shows that in equilibrium no miner holds more than half of all accounts. In fact, the largest coalition of dishonest miners holds at most half of all verification accounts

  Theorem 1 *The equilibrium number of verification accounts held by honest agents exceeds that of dishonest agents. Furthermore, as p^* increases, the share of verification accounts held by dishonest agents increases*

Ratio of verifiers

- In equilibrium,

$$\frac{km_D}{nm_H} = \frac{nu + 2(n+k)^2 p^*}{nv + 2(n+k)^2 p^*}$$

- Increase in p^* increases the share of dishonest verifiers

Implications and Assumptions

- The conclusion of Theorem 1 relies on the marginal cost of a verification account being constant. It is not true otherwise
  - Were verification costs to grow quadratically with number of accounts, say, the conclusion of Theorem 1 does not hold
  - This suggests that raising the cost of holding multiple verification accounts is counterproductive
  - Instead, one should encourage many agents to hold multiple verification accounts, i.e., become miners

Budish (2018)

- In Budish (2018), it is argued that one must increase p^* to discourage a dishonest agent from setting up multiple verification accounts

- The difference arises because we allow multiple agents to compete to secure the right to be selected as miners

- An increase in p^* encourages dishonest agents to hold relatively more accounts. Hence one should lower the fee paid for verification

Total number of accounts

- The next result shows that the number of miner accounts decreases as C, the cost of setting up such an account increases. This is what one would expect

  Theorem 2 *In equilibrium, the total number of miner accounts is*

$$\frac{1}{C(n+k)[\frac{1}{nu+2(n+k)^2p^*}+\frac{1}{nv+2(n+k)^2p^*}]}$$

Social welfare

- Next, we show that total welfare is *independent* of C

Theorem 3 *In equilibrium, total welfare is*

$$\frac{n^2w}{n+k} - \frac{1}{(n+k)[\frac{1}{nu+2(n+k)^2p^*} + \frac{1}{nv+2(n+k)^2p^*}]}(1 + \frac{n(v-u)}{nv+2(n+k)p^*}).$$

Social welfare

- Theorem 3 runs counter to the intuition that a high cost for setting up a verification account is needed to discourage dishonest agents from corrupting the database

- This is a consequence of the assumption that verification costs grow linearly with the number of accounts but that strengthens the point made

Zero fees increase welfare

- Bertrand competition between miners will cause p^* to decline to zero

- Theorem 3 shows that this results in an increase in welfare
  - When $p^* = 0$, total welfare is

$$\frac{n^2 w}{n+k} - \frac{n^2 uv}{(n+k)(nv+nu)}(1+\frac{n(v-u)}{nv}) = \frac{n}{n+k}[nw - \frac{u(2v-u)}{v+u}]$$

- It is straightforward to check that total welfare is increasing in u and decreasing in v as one might expect.

Large markets

- **Theorem 4** *When $p^* = 0$ the equilibrium expected profit of an honest agent is*

$$(n+k)^{-1}[nw - \frac{vu}{2(v+u)}(1 + \frac{v}{v+u})].$$

The equilibrium expected profit of a dishonest agent is

$$\frac{nu^3}{2k(n+k)(v+u)^2}.$$

- If there was free entry of agents until the point of zero profit, the number of dishonest agents has to grow to infinity

- To understand the impact on welfare we also need to specify how number of honest agents grows

Large markets

- Suppose first that k and n grow such that $\frac{n^2}{k}$ goes to zero, i.e., the number of dishonest agents grows much faster than the number of honest agents

- From Theorem 3, we see that the expression for welfare tends to $-\infty$ no matter the value of p^*

- This means that at some point agents are better off opting out the platform, i.e., there is no trade

Large markets

- Let k and n grow such that $\frac{n}{k}$ goes to zero. Thus, the number of dishonest agents still grows faster than the number of honest agents

- The expression for welfare in Theorem 3 converges to zero.

Large markets

- Now suppose that k and n grow such that $\frac{k}{n}$ goes to zero

- Thus, the number of honest agents grows faster than the number of dishonest agents. In this case, when $p^* > 0$, total welfare grows with n provided w is sufficiently large. However, if $p^* = 0$, total welfare grows with n as long as $w > 0$

- This emphasizes the point that a large verification fee, i.e. $p^* > 0$, has negative effects

- If k and n grow at the same rate, total welfare grows with n. This highlights the fact that for the platform to be economically viable it must attract honest agents at least as high a rate than dishonest ones

Conclusions

- Trade presumes no uncertainty about the ownership of endowments being exchanged

- The blockchain substitutes dependence on a centralized authority with a software embodied protocol that provides incentives to maintain consensus about the distribution of endowments

- This paper argues that such incentives are counterproductive. Rather, the goal should be to encourage those who directly benefit from trade to shoulder the burden of maintaining consensus.