2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing,
Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics

A Mechanism Design Approach to Blockchain Protocols

Abhishek Ray
Krannert School of Management,
Purdue University
West Lafayette, IN, USA
Email: ray52@purdue.edu

Mario Ventresca
School of Industrial Engineering
Purdue University
West Lafayette, IN, USA
Email: mventresca@purdue.edu

Hong Wan
School of Industrial Engineering
Purdue University
West Lafayette, IN, USA
Email: hwan@purdue.edu

***Abstract*—Blockchain-based systems such as cryptocurrencies are achieving widespread usage, with a market capitalization of $150B (USD) as of September 2017. However, the most prominent platforms that account for over 70% of this market - Bitcoin & Ethereum - are exhibiting increasingly lower levels of decentralization. This poses the problem of concentrating levers of consensus to a select group of agents in the system. At the same time, attempts at higher levels of decentralization poses the problem of limiting scalability of such systems. In this paper, using mechanism design we propose a way of designing payoffs in order to disincentivize certain exhibited behaviors and incentivize desired behaviors of miners in such systems. Our approach indicates potential for research in this area for solving the much larger problem of centralization in decentralized systems such as blockchain.**

***Keywords*-blockchain, decentralization, game theory, centralization, mechanism design.**

I. Introduction

Blockchain is essentially an internet based system, that comprises of three major components. First, blockchain uses cryptographic methods (protocols) for maintaining a public ledger [12]. Second, blockchain has a container (coin/token) for generating value for users' transactions [6]. Third, any blockchain system has an incentive scheme for participants for eliciting effort and contribution of resources to conduct various record-keeping and verification activities for the transactions conducted by users [11]. These incentive schemes are implemented as part of the blockchain protocols [11]. Apart from incentives, blockchain protocols provide a set of rules for sending and receiving transactions [12]. Since the process of recording and validating transactions requires computational effort [2], incentive schemes are an integral part of these protocols. Blockchain systems have different incentive schemes but all such schemes inherently depend on the nature of transactions between participants. In cryptocurrency applications, transactions are in the form of exchange of coins/tokens between nodes whereas in other applications, it is transfer of value, through smart contracts [15]. The validity of a transaction is determined using two mechanisms - the account/ledger balances of entities involved in the transaction (as recorded on blocks) and solving of a cryptographic problem to provide proof of work/activity in validation of the transaction [12], [7], [18]. Selected nodes on the blockchain networks choose to participate and dedicate either computing power (Bitcoin) or stake in coins (Ethereum) to solving such problems [6]. These problem solving activities, referred to as mining, are considered to be incentive compatible since each mining operation performed successfully has a financial payoff - new coins produced in addition to a fraction of the transaction amount [8]. However, incentive compatibility of mining operations can prove to be problematic for a system designed to be decentralized [1].

A. Incentive Compatibility & Mining

Mining assumes that a majority of honest miners would keep the blockchain system decentralized and free from malicious attacks. An honest miner by definition is one who mines valid transactions on the longest chain that is recognized by other miners or on the chain that is longest at the time of mining [4], [11]. This assumption has been recently shown to be wrong [1], [2]. Empirically, it has been found that the top four Bitcoin-mining operations had more than 53% of the systems average mining capacity, measured on a weekly basis [14]. Mining for Ethereum was even more consolidated: three miners accounted for 61% of the systems average weekly capacity [3]. It was also found that 56% of Bitcoins nodes running its software are located in data centers, versus 28% for Ethereum [4]. Using game theoretic notions [1], [4], it has been shown that concentration of majority power in mining can pose the danger of 51% and selfish mining attacks. Essentially, tendencies of centralization in systems such as blockchain pose the threat of introducing the same problems of centralized mechanisms as found in existing banking and financial institutions. These problems can be broadly characterized as SPOF (Single Point of Failure), limited scalability and privacy issues [8]. At the same time, higher degree of decentralization leads to its own sets of issues such as the network's ability to scale to an ever-growing number of users, nefarious attacks on common pooled funds in DAO (Decentralized Autonomous Organization) [32], [33].

The fundamental question this poses is: *how should centralization tendencies be reduced in a system intended to be decentralized*? Relatedly, *how can the trade-off between decentralization and centralization be resolved for blockchain*

978-1-5386-7975-3/18/$31.00 ©2018 IEEE
DOI 10.1109/Cybermatics_2018.2018.00268

systems? Given the fact that the participants in such systems are agents with hidden information (honest or malicious miners/validators) how should blockchain protocols take into account such agents and provide incentive schemes for validation operations?

B. Main Contributions

Following are the main contributions of the paper:

1) This paper identifies intrinsic problems in designing mechanisms using non-cooperative game theoretic notions for blockchain based protocols.
2) Simple models of 2 and 3 miners are used to design a mechanism that disincentivizes collusion or cartel forming behavior among miners using non-cooperative simultaneous games. Our analysis shows that in the simplest case, payoffs can be constructed in a way that makes miners indifferent between forming cartels/pools and being of one type (either all S or all C). Further, we show the counterintuitive result that in the 2 player scenario, when types are identical and independently distributed, then designing mechanism with strictly positive payoffs is impossible.

II. Centralization tendencies in Blockchain

A. Centralization due to Scalability

Scalability essentially implies increased amount of transactions [11]. For scalability, more miners need to be incentivized to join in on the mining process [5]. In certain blockchain applications such as Bitcoin, mining operations also impact the overall supply of coins. Coin supply determines the off-platform value of such coins and motivates the type and quantity of coins used in transactions. The need for a much higher throughput in cryptocurrencies is therefore been a much desired change [9]. In Bitcoin specifically, scalability is desired mainly through increasing the block size [13]. But, increase in block size in particular and scalability in general is a huge concern because larger blocks mean increased storage space and slower propagation of messages through the network. This is bound to concentrate participation in blockchain to participants likely to maintain the higher sized blocks, which would lead to concentration of mining operations among fewer nodes. This would imply centralization of mining operations.

B. Centralization due to Protocols in Public Blockchains

Centralization tendencies are a problem mainly in public blockchains where any network participant can participate in the consensus process [11]. Distributed consensus requires protocols such as PoS (Proof of Stake) and PoW (Proof of Work) [18]. PoW (used in Bitcoin) essentially relies on the workload of solving a hash problem as a safeguard against malicious behavior [3]; PoS (used in Ethereum) takes coin-age as safeguard against malicious behavior [5]. In practice PoS and PoW have centralization tendency issues [15]. In PoW, mining difficulty increases for every 2016 blocks added to the longest chain. Miners may therefore collude to maintain a stable revenue stream in the face of increasing computational power needed to mine [1]. In the case of PoS, the age of a coin (amount of time for which a miner has the cryptocurrency) determines which miner gets to mine [12]. This does not essentially solve the problem of hashing power concentration since the ‘rich get richer’ problem still persists. Specifically, given the fact that the larger stake-holder (miner with larger and older units cryptocurrency) ends up with a larger profit margin, as a rational agent, a miner in PoS is incentivized to keep more of the mined cryptocurrency to increase its own probability of mining success. Hence, a larger stake-holder would grow his cryptocurrency stake faster than a smaller stake-holder [4]. After a point, the cost of being part of the mining operation would be too high relative to the payout for small stake holders and they would rationally drop out of the mining business. This therefore leads to centralization of mining and the rich get richer, faster [7].

C. Centralization due to Consensus Algorithms

Consensus algorithms in blockchain mainly solve the Byzantine Generals Problem (BGP) [15]. BGP is a known problem in computer science that basically deals with consensus in distributed systems [28]. In terms of blockchain systems, the network in its entirety has to agree upon every message (transaction) transmitted in the network [24], in the presence of nodes (agents using blockchain) that might be corrupt/malicious [11], [31]. The types of agents that participate in blockchain systems determine complexity of consensus [21]. There are mainly two types of agents - blockchain service firms and blockchain processing firms [16]. The blockchain service firms are those that accept or provide services in lieu of the token or coin (based on the blockchain system) being used by users. The blockchain processing firms are basically miners and participate in the blockchain ecosystem to provide labor for processing transactions - recording and validation. Currently, mining is dependent on three types of consensus [5]: **Rule Consensus** - validity of transactions should be based on rules decided by agents in the blockchain system. Only valid transactions end up in blocks. **History Consensus/Account Ledger Consensus** - history of transactions should be agreed upon by consensus of agents. This is important to verify every agent’s account balance, and which blockchain represents the true state of the ecosystem at any point in time. **Value Consensus** - agents have consensus on the value of each token being traded using the blockchain. This is important for transactions among agents to be of value. Ethereum and Bitcoin use different consensus algorithms to execute mining [11], [7]. Evidently, rule and history consensus suggests the tendency of centralization in blockchains (especially cryptocurrencies) as a real possibility. Specifically, miners tend to pool computing resources to extend a single branch of a tree, in order to ensure consensus on which transactions are valid (Rule), which is the true and most accurate chain of transactions in the system (History) as well as limit waste of resources in trying to fork the longest branch at any point [11], [1], [4]. However, this pooling of resources is under the assumption of honest mining[1], which may not always hold. For instance, if dishonest miners pool resources to extend the longest chain then a 51% attack in Bitcoin can lead to two main issues - miners deliberately fork the chain and double-spend transactions, or execute denial-of-service attacks against specific transactions or addresses.

D. Decentralization vs. Centralization

Higher levels of blockchain decentralization isn't free from its own set of problems. One of the problems that might come up is lack of scalability of network, with increasing participation from users [34]. Interest in blockchains has risen owing to its promise of decentralization of control among entities with minimal trust relationships [18]. But, there is a fundamental tension between scale and decentralization [19]. With higher participation from users, the need for faster throughput becomes more important, as evidenced in arguments for making Bitcoin a mainstream currency [11], [12]. Faster throughput is possible if more users opt to be miners or if mining power is increased, since each successful mining operation increases the difficulty of mining [1]. Hence scaling mining operations may require compromising the decentralized nature of blockchains [34]. In recent trends, it has been observed that higher throughput of transactions in a cryptocurrency such as Bitcoin or Ethereum is possible with lower degree of decentralization or higher concentration of processing power among select nodes [15], [23], [5]. In light of applications of blockchain to business and industrial operations at scale (e.g., cryptocurrency or smart contracts) this suggests that a balance needs to be achieved between centralization and decentralization [34]. This trade-off is incorporated in our analysis for designing a mechanism as described in Section IV-A.

III. Research Questions

Designing the protocols clearly needs improvement, given the aforementioned problems in Bitcoin and Ethereum. The area of mechanism design can help in designing improved protocols for blockchains [17]. Specifically, since each agent acting as a miner on the blockchain transacts given some incentive, the main research question is - *is there a mechanism that incentivizes one type of behavior and disincentivizes the other type, among miners?* If so, *how can such a mechanism be designed and what are the parameters of the mechanism that can help achieve the desired behavior?* Further, *how can the design of such mechanisms inform the development of better consensus protocols in blockchain?*

A. Why Mechanism Design?

In the case of blockchain consensus protocols, mechanism design can help in solving the problem of centralization vs. decentralization in two primary ways. First, mechanism design can help in designing better incentive schemes in protocols when private information[2] among participating users is unknown to the designer[1]. Second, better designed incentives help truthful revelation of information about costs and objectives such that cartel formation and collusion is alleviated[17]. Hence, any effective protocol should take into account truthful information of such self-interested agents. Mechanism design approach to the problem has been discussed mainly in forums such as recent blockchain conferences[35], Ethereum Open Challenge[7] etc. We hope to add to this growing body of work through this paper.

IV. Game Theoretic Model

A. Setting

Assume the existence of a blockchain and an underlying consensus mechanism[3] that allows mining. Using abstraction, a blockchain mining game can be considered as a set of N players, each with hidden information of its own type t, incurring a fixed or stochastic cost to build the most relevant branch of the chain. The relevance of a chain is dependent on the application - in Bitcoin or Ethereum it is the longest chain or the one with highest cumulative difficulty. Further, mining blocks is a stochastic endeavor and hence, miners engaging in mining receive expected payoffs. In the game setting, the branch of the chain is built by adding blocks to it and each player $i \in N$ is trying to add blocks by solving a problem of varying difficulty. The game plays for T rounds and each round ends with one player winning the round by adding a block to the relevant branch. In this way, each player realizes an expected payoff at the end of the game based on the probability of winning some number of rounds. The decision each player faces at the beginning of the game is to choose a type, which would dictate the expected payoff at the end of T rounds. The problem for the designer is to specify payoffs for this game, such that players are less incentivized to cooperate with other selfish players. In the following two sections, we present a simplified version of this setting to demonstrate the approach.

B. Example: Two Player Mechanism

Consider two players (miners) and a type space $\Phi = \{S, C\}$. Here, S refers to Selfish behavior and C refers to Cooperative behavior. Each player can assume a type that is privately known. Irrespective of type, the expected payoffs of the game are common knowledge and it is assumed that once the players know their type, they mine blocks to either compete to extend the branch they think should be

[1] Refer definition of Honest Mining in Section 1

[2] Costs and objectives from mining is private information to miners

[3] Assume PoW as the mechanism for mining

longest (S-S) or extend the chain that they both know to be longest (C-C). In practice, these two scenarios capture the fact that all miners add blocks to the longest chain they know of, or the first one they heard of if there are branches of equal length [1]. Alternatively, one player may cooperate with the other player to extend their chain (S-C or C-S). This is equivalent to mining pools. All members of a pool work together to mine each block, with the the profit-making entity distributing their revenues when one of them successfully mines a block[4]. The payoffs for player i from choosing any one of type a, b such that $a, b \in \Phi$ is given by V_{iab}. So, if player 1 chooses S and player 2 chooses C, the payoff to player 1 is V_{1sc}, as shown.

1) Assumptions: Clearly, for this simple case it is assumed that the game is completely mixed. That is, the Nash Equilibrium of the game is such that the mixed strategy of each player places positive probability on every strategy available to the player. This is reasonable in the setting of blockchain mining pools since miners can have a purely mixed strategy of either mining for a mining pool or running their own mining operation [4]. Further, for simplicity of exposition following is the assumed prior on types: $P(S) = \alpha \in (0, 1)$, $P(C) = 1 - \alpha \in (0, 1)$. Two cases are considered, given assumed prior. Types of each player are either correlated or are independent of each other. With independent types, it follows that $P(S, S) = \alpha^2$, $P(C, C) = (1 - \alpha)^2$ and $P(C, S) = P(S, C) = \alpha(1 - \alpha)$. With correlated types, $P(C, C) = P(S, S) = \beta$, $\beta < \alpha$ along with $P(C, S) = P(S, C) = \frac{1}{2} - \beta \; s.t. \; \frac{1}{2} > \beta > \frac{1}{4}$. These values are assumed for expositional simplicity.

2) Objective Function: We consider minimizing the tendencies between centralization and decentralization. In other words, it is desired that collusive behavior is discouraged and honest behaviors are encouraged. Equilibria corresponding to honest behavior is either in (S-S) or (C-C) cases. Dishonest behavior is where agents collude to maximize payoff and is either (S-C) or (C-S) (e.g., selfish mining/mining pools)[12]. We consider minimizing the ratio between honest behavior payoffs desired and dishonest behavior payoffs exhibited, which is similar to notions of price of anarchy or price of stability[10]. The objective function can be expressed as

$$\Phi = \frac{V_{1ss} + V_{2ss} + V_{1cc} + V_{2cc}}{V_{1sc} + V_{2sc} + V_{1cs} + V_{2cs}} \tag{1}$$

This functional form assumes that trade-off between centralization & decentralization can be expressed as ratio between honest behavior and dishonest behavior[4]. Hence, this ratio is minimized. Clearly, with increase/decrease in either centralization or decentralization, the ideal case would be where this ratio is 1. Proposition 1 & 2 are related to problems when designing mechanisms when minimizing this trade-off.

3) Constraints: The constraints for the game are the Incentive Compatibility and Individual Rationality conditions. Since the type chosen by each player is private information, we use Bayesian Incentive Compatibility. Further to rule out cases where players might not participate we assume ex-post individual rationality. For the cases enumerated previously considering independent and correlated types, the constraints are as follows $\forall \; i = 1, 2$.
Independent Types:

$$(1 - \alpha)\left(V_{isc} - V_{icc}\right) \geq \alpha\left(V_{ics} - V_{iss}\right) \tag{2}$$

$$(1 - \alpha)\left(V_{icc} - V_{isc}\right) \geq \alpha\left(V_{iss} - V_{ics}\right) \tag{3}$$

Correlated Types:

$$\frac{\left(\frac{1}{2} - \beta\right) V_{isc} + \beta V_{iss}}{\alpha} \geq \frac{\left(\frac{1}{2} - \beta\right) V_{icc} + \beta V_{ics}}{\alpha} \tag{4}$$

$$\frac{\left(\frac{1}{2} - \beta\right) V_{ics} + \beta V_{icc}}{1 - \alpha} \geq \frac{\left(\frac{1}{2} - \beta\right) V_{iss} + \beta V_{isc}}{1 - \alpha} \tag{5}$$

Strictly positive payoff is assumed as

$$V_{iss}, V_{icc}, V_{isc}, V_{ics} > 0 \tag{6}$$

Strictly positive payoff is assumed to maintain strict individual rationality of miners in the system. Relaxing this assumption may lead to cases where miners are indifferent between mining or not mining.

4) Optimization Problem: The mechanism design problem is framed as an optimization problem as follows.

$$\underset{V_{iss}, V_{isc}, V_{ics}, V_{icc} \; \forall \; i=1,2}{\text{Minimize}} \quad \frac{V_{1ss} + V_{2ss} + V_{1cc} + V_{2cc}}{V_{1sc} + V_{2sc} + V_{1cs} + V_{2cs}} \tag{7}$$

subject to IC and IR constraints, given the scenario. For each scenario, analysis has been conducted to give the following results.

Proposition 1. *No solution exists for i.i.d miner types.*

The general strategy of the proof is to analyze cases of the Lagrangian of this optimization, with the constraint of positive payoffs holding, and show that a solution under these conditions is impossible. The intuition for this proposition sheds light on the difficulty of designing a mechanism where the probability of miners choosing types are i.i.d. In practice, this may imply that designing mechanisms to induce desired behavior when faced with equally capable miners playing the same strategy is impossible when payoffs have to be designed that are positive (individually rational) in all scenarios. Of course, if the positive payoff constraint is relaxed, the trivial solution is setting $V^*_{iss} = V^*_{icc} = 0$ along with $V^*_{isc} = V^*_{ics}$.

Proposition 2. *The optimal solution to minimizing Φ for correlated types is*

$$V^*_{ics} = V^*_{iss} \tag{8}$$

$$V^*_{isc} = V^*_{icc} \tag{9}$$

[4] E.g.- AntPool run by BitMain Technologies

$\forall\ i = 1, 2.$

The general proof strategy is to analyze the Lagrangian of the optimization problem for all scenarios of Lagrangian coefficients (inequalities holding or not holding with equality). In addition, note that mixed equilibrium conditions still hold. The proposition intuitively states that making miners indifferent between defecting to S when the other miner is C or vice versa reduces ratio between the two possible equilibria. Further, if each decision variable ($V_{isc}, V_{ics}, V_{icc}, V_{iss}$) is considered as a function of parameters of blockchain system (longest blockchain length, costs of mining etc.) then by the Spence Mirrlees property [31], further restrictions can be placed on the payoffs in terms of these parameters. This part of the analysis is left for future work.

C. Example: Three Player Mechanism

The three player mechanism has the same type space of $\Phi = \{S, C\}$, distributed over three players. The payoffs are now constructed using two matrices - one for each type for player 3. The payoffs are expressed as e.g., V^c_{ics} when player i is of type c and other two players are of types c, s. For simplicity of exposition, the prior in this case is assumed in a similar manner as for two players - either independent or correlated. For correlated, the simplest case is analyzed. The priors are assumed as $P(S, S, S) = P(C, C, C) = \beta \in (0, 1)$ while all other combinations are assumed to have probability γ such that $2\beta + 6\gamma = 1$. Φ in this case is similar to two player case. S-S-S and C-C-C behaviors are encouraged and all other combinations are discouraged. The objective function is therefore defined as,

$$\Phi = \frac{\sum_{i\in\{1,2,3\}} V^s_{iss} + V^c_{icc}}{\sum_{i\in\{1,2,3\}} V^c_{iss} + V^s_{icc} + V^s_{isc} + V^c_{isc} + V^s_{ics} + V^c_{ics}} \tag{10}$$

The optimization problem to be solved is similar to (7). Further, we assume strictly positive payoffs for designing the mechanism.

Proposition 3. *No optimal solution exists for i.i.d miner types. For correlated types, the optimal values of payoffs satisfy the following condition:*

$$\frac{\beta}{\gamma}\left(V^{s*}_{iss} - V^{c*}_{iss}\right) = \left(V^{c*}_{ics} - V^{s*}_{ics}\right) + \left(V^{c*}_{isc} - V^{s*}_{isc}\right) + \left(V^{c*}_{icc} - V^{s*}_{icc}\right) \tag{11}$$

$$\frac{\beta}{\gamma}\left(V^{c*}_{icc} - V^{s*}_{icc}\right) = \left(V^{s*}_{iss} - V^{c*}_{iss}\right) + \left(V^{s*}_{isc} - V^{c*}_{isc}\right) + \left(V^{s*}_{ics} - V^{c*}_{ics}\right) \tag{12}$$

The proof for this is similar to the proof for two agent mechanism with correlated types and has been left out due to space constraints. At the optimal, Incentive Compatibility equations hold with equality $\forall\ i = 1, 2, 3$. Intuitively this proposition states that $\forall\ i = 1, 2, 3$, players can be made indifferent between defecting from e.g., S to other type C when the majority is one type (S), by incentivizing being S in all other scenarios. Again, since either S-S-S or C-C-C behaviors are considered optimal from a design perspective, defecting from scenarios where majority are S or C is to be discouraged. Hence, designing payoffs that reduce these tendencies would reduce Φ due to cartel or collusive behaviors (e.g.,S-C-C, C-S-S).

V. Conclusion & Future Research Directions

The previous sections identified a new way of framing and solving the problem of centralization in blockchain. However, the work on designing robust and optimal mechanisms for blockchains is a fast emerging area of research as evidence in recent industry discussions [23]. Blockchains enable development of a medium for value transfer in areas where it would otherwise be impossible, such as smart contracts and cryptocurrencies. Consequently, applications of blockchains radically expand the range of problems to which economic incentives can successfully be applied [21]. The work involving mechanism design can proceed in broadly two directions - uncoordinated majority models assume protocol participants make independent choices and no actor controls more than a given percentage of the network. Coordinated choice models on the other hand assume that most or all actors are colluding through some agent or coalition of agents, though sometimes free entry from non-colluding actors is assumed. In line with this, this paper highlighted probable approaches to design mechanisms using the uncoordinated line of analysis. In the future, we plan on working on extending this to add simulations to theoretically derived policies/payoff allocations.

Acknowledgment

The authors would like to thank the anonymous conference reviewers for their constructive comments. The authors would also like to express their gratitude to Vaneet Aggarwal, Arnob Ghosh, Viplove Arora and Bryan Chong for their review comments in the initial stages of the paper.

References

[1] Eyal, I. and Sirer, E.G., 2014, March. Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security (pp. 436-454). Springer, Berlin, Heidelberg.

[2] Kroll, J.A., Davey, I.C. and Felten, E.W., 2013, June. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (Vol. 2013, p. 11).

[3] Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A. and Rosenschein, J.S., 2015, May. Bitcoin mining pools: A cooperative game theoretic analysis. In Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems (pp. 919-927). International Foundation for Autonomous Agents and Multiagent Systems.

[4] Eyal, I., 2015, May. The miner's dilemma. In Security and Privacy (SP), 2015 IEEE Symposium on (pp. 89-103). IEEE.

[5] Bhme, R., Christin, N., Edelman, B. and Moore, T., 2015. Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), pp.213-38.

[6] Bradbury, D., 2013. The problem with Bitcoin. Computer Fraud & Security, 2013(11), pp.5-8.

[7] Buterin, V., 2014. Long-range attacks: The serious problem with adaptive proof of work.

[8] Karame, G., 2016, October. On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1861-1862). ACM.

[9] Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A. and Rosenschein, J.S., 2015, May. Bitcoin mining pools: A cooperative game theoretic analysis. In Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems (pp. 919-927). International Foundation for Autonomous Agents and Multiagent Systems.

[10] Roughgarden, T., 2012, June. The price of anarchy in games of incomplete information. In Proceedings of the 13th ACM Conference on Electronic Commerce (pp. 862-879). ACM.

[11] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[12] Pilkington, M., 2016. 11 Blockchain technology: principles and applications. Research handbook on digital transformations, p.225.

[13] Sapirshtein, A., Sompolinsky, Y. and Zohar, A., 2016, February. Optimal selfish mining strategies in bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 515-532). Springer, Berlin, Heidelberg.

[14] Primavera, D.F. and Loveluck, B., 2016. The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. Internet Policy Review, 5(4).

[15] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE International Congress on (pp. 557-564). IEEE.

[16] Papadopoulos, G., 2015. Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies. In Handbook of Digital Currency (pp. 153-172).

[17] Maskin, E., 2008, December. Mechanism Design Theory: How to Implement Social Goals. In WINE (p. 1).

[18] Abdulkadirolu, A. and Snmez, T., 2003. School choice: A mechanism design approach. American economic review, 93(3), pp.729-747.

[19] Aumann, R.J., 1961. The core of a cooperative game without side payments. Transactions of the American Mathematical Society, 98(3), pp.539-552.

[20] Garey, M.R. and Johnson, D.S., 2002. Computers and intractability (Vol. 29). New York: wh freeman.

[21] Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D. and Weinhardt, C., 2018. A blockchain-based smart grid: towards sustainable local energy markets. Computer Science-Research and Development, 33(1-2), pp.207-214.

[22] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S., 2013, October. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.

[23] Ethereum Summit, Waterloo - https://ethwaterloo.com/.

[24] Sandholm, T., Larson, K., Andersson, M., Shehory, O. and Tohm, F., 1999. Coalition structure generation with worst case guarantees. Artificial Intelligence, 111(1-2), pp.209-238.

[25] Yokoo, M., Conitzer, V., Sandholm, T., Ohta, N. and Iwasaki, A., 2005, July. Coalitional games in open anonymous environments. In AAAI (Vol. 5, pp. 509-514).

[26] Sargent, T.J., 2009. Dynamic macroeconomic theory. Harvard University Press.

[27] Mainland, G., Parkes, D.C. and Welsh, M., 2005, May. Decentralized, adaptive resource allocation for sensor networks. In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2 (pp. 315-328). USENIX Association.

[28] Lamport, L., Shostak, R. and Pease, M., 1982. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), pp.382-401.

[29] Rosen, J.B., 1965. Existence and uniqueness of equilibrium points for concave n-person games. Econometrica: Journal of the Econometric Society, pp.520-534.

[30] Gordon, G. and Tibshirani, R., 2012. Karush-kuhn-tucker conditions. Optimization, 10(725/36), p.725.

[31] Milgrom, P. and Shannon, C., 1994. Monotone comparative statics. Econometrica: Journal of the Econometric Society, pp.157-180.

[32] Goodin, D., 2016. Bitcoin rival Ethereum fights for its survival after $50 million heist. ArsTechnica Online.

[33] Hemprel, J. 2016. A $50 Million Heist calls a new Virtual Currency into Question. What should Ethereum do about it? Wired Inc.

[34] Slepak, G. and Petrova, A., 2018. The DCS Theorem. arXiv preprint arXiv:1801.04335.

[35] Weeks, M., 2018. The Evolution and Design of Digital Economies.