Researchers on Coalition-Proof Consensus in Blockchain

Yonghong Yu[1,a], Li Wu[2,b]

[1]School of Management Science and Engineering, Anhui University of Finance & Economics, Bengbu 233030, China;

[2]School of Finance and Public Management, Anhui University of Finance & Economics, Bengbu 233030, China.

[a]ac120107@163.com, [b]bbwuli@163.com

Abstract

Public blockchain is a completely decentralized distributed ledger technology, which allows nodes to freely choose whether to participate in data verification, mining and other key tasks to maintain system stability, and among all the key tasks, the consensus algorithms play an important role in the blockchain systems. In addition to considering technologies and mathematics to ensure consensus algoritm efficiency in blockchain system, many other factors need also be considered, such as the behaviors of all players. This paper diccusses about the consensus of blockchain under the view of game theory, it provides a complete information static game theory frame among all players in blockchain system, and gives the coalition-proof Nash equilibrium. Some suggestions are also proposed to ensure consensus can be effectively implemented in public blockchain system.

Keywords

Public Blockchain; Game Theory; Coalition-Proof Nash Equilibrium; Consensus.

1. Introduction

Public blockchain is a completely decentralized distributed ledger technology, which allows nodes to join or exit freely without registration, authentication and authorization of central nodes. Network nodes have equal status, share the entire blockchain account book, and each node can freely choose whether to participate in data verification, mining and other key tasks to maintain system stability. Due to the lack of identity authentication and privacy protection mechanism, public blockchain needs to rely on economic incentive mechanism to encourage network nodes to maintain the system spontaneously. Therefore, it faces many problems such as security risks, weak anonymity and incompatible incentive mechanism.

There exist a number of strategies and methodologies of consensus of blockchain system[1,2,3,4], and these strategies and methodologies are mainly based on the viewpoint of engineering and mathematics[5,6,7], and they play an important role in the blockchain systems. Nakamoto [5] used proof of work(POW) as consensus algorithm, POW is a kind of reuseable hashcash proof of work, it processes the advantage of decentralization and distribution, it also processes the disadvantage of resource wasting, attacking security issues. Larimer [6] presented proof of stake(POS), the core idea of POS is to control the number of assets and use time to determine the accounting rights of participating nodes, the advantages of POS is that it does not consume resources, and the holders of core rights have the ability to change the network without the approval of all network participants. The disadvantage of POS is that the monopoly control of the network by the master of core rights destroys the decentralized function of the distributed ledger system. Castro [7] proposed a practical Byzantine fault-tolerant algorithm(PBFT) to solves the problem of lower efficiency of the original Byzantine fault-tolerant algorithm. It reduced the complexity from exponential level to polynomial level and made Byzantine fault-tolerant algorithm is feasible in practical system application. This consensus mechanism can be applied to digital asset platforms that do not need large throughput but need to handle many events. In the process of reaching a consensus, each node publishes the public

key, and verifies its format by signing the message of the node. Once the same sufficient number of responses are reached, the transaction reaches a consensus.

Public blockchain is suitable for fully open, nationwide supervision and network autonomy application fields. Bitcoin and Ethereum are typical application cases. With the increasing of large-scale and complexity of Bitcoin, Ethernet, Hyperledger and so on, however, it is difficult for the point of technologies and mathematics to control and ensure the consensus efficiency of public blockchain, and we need to introduce new mechanism to guarantee the consensus efficiency of public blockchain systems. Public blockchain systems involves different types of participants, these players are rational and self-interested, and have no malicious intention. Due to the lack of identity authentication and privacy protection mechanism, lacking of incentive and constraint mechanism will greatly influence the behavior between players which may perform negative behaviors under the consideration of cost and other factors, and thus affecting the consensus implementation in the public blockchain systems, causing the failure of consensus in public blockchain systems. Because the participants have different responsibilities in public blockchain system, they may have different behaviors under the consideration of payoff, cost and workload, and there exists a game among them. This paper designs an effective mechanism that the rational and self-interested players should be liable for their negative behaviors of causing failure of consensus and bear the relevant punishment. On the other hand, if players abide by the agreement, they should get appropriate incentives. This paper mainly discusses the consensus efficiency of public blockchain systems based on the perspective of game theory. All players of this game are assumed to be rational and risk neutral, and this is common knowledge.

2. Preliminary

The concept of Coalitin-Proof Nash Equilibrium(*CPNE*) was first introduced by Bernheim[8], which stated that a profile of strategies is *CPNE* if no coalition can find another profile strategy to chieve better payoff. Keiding[9] considered the representation problem for *CPNE* by introducing an efficiency function to find euqilibrium. Let *N={1,...,n}* be a set of players, a coalition is a nonempty subset of *N*, the number of all coalitions is 2^N, and we denote by 2^N the set of all coalition and denotes S^C the set of strategies of coalition *C*.

According to Bernheim[8], Keiding[9] and Nisan [10], there exist following basic definitions and theorem:

Definition 1 Given the n-player normal-form game $G = \{S_1, \dots S_n; u_1, \dots, u_n\}$, the strategies $\sigma^N = \{s_1, \dots, s_n\}, \sigma^N \in S$ and let $C \in 2^N$, then $\tau^C \in S^C$ is an improvement of C upon σ^N *if* $u_i(\tau^C, \sigma^{N\setminus C}) \geq u_i(\sigma^N)$, for all $i \in C$.

Definition 2 Given the n-player normal-form mgae $G = \{S_1, \dots S_n; u_1, \dots, u_n\}$, the strategies $\sigma^N = \{s_1, \dots, s_n\}, \sigma^N \in S$ is a Nash Equilibrium if no $i \in N$ has an improvement upon σ^N.

Definition 3 Given the n-player game $G = \{S_1, \dots S_n; u_1, \dots, u_n\}$, for each player i, $S_i = \{s_{i1}, \dots, s_{ik}\}$, Then a mixed strategy for player i is a probability distribution $p_i = \{p_{i1}, \dots, p_{ik}\}$, where $k = 1, \dots K, 0 \leq p_{ik} \leq 1, \sum_i^k p_{ik} = 1$.

Definition 4 Given the n-player normal-form game $G = \{S_1, \dots S_n; u_1, \dots, u_n\}$, the mixed strategies $\rho^* = \{\rho_1^*, \dots \rho_i^*, \dots, \rho_n^*\}$ is a Nash equilibrium if $v_i(\rho_i^*, \rho_{-i}^*) \geq v_i(\rho_i, \rho_{-i}^*), \forall \rho_i \in \sum_i$ for each player $i = 1,2, \dots, n$.

Definition 5 Given the n-player normal-form game $G = \{S_1, \dots S_n; u_1, \dots, u_n\}$, the strategies $\sigma^N = \{s_1, \dots, s_n\}, \sigma^N \in S$ and let $C \in 2^N$. An internally consistent improvement of C upon σ^N is defined as follow: if (a) τ^C is an improvement of C upon σ^N, (b) if $T \subset C$ *and* $|T|<|C|$ then T has no internally consistent improvement upon σ^N.

Definition 6 Given the n-player normal-form game $G = \{S_1, \dots S_n; u_1, \dots, u_n\}$, then $\sigma^N = \{s_1, \dots, s_n\}, \sigma^N \in S$ is a coalition-proof Nash equilibrium if no $C \in 2^N$ has a internally consistent improvement upon σ^N.

Theorem 1 In the *n*-player game $G = \{S_1, \dots, S_n; u_1, \dots, u_n\}$, if *n* is finite and S_i is finite for every *i*, then there exist at least one Nash equilibrium, possibly involving mixed strategies.

3. Game Analysis of Coalition-Proof Consensus in Blockchain System

Without loss of generality, there exists a 3-players game among all players joining consensus blockchain, we can represent the Normal form of 3-players complete inofrmation static game may as follows:

(1) Player set: defined as $N=\{1,2,3\}$,here *1* means the first player, *2* means the second player, and *3* means the third player.

(2) Strategy set : defined as $s_1=\{honesty,coalition\}, s_2=\{honesty,coalition\}, s_3=\{honesty,coalition\}$.

(3) Payoff function : defined as $u_1(s_{1j},s_{2j},s_{3j})$, $u_2(s_{1j},s_{2j},s_{3j})$, $u_3(s_{1j},s_{2j},s_{3j})$, each represents the payoff of player respectively, and they can be represented as follows:

$$u_1(s_{11},s_{21},s_{31})=0,\ u_1(s_{11},s_{22},s_{31})=0,\ u_1(s_{12},s_{21},s_{31})=-b,\ u_1(s_{12},s_{22},s_{31})=-b$$
$$u_1(s_{11},s_{21},s_{32})=0,\ u_1(s_{11},s_{22},s_{32})=0,\ u_1(s_{12},s_{21},s_{32})=c,\ u_1(s_{12},s_{22},s_{32})=c-f$$
$$u_2(s_{11},s_{21},s_{31})=0,\ u_2(s_{11},s_{22},s_{31})=-b,\ u_2(s_{12},s_{21},s_{31})=0,\ u_2(s_{12},s_{22},s_{31})=-b$$
$$u_2(s_{11},s_{21},s_{32})=0,\ u_2(s_{11},s_{22},s_{32})=c,\ u_2(s_{12},s_{21},s_{32})=0,\ u_2(s_{12},s_{22},s_{32})=c-f$$
$$u_3(s_{11},s_{21},s_{31})=d-a,\ u_3(s_{11},s_{22},s_{31})=-a,\ u_3(s_{12},s_{21},s_{31})=-a,\ u_3(s_{12},s_{22},s_{31})=-a$$
$$u_3(s_{11},s_{21},s_{32})=a-e,\ u_3(s_{11},s_{22},s_{32})=a-e,\ u_3(s_{12},s_{21},s_{32})=a-e,\ u_3(s_{12},s_{22},s_{32})=a-f$$

Here *a* means the loss of the third player selecting honesty strategy, *b* means the penalty to the other player because of their coalition strategy being found but not causing consensuns failure, *c* means the additional payoff of the third player selecting coalition strategy, *d* means the incentive of the third player for his normal service, *e* means the credibility loss of the third player by selecting coalition and without causing consensus failure, *f* means the penalty to all players for the first and second player coalition and the third player not joining coalition thus causing consensus failure. The game of all players can be denoted in the payoff matrix in Table 1.

Table 1. Analysis of Coalition-Proof Nash equilibrium

		Player3			
		honesty		coalition	
		Player2		Player2	
		honesty	coalition	honesty	coalition
Player1	honesty	0, 0, d-a	0, -b, -a	0, 0, a-e	0, c,a-e
	coalition	-b, 0, -a	-b, -b, -a	c, 0, a-e	c-f,c -f, a-f

In order to obtain the solution of Nash equilibrium of this three-players game, two situations can be considered :

(1) Given $c>f$, $a>f$, $e<f$ and $d+e < 2a$, there exists only one pure strategy Nash equilibrium in this game (coalition, coalition, coalition). Because of the payoff conflicting between the third player and other two players, (coalition, coalition, coalition) is not a self-enforcing strategies profile. Suppose the players select the (coalition, honesty,coalition) or (honesty, coalition, coalition) strategies profile, due to $c>c-f$, player1 or player2 has incentive to deviate from (coalition, coalition, coalition) strategies profile, so (coalition, coalition, coalition) is not a coalition-proof Nash equilibrium.

(2) Given $c>f$, $a<f<2a$, $e<f$ and $d+e>=2a$, there exist two pure strategy Nash equilibrium as (honesty, honesty, honest) and (coalition, coalition, coalition). We have proved that the strategy profile (coalition, coalition, coalition) is not a coalition-proof Nash equilibrium, now, we will proof the

strategies profile (honesty, honesty, honest) is a coalition-proof Nash equilibrium under the assumptions mentioned above.

The equilibrium shows that if anyone of the players wants to deviate from the equilibrium, the payoff of the player will descrease. Suppose that if the player1 or the player2 changes his strategy unilaternally, the payoff of the player will descrease from 0 to *-b*, and if both of the two players change their strategies profile from (honesty, honesty) to (coalition, coalition), the payoffes of the two players will decrease from 0 to *-b*. As we assume that all players are rational and risk neutral, anyone has incentive to derivate from the equilibrium, and there exists no enforcing rules to force the players to obey the rules.

There are three players and each player has only two strategies, all of them are finite. According to theorem 1, there exists a Nash equilibrium of mixed strategy. Assume player1 selects coalition strategy in probability α, and honesty strategy in probability $1-\alpha$. The player2 selects coalition strategy in probability β, and honesty strategy in probability $1-\beta$. The player3 selects coalition strategy in probability γ, and honesty strategy in probability $1-\gamma$. Then, the expected payoff function of the player1 can be represented as follows:

$$\pi_1 = (1-\alpha)[(1-\beta)(1-\gamma)0 + \beta(1-\gamma)0 + (1-\beta)\gamma 0 + \beta\gamma 0] + \alpha[-(1-\beta)(1-\gamma)b - \beta(1-\gamma)b + (1-\beta)\gamma c + \beta\gamma(c-f)]$$

The first order partical derivative of the expected payoff function with respect to independent variable α is:

$$\frac{\partial \pi_1}{\partial \alpha} = (1-\beta)(1-\gamma)(-b) + \beta(1-\gamma)(-b) + (1-\beta)\gamma c + \beta\gamma(c-f) = \gamma b - b + \gamma c + \beta\gamma f = 0$$

We can calculate the expected payoff function of the player2 and the player3 as the same way:

$$\pi_2 = (1-\beta)[(1-\alpha)(1-\gamma)0 + \alpha(1-\gamma)0 + (1-\alpha)\gamma 0 + \alpha\gamma 0] + \beta[-(1-\alpha)(1-\gamma)b - \alpha(1-\gamma)b + (1-\alpha)\gamma c + \alpha\gamma(c-f)]$$

$$\pi_3 = (1-\gamma)[(1-\alpha)(1-\beta)(d-a) + \alpha(1-\beta)(-a) + (1-\alpha)\beta(-a) + \alpha\beta(-b)] + \gamma[(1-\alpha)(1-\beta)(a-e) - \alpha(1-\beta)(a-e) + (1-\alpha)\beta(a-e) + \alpha\beta(a-f)]$$

We can calculate the first order partical derivative of the expected payoff function with respect to independent variable β and γ as follows:

$$\frac{\partial \pi_2}{\partial \beta} = (1-\alpha)(1-\gamma)(-b) + \alpha(1-\gamma)(-b) + (1-\alpha)\gamma c + \alpha\gamma(c-f) = \gamma b - b + \gamma c + \alpha\gamma f = 0$$

$$\frac{\partial \pi_3}{\partial \gamma} = -[(1-\alpha)(1-\beta)(d-a) + \alpha(1-\beta)(-a) + (1-\alpha)\beta(-a) + \alpha\beta(-a)] + [(1-\alpha)(1-\beta)(a-e) + \alpha(1-\beta)(a-e) + (1-\alpha)\beta(a-e) + \alpha\beta(a-f)] = 0$$

Let 2a-d-e=0,the mixed strategies Nash equilibrium can be obtained as:

$$\alpha^* = 2d/(d+f-e) = 2(2a-e)/(2a+f)$$

$$\beta^* = 2d/(d+f-e) = 2(2a-e)/(2a+f)$$

$$\gamma^* = b(d+f-e)/((b+c)(d+f-e)-2df) = b/(b+c-a^*f) = b/(b+c-\beta^*f)$$

It means when the player3 selects coalition strategy in probability $b(d+f-e)/((b+c)(d+f-e)-2df)$, the player1 and player2 will select coalition strategy in probability $2(2a-e)/(a2+f)$. It showes that the probability of the player1 and player2 choosing coalition strategy is mainly related to the factor *e* which is the credibility loss of the player3 not selecting honesty, and also related to the factor *f* which if the penalty to player1 and player2 for their coalition strategies. The larger *e* and *f* is, the smaller the probability that player1 and player2 select coalition strategy is. If the credibility loss *e* and the penalty *f* are increased, the player3 will increase the probability of selecting honesty strategy, and the payoff will exceed the benefit for player1 and player2 once their coalition causing consensus failure.

It also showes that the probability of player3 selecting coalition strategy is mainly related to the factor *c* which is the additional benefits of other players selecting coalition strategies, the factor *f* which if

the penalty to player1 and player2 for their coalition strategies, and also related to the probability of player1 and player2 selecting coalition strategy. The larger *c* is, the smaller the probability that player3 selecting coalition strategy is. The larger *f* is, the largere the probability the player3 selecting coalition strategy is. Because the larger the *c* is, the larger the probability of player1 and player2 selecting coalition strategy is, and this operation can increase the probability of consensus failure, and hence decrease the payoff of player3. The larger the *f* is, the smaller the probability of player1 and player2 selecting coalition strategies is, and this can decrease the probability of consensus failure in blockchain system.

4. Conclusion

This paper discusses the consensus of blockchain under the view of game theory. The aim of this article is to design a rational mechanism that can avoid coalition of all players and also obtain the outcome of coalition-proof Nash equilibrium. According to the analysis result mentioned above,when we design a mechanism that can provide the efficient consensus of blockchain, we should enlarge the penalty to players for their coalition operation, and enlarge the credibility loss of players for not conducting honesty operation to decrease the probability of other players choosing coalition strategies, and ensure that the sum value of the incentive and the credibility loss to the player is larger than or equal to two times value of the cost of the player selecting honesty to achieve a coalition-proof nash equilibrium in blockchain system.

References

[1] Pease M, Shostak R, Lamport L: Reaching Agreement in the Presence of Fault. Journal of the ACM, Vol.27(1980)No.2, p.228-234.

[2] Lamport L, Shostak R, Pease M: The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, Vol.4(2016)No.3, p.382-401.

[3] Fischer M: The Consensus Problem in Unreliable Distributed Systems[C]. International Conference on Fundamentals of Computation Theory(Sweden,1983), p.127-140.

[4] Chandra T, Toreg S: Unreliable Failure Detectors for Reliable Distributed Systems. Jounal of the ACM, 1996,Vol.43(1996)No.2, p.225-267.

[5] Information on http://bitcoins.info/bitcoin.pdf,.

[6] Information on https://bravenewcoin. com/asserts/Uploads/TransactionsAsProofOfStake10.pdf

[7] Castro M: Practical Byzantine Fault Torlerance and Proactive Recovery. ACM Transactions on Computer Systems, Vol.20(1999)No.4, p.398-461.

[8] Bernheim B, Peleg B, Whinston M.D: Coalition-proof equilibria. Journal of economic theory, Vol.42(1987), p.1-12.

[9] Keiding H, Peleg B. Representation of effectivity functions in coalition proof Nash equilibrium: a complete characterization(Copenhagen University, Denmark 1997).

[10] Nisan,N. Algorithmic game theory(Cambridge University, England 2007).