Study on Consensus of Private Blockchain based on Game Theory

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

Private Blockchain is a kind of distributed ledger system with characteristics of centralization, non-tempering, security and crediblity, and consensus algorithms play an important role in the private blockchain systems. In addition to considering technologies and mathematics to ensure consensus algoritm efficiency in private blockchain system, many other factors need also be considered, such as the behaviors of all players. This paper diccusses about the consensus of private blockchain under the view of game theory, it provides a complete information static game theory analysis among all players in a private blockchain system, and gives the mixed strategy Nash equilibrium. Some suggestions are also proposed to ensure consensus can be effectively implemented in private blockchain system.

Keywords

Private Blockchain, Game Theory, Mixed Strategy Nash Equilibrium, Consensus.

1. Introduction

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.

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 private blockchain, and we need to introduce new mechanism to guarantee the consensus efficiency of private blockchain systems. As we know, there are many factors which influence on the consensus implementation in the private blockchain systems, and the participant‘s behaviors of blockchain is one of the important factors. On the one hand, the level of technology and management of the participants directly determine the consensus efficiency. On the other hand, the

private blockchain systems involves different types of participants, these players are rational and self-interested, and have no malicious intention. 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 private blockchain systems, causing the failure of consensus in private blockchain systems. Because the participants have different responsibilities in private 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 private 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

Game theory is the formal study of decision-making in which economic agents make strategic interactions to produce outcomes to maximize their own utility under certain constraints. According to Gibbons [8], Zhang[9] and Nisan[10], there exist following basic concepts and theorem:

Definition 1 Given the n-player game $G=\{S_1,...,S_n;u_1,...,u_n\}$, the strategies $\{S_1^*,\dots,S_n^*\}$ is a Nash equilibrium if, for each player i, si* is player i's best response to the strategies of the n-1 other players $\{S_1^*,\dots,S_{i-1}^*,S_{i+1}^*,\dots,S_n^*\}$, $u_i(s_i^*,s_{-i}^*)\geq u_i(s_i,s_{-i}^*),\forall s_i\in S_i,\forall i$ for every feasible strategy si in Si, that is, si* solves $\max_{s_i\in S_i} u_i(s_1^*,\dots,s_{i-1}^*,s_i^*,s_{i+1}^*,\dots,s_n^*), i=1,2,\dots,n.$

Definition 2 Given the n-player game $G=\{S_1,...,S_n;u_1,...,u_n\}$, 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 3 Given the n-player game $G=\{S_1,\dots S_n;u_1,\dots,u_n\}$, the mixed strategies $p^*=\{p_1^*,\dots,p_i^*,\dots,p_n^*\}$ is a Nash equilibrium if $v_i(p_i^*,p_{-i}^*)\geq v_i(p_i,p_{-i}^*),\forall p_i\in\sum_i$ for each player i=1,2,...,n.

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

3. Game Analysis of Consensus Implementation in Private Blockchain

Without loss of generality, there exists a 3-players game among all players joining private 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}*, each of them represents a player in blockchain system, here 1 means the player1, 2 means the player2, 3 means the regulator.

(2)Strategy set: defined as s_1*={honesty,coalition}*, s_2*={honesty,coalition}*, s_3*={supervise, no-supervise}*. Strategy s_{11}*= honesty*, s_{12}*=coalition*, s_{21}*= honesty*, s_{22}*= coalition*, s_{31}*= supervise*, s_{32}*= no-supervise*.

(3) Payoff function: defined as $u_1(s_{1j},s_{2j},s_{3j})$, $u_2(s_{1j}, s_{2j},s_{3j})$ and $u_3(s_{1j},s_{2j},s_{3j})$ as the payoff of player1, player2 and the regulator respectively, which can be expressed as follows:

$$u_1(s_{11},s_{21},s_{31})= 0,\ u_1(s_{11},s_{22},s_{31})= 0,\ u_1(s_{12},s_{21},s_{31})= -a,\ u_1(s_{12},s_{22},s_{31})= -a$$

$$u_1(s_{11},s_{21},s_{32})= 0,\ u_1(s_{11},s_{22},s_{32})= 0,\ u_1(s_{12},s_{21},s_{32})= b,\ u_1(s_{12},s_{22},s_{32})= b-c$$

$$u_2(s_{11},s_{21},s_{31})= 0,\ u_2(s_{11},s_{22},s_{31})= -a,\ u_2(s_{12},s_{21},s_{31})= 0,\ u_2(s_{12},s_{22},s_{31})= -a$$

$$u_2(s_{11},s_{21},s_{32})= 0,\ u_2(s_{11},s_{22},s_{32})= b-c,\ u_2(s_{12},s_{21},s_{32})= 0,\ u_2(s_{12},s_{22},s_{32})= b-c$$

$$u_3(s_{11},s_{21},s_{31})= e-d,\ u_3(s_{11},s_{22},s_{31})= -d,\ u_3(s_{12},s_{21},s_{31})= -d,\ u_3(s_{12},s_{22},s_{31})= -d$$

$$u_3(s_{11},s_{21},s_{32})= d-f,\ u_3(s_{11},s_{22},s_{32})= d-f,\ u_3(s_{12},s_{21},s_{32})= d-f,\ u_3(s_{12},s_{22},s_{32})= d-c-f$$

Where *a* denotes the penalty to the player1 because of the negative operation coalition, *b* denotes the additional benefits of player1 providing coalition service, *c* denotes the credibility loss of all caused by consensus efficiency reduction, *d* denotes the supervice cost of the regulator, *e* denotes the incentive given to the regulator for providing supervice service, *f* denotes the penalty to the regulator for not providing supervice serivce. In normal situation, $d<f<e$, otherwise, a rational player will not providing honesty strategy and choose coalition strategy in consensus implemnetation in private blockchain, thus causing consensus failure in private blockchain. This game can be represented in the payoff matrix in Table 1:

Table 1. Analysis of Nash equilibrium

		The regulator			
		Supervice		No-supervice	
		Player2		Player2	
		honesty	coalition	honesty	coalition
Player1	honesty	0, 0, e-d	0, -a, -d	0, 0, d-f	0, b-c,d-f
	coalition	-a, 0, -d	-a, -a, -d	b-c, 0, d-f	b-c,b -c, d-f-c

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 regulator selects no-supervice strategy in probability γ, and supervice strategy in probability $1-\gamma$. Then, the expected payoff function of all players can be represented as follows:

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

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

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

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

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

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

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

Let $2d-c-f=0$ *and* $\alpha=\beta$, we can obtain the mixed strategies Nash equilibrium as:

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

As mentioned above, many factors are related to the Nash equilibrium of game among all players in private blockchain. In order to assure consensus implemntation, it is necessary to design an effective incentive and punishment mechanism to ensure that all players perform positive behaviors. As we have assumed $\alpha=\beta$, the probability of player1 and player2 choosing coalition strategy is mainly related to the factor *c*, the credibility loss of all caused by consensus failure, the factor *f*, the penalty to the regulator for not supervicing consensus process, and the factor *e*, the incentive given to the regulator for providing supervice service. In general, *d* is fixed, the larger *c*, *e* and *f* is, the smaller the probability that players choose coalition strategy is. When the penalty and credibility loss increase, the regulator will increase the probability of supervice to ensure consensus efficiency, and the payoff will exceed the benefit for players once their negative behaviors which lead to the consensus failure are exposed.

The probability of the regulator choosing no-supervice strategy is mainly related to the factor *c*, the credibility loss of all caused by consensus failure, and the factor *a*, the penalty to other players because of their negative operation, and is related to factor *b*, the additional benefits of other players providing coalition strategies. In general, *b* is fixed, the larger *c* and *a* is, the smaller the probability of the regulator choosing no-supervice strategy is. The reason is that the larger the *c* is, the smaller the probability that other players choose coalition strategy is, and this increases the probability of consensus sucess and decreases the probability of the regulator choosing supervice strategy.

4. Conclusion

This paper discusses the consensus of private blockchain under the view of game theory. The aim of this article is to design a rational mechanism that can avoid coalition of two players and also obtain the outcome of mixed strategy Nash equilibrium. In fact, in 3-players complete information static game, the coalition can only occurs between player1 and player 2. According to the analysis result mentioned above,when we design a mechanism that can provide the efficient consensus of private blockchain, we should enlarge the penalty to players for their coalition operation, and enlarge the credibility loss of trusted third party for not conducting supervice to decrease the probability of player 1 and player 2 choosing coalition strategies, that is both players choose honesty strategy and the trusted third party choose supervice strategy to achieve efficient consensus in private blockchain.

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] Gibbons, R: A primer in game theory(Prentice Hall,1992).

[9] Zhang, W: Game theory and information economics(Shanghai People's Publishing House,China 2002).

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