Consensus en Présence de Participants Rationnels et Byzantins

Yackolley Amoussou-Guenou, Bruno Biais, Maria Potop-Butucaru, Sara Tucci-Piergiovanni

Consensus en Présence de Participants Rationnels et Byzantins †

Yackolley Amoussou-Guenou[1,2] et Bruno Biais[3] et Maria Potop-Butucaru[2] et Sara Tucci-Piergiovanni[1]

[1]*CEA LIST, PC 174, 91191 Gif-sur-Yvette, France*
[2]*Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*
[3]*HEC Paris, 1 Rue de la Libération, 78350 Jouy-en-Josas, France*

Nous étudions les comportements des participants d'un protocole de consensus lorsqu'ils présentent des comportements rationnels ou Byzantins. Nous nous inspirons des protocoles de blockchains tolérantes aux fautes Byzantines (comme Tendermint). Dans ces protocoles, les participants proposent des blocs et s'échangent des messages. Un bloc est accepté si une majorité de participants envoie le message correspondant à ce bloc (un vote), et les votants sont récompensés. Dans ce travail, nous étudions les conditions sous lesquelles ce protocole satisfait les deux propriétés suivantes : la *terminaison* (le système converge vers une décision) et la *validité* (toute décision est valide), quand certains participants sont rationnels et les autres Byzantins. Nous supposons que les participants Byzantins ont le comportement infligeant le plus de dégâts au système, tandis que les stratégies des participants rationnels forment un équilibre Bayésien parfait. Nous considérons les paramètres suivant : (i) le nombre de votes nécessaires, ν, pour qu'un bloc soit considéré comme accepté, et (ii) le nombre de participants Byzantins, noté f, dans le système. Nous obtenons les résultats suivants : Quand $f \geq \nu$, les blocs invalides sont acceptés, et donc la *validité* ne peut être garantie ; Quand $f < \nu$, il existe un équilibre où la *validité* et la *terminaison* sont toutes deux satisfaites, par contre, il existe d'autres équilibres où la *terminaison*, et dans quelques cas la *validité*, ne sont pas satisfaites. Cela nous permet de conclure à l'existence de problèmes de coordination dans les protocoles étudiés.

Mots-clefs : Blockchain; Comité; Théorie des jeux; Équilibre de Nash; Terminaison; Validité

1 Introduction

Résoudre le consensus en présence de Byzantins est l'un des problèmes les plus étudiés en algorithmique distribuée. Les blockchains ont pourtant réussi à augmenter l'attrait de la recherche sur le consensus en apportant de nouvelles problématiques. Là où les analyses "classiques" sur le consensus s'intéressent généralement au cas où les processus sont corrects (qui suivent la spécification) et Byzantins (qui se comporte arbitrairement) ; dans les systèmes blockchains, de par les récompenses distribuées, un autre type de processus est à étudier : les processus *rationnels*. Ces derniers prennent des actions afin de maximiser leurs gains. Même si l'objectif des processus rationnels n'est pas de nuire au système mais d'en profiter, la maximisation de leur gain peut entraîner un effondrement du système. Il faut donc trouver des protocoles dans lesquels les incitations des processus rationnels ne nuisent pas au système.

Quelques travaux ayant analysé le consensus avec des processus rationnels existent, mais restent limités. [GKTZ12] par exemple considère uniquement des processus rationnels ou corrects. Bien qu'ils prouvent des bornes afin d'atteindre le consensus avec les incitations des rationnels, les Byzantins ne sont pas pris en compte dans leurs analyses. [LT06] étudie un environnement composé de processus Byzantins et rationnels pour le problème du calcul multipartite (*multi-party computation* en anglais) et du secret réparti (*secret sharing* en anglais). [LT06] propose un protocole où les incitations des processus rationnels sont alignées avec le protocole proposé. L'étude ne prend par contre pas dans son analyse le coût des actions des processus. Contrairement à notre étude, dans les analyses précédentes, ni les récompenses ni les coûts ne sont pris en

†Une version étendue de cet article [ABPT20] a été acceptée à AAMAS 2020.

compte dans les analyses, et s'il est atteint seul la valeur du consensus importe. Notre étude porte sur un modèle plus réaliste où les actions des processus (envois de messages, vérifications de messages) ont des coûts, et dans certains cas les processus peuvent être récompensés.

Dans cet article, nous étudions le comportement des processus rationnels, ainsi que les limites du consensus en présence de processus rationnels et Byzantins. Nous montrons qu'il existe des situations où le consensus peut être garanti, mais cette situation n'est pas unique et des problèmes de coordination peuvent arriver.

2 Problème du Consensus en Présence de Participants Rationnel et Byzantins

2.1 Modèle et Problème étudié

Modèle du Système Nous considérons un système composé d'un ensemble fini $\Pi = \{1, \ldots, n\}$ de processus ou joueurs séquentiels et synchrones. Chaque processus ou joueur est désigné par son indice i, et nous supposons que chaque joueur connaît son indice ainsi que le nombre total de processus et joueurs $|\Pi| = n$. Dans la suite, nous considérons les termes joueurs et processus comme ayant la même signification.

[AAC+05] définit le modèle BAR (pour Byzantins-Altruistes-Rationnels) où chaque processus dans le système est soit Byzantin, altruiste (correct) ou rationnel. Dans cet article, nous considérons un système avec un mélange de joueurs rationnels (qui visent à maximiser leur propre gain) et de processus Byzantins. Comme dans les travaux [AAC+05], nous faisons l'hypothèse supplémentaire que les Byzantins ont comme objectif de minimiser les gains des joueurs rationnels. Le terme *adversaire* serait plus convenable, mais nous utilisons le nom Byzantin comme dans [AAC+05].

Les processus évoluent en ronde, et chaque ronde est subdivisée en trois étapes séquentielles (i) Envoi de message, (ii) Réception des messages, et (iii) Calcul. Après la fin de ses trois phases, la ronde se termine et la suivante commence. Les processus communiquent par envoi de message au travers d'un réseau fiable et synchrone. Les messages sont signés, et les signatures ne peuvent être falsifiées. Tout message envoyé en début de ronde est reçu par tous les autres processus avant la fin de l'étape de réception de cette ronde. De plus, nous demandons que tout message reçu par un processus rationnel avant la fin de sa ronde soit aussi reçu par tous les autres processus rationnels lors de la même ronde.

Problème Un protocole (algorithme) résout le problème du consensus quand les propriétés suivantes sont satisfaites : (i) *Terminaison*. Tous les processus non-Byzantins décident ultimement une valeur ; (ii) *Accord*. Si un processus non-Byzantin décide une valeur v, et un autre processus non-Byzantin décide une valeur v', alors $v = v'$; (iii) *Validité*. Une valeur décidée par un processus non-Byzantin est valide par rapport à un prédicat prédéfini. Dans cet article, nous utilisons les termes valeurs et blocs de manière interchangeable.

Dans ce travail, nous établissons les conditions nécessaires pour satisfaire les propriétés du consensus dans un système avec des participants rationnels et Byzantins. Notons que notre modèle, en particulier l'hypothèse de réception de tous les messages avant la fin de chaque ronde, nous permet de garantir la propriété d'*Accord*. Dans la suite, nous calculons différentes situations stables (les équilibres) de notre système, et nous les analysons par rapport aux propriétés de *Terminaison* et de *Validité*.

2.2 Définition du Jeu

Rappelons que $\Pi = \{1, \ldots, n\}$. Nous considérons que dans Π il y a un nombre $f \geq 1$ de byzantins, et les $n - f$ restant sont rationnels. Chaque joueur connaît sa position (indice) ainsi que son type (Byzantin ou rationnel), mais ne connaît pas à l'avance le type des autres joueurs.

Au début de chaque ronde, un joueur est désigné comme proposeur. Le proposeur est désigné selon la méthode du round-robin. A la ronde 1, le joueur 1 est le proposeur, $\forall i \leq n$, le joueur i est le proposeur de la ronde i. A la ronde $n+1$, le joueur 1 est le proposeur, puis le joueur 2 à la ronde $n+2$, etc.

Actions Nous utilisons un vocabulaire venu des blockchains. Un proposeur a deux actions : (i) envoyer un bloc valide ou (ii) envoyer un bloc invalide. Le proposeur envoie donc de toute façon un bloc, et cet envoi est à destination de tous les joueurs.

Une fois le bloc du proposeur reçu, un joueur décide dans cet ordre :

1. De vérifier la validité du bloc ou non. Si un joueur décide de vérifier, il sait si le bloc proposé est valide ou non. Si le joueur ne vérifie pas, alors il n'a pas d'informations sur la validité.
2. D'envoyer ou non un vote pour le bloc proposé.

Soit $\nu \geq 1$. Si un bloc reçoit des votes d'au moins ν joueurs différents, alors ce bloc est considéré comme produit. ν est le seuil de production d'un bloc. Nous supposons $n - f \geq \nu$ afin que les rationnels puissent sans l'aide des Byzantins produire un bloc. Si le bloc ne reçoit pas suffisamment de votes, la ronde se termine et la suivante commence.

Informations Chaque joueur a un ensemble d'informations qui contient toutes les informations collectées. Par exemple cet ensemble contient le numéro de la ronde, le type du joueur, les messages reçus, l'information de validité des blocs, etc.

Stratégies Une stratégie d'un joueur est une fonction de son ensemble d'informations vers ses actions.

Gains et coûts Inspiré des blockchains, si un bloc est produit, alors tous les joueurs ayant envoyé un message ont une récompense $R > 0$. Si le bloc produit est invalide, alors tous les joueurs rationnels paient un coût de κ. Si un joueur rationnel fait une vérification de validité d'un bloc, il paie un coût de vérification $c_{\text{vérif}} > 0$ et s'il envoie un vote, il paie un coût d'envoi $c_{\text{envoi}} > 0$.

Nous faisons l'hypothèse d'étude suivante : $\kappa > R > c_{\text{vérif}} > c_{\text{envoi}}$, car la production de blocs invalides a un impact sur tout l'écosystème d'une blockchain, et la récompense doit être plus grande que les coûts de vérifications et d'envois.

Un joueur rationnel cherche à maximiser son gain et réduire le plus possible ses coûts. Un joueur Byzantin lui a comme objectif de minimiser le gain d'un joueur rationnel. Un joueur Byzantin n'est pas sensible aux coûts présentés ci-dessus. Pour cela, nous supposons qu'un joueur Byzantin propose toujours un bloc invalide, puis vérifie toujours la validité d'un bloc reçu, et vote pour un bloc uniquement si ce dernier est invalide. Cela est le comportement optimal pour un joueur Byzantin.

Équilibre Le jeu considéré étant un jeu dynamique à informations incomplètes, le concept de solution le plus adéquat est la notion d'équilibre Bayésien parfait [FT91].

Un équilibre Bayésien parfait est une situation dans laquelle chaque joueur i) choisit ses actions afin de maximiser son gain, ii) anticipe rationnellement les actions des autres joueurs, et iii) fait rationnellement des inférences par rapport aux observations, en utilisant les prédictions à propos des stratégies des autres joueurs, respectant tant que possible la formule de Bayes.

Une situation satisfaisant les deux premiers points uniquement est un équilibre de Nash pur.

Notons que si tous les joueurs choisissent de toujours vérifier la validité des blocs proposés, et n'envoyer de vote que si le bloc proposé est valide, alors la validité et la terminaison seraient garanties. Malheureusement, cette situation n'est pas un équilibre. Dans cette situation, chaque joueur a une incitation à ne pas vérifier la validité des blocs, laissant aux autres le soin d'effectuer cette tâche.

3 Résultats

Proposition 1 *Soit f une variable aléatoire telle que $f < \nu$ et $n - f \geq \nu$ alors il existe un équilibre où la validité est garantie, mais la terminaison n'est jamais satisfaite.*

Dans l'équilibre ci-dessus, aucun joueur rationnel n'envoie jamais de vote ni ne vérifie. Dans ce cas, aucun rationnel n'a d'incitation à envoyer de vote car un seul vote ne permettrait pas de produire un bloc valide, et au pire cela pourrait plutôt aider à produire un bloc invalide (si $f = \nu - 1$).

Proposition 2 *Soit f une variable aléatoire telle que $n - f \geq \nu + 1$ et $f \in \{1, \ldots, n - \nu - 1\}$, alors il existe un équilibre Bayésien parfait où la terminaison est satisfaite, mais la validité ne peut pas être garantie.*

Dans l'équilibre de la Proposition 2, un proposeur rationnel propose un bloc valide, mais un Byzantin propose un bloc invalide. Tous les rationnels votent pour gagner la récompense de la production du bloc. Aucun rationnel n'a d'incitation à vérifier le bloc proposé, car il sera produit à la fin de la ronde dans tous les cas (que le bloc soit valide ou non).

Proposition 3 *Soit f une constante connue de tous. Soient t la ronde en cours, et T la première ronde où il y a un bloc produit. Soit la fonction ϕ définie comme suit : $\phi(f) = 1$ et $\forall t < f, \phi(t) = \left(1 + \frac{f-(t-1)}{n-t+1}\phi(t+1)\right)$, et soit i_B l'indice le plus grand d'un joueur Byzantin [‡]. Si $f < \nu$ et $n - f > \nu$, si de plus le coût de production d'un bloc invalide est grand, i.e.,*

$$\kappa > \alpha(t)c_{vérif} - \beta(t)c_{envoi}, \forall t < f,$$

avec

$$\alpha(t) = \frac{(n-t+1)\phi(t) - (f-t+1)\Pr(i_B \geq n-\nu+f+2 | T \geq t)\phi(t+1)}{(f-t+1)\Pr(i_B < n-\nu+f+2 | T \geq t)}$$

et

$$\beta(t) = \frac{\Pr(i_B \geq n-\nu+f+2 | T \geq t)}{\Pr(i_B < n-\nu+f+2 | T \geq t)},$$

et si la récompense est suffisamment élevée, i.e., $R \geq \max\left[\frac{n}{n-f}c_{envoi}, c_{envoi} + \frac{n}{n-f}c_{vérif}\right]$, alors il existe un équilibre Bayésien parfait où les propriétés de terminaison et de validité sont toujours satisfaites.

Dans l'équilibre de la Proposition 3, un proposeur rationnel propose un bloc valide. Lors des f premières rondes, les joueurs rationnels entre les positions 1 et $n-\nu+f+1$ vérifient la validité des blocs et n'envoient de votes que si le bloc est valide, et les autres joueurs rationnels envoient toujours un vote sans faire de vérifications. De cette manière, tout bloc valide proposé est produit, mais tout bloc invalide est rejeté car il n'y aura qu'au plus $\nu - 1$ votes pour les blocs invalides. Si la ronde $f+1$ est atteinte les joueurs rationnels votent sans faire de vérifications. On sait dans ce cas que les f premiers proposeurs étaient Byzantins ; ne restant plus de Byzantins, le proposeur de la ronde $f+1$ sera rationnel et le bloc proposé valide.

Notons que dans ce dernier équilibre, et contrairement aux précédents, les joueurs connaissent la valeur exacte de f ; le nombre de Byzantin est connu de tous.

4 Conclusions et Perspectives

Nous avons modélisé les interactions dans les blockchains utilisant un protocole de consensus tolérant aux fautes Byzantines comme un jeu de coordination entre des processus rationnels et Byzantins. Nous avons établi précisément les conditions sur le nombre de Byzantins et le nombre nécessaire de vote sous lesquelles les propriétés de validité et de terminaison du consensus sont garanties. Dans les travaux futurs, nous nous intéresserons à étendre le modèle et notre analyse pour prendre en compte des stratégies plus générales.

Références

[AAC+05] Aiyer, Amitanand S., Lorenzo Alvisi, Allen Clement, Michael Dahlin, Jean-Philippe Martin et Carl Porth: *BAR fault tolerance for cooperative services*. Dans *Proceedings of the 20th ACM Symposium on Operating Systems Principles 2005, SOSP 2005, Brighton, UK, October 23-26, 2005*, pages 45–58. ACM, 2005.

[ABPT20] Amoussou-Guenou, Yackolley, Bruno Biais, Maria Potop-Butucaru et Sara Tucci Piergiovanni: *Rational vs Byzantine Players in Consensus-based Blockchains*. Dans *Proceedings of the 19th International Conference on Autonomous Agents and Multiagent Systems, AAMAS '20, Auckland, New Zealand, May 9-13, 2020*, pages 43–51. International Foundation for Autonomous Agents and Multiagent Systems, 2020.

[FT91] Fudenberg, Drew et Jean Tirole: *Perfect Bayesian equilibrium and sequential equilibrium*. Journal of Economic Theory, 53(2) :236 – 260, 1991, ISSN 0022-0531.

[GKTZ12] Groce, Adam, Jonathan Katz, Aishwarya Thiruvengadam et Vassilis Zikas: *Byzantine Agreement with a Rational Adversary*. Dans *Automata, Languages, and Programming - 39th International Colloquium, ICALP 2012, Warwick, UK, July 9-13, 2012, Proceedings, Part II*, pages 561–572, 2012.

[LT06] Lysyanskaya, Anna et Nikos Triandopoulos: *Rationality and Adversarial Behavior in Multi-party Computation*. Dans *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, pages 180–197, 2006.

‡. Formellent, $i_B = \max\{i : i \in \Pi \text{ et } i \text{ est Byzantin}\}$.