分散型オラクルの合意形成に対するピア予測法の潜在的有用性

A Potential Utility of Peer Prediction Method to Consensus Building on Decentralized Oracle Systems

伊東　謙介 *
Kensuke ITO

1 はじめに

Nakamoto（2008）によるビットコインが持つ新規性の 1 つは、悪意のあるノードが含まれ得る P2P システムが抱える合意形成に関する問題群（e.g., ビザンティン将軍問題）に対して、インセンティブ設計を通じた制御という新たなアプローチを提示した点である。具体的にはビットコインはコストを負ってシステムの検証と管理に貢献した者[1]に対する報酬を、その価値がシステム全体と連動するビットコインそのもので与えることにより、プレイヤーにとってシステムに悪影響を及ぼす行為が非合理的となるような制度を提案している[2]。このアプローチは、取扱情報を暗号通貨の移転からあるプログラムの実行に必要なトリガーの移転へと拡張することでより複雑な処理を P2P 環境で実現させるスマートコントラクト[3]用のプラットフォームにおいても継承されており、例えばその代表例である Buterin（2014）では固有のトークンである ether を報酬としている。

スマートコントラクトがより汎用的に機能するためには、管理がブロックチェーン内部で完結するビットコインとは異なり、トリガーとなる情報をブロックチェーンの外部から取得する必要がある。例えば将来の天気や株価に対する予測市場を実装する場合には、期限に達した時点で予測対象の結果を示す情報、つまり実際の天気や株価がどうなったかに関する情報の入力が求められるだろう。このようなスマートコントラクト用に外部から情報を入力する仕組みは、ブロックチェーンの文脈において「オラクル」と呼ばれている[4]。運用の利便性から多くの場合オラクルは中央集権型、すなわち上記の例では気象庁や証券取引所などの信頼出来る第三者機関（TTP: trusted third party）が提供する情報を直接使用するが、最近では TTP に依存せずネットワーク全体で入力情報の妥当性に関して合意形成を行う分散型オラクルの設計も少数ながら試みられている。本稿執筆時点では

* 東京大学大学院学際情報学府社会情報学コース博士課程
キーワード：分散型オラクル , ピア予測法 , ブロックチェーン , 合意形成 , メカニズムデザイン .

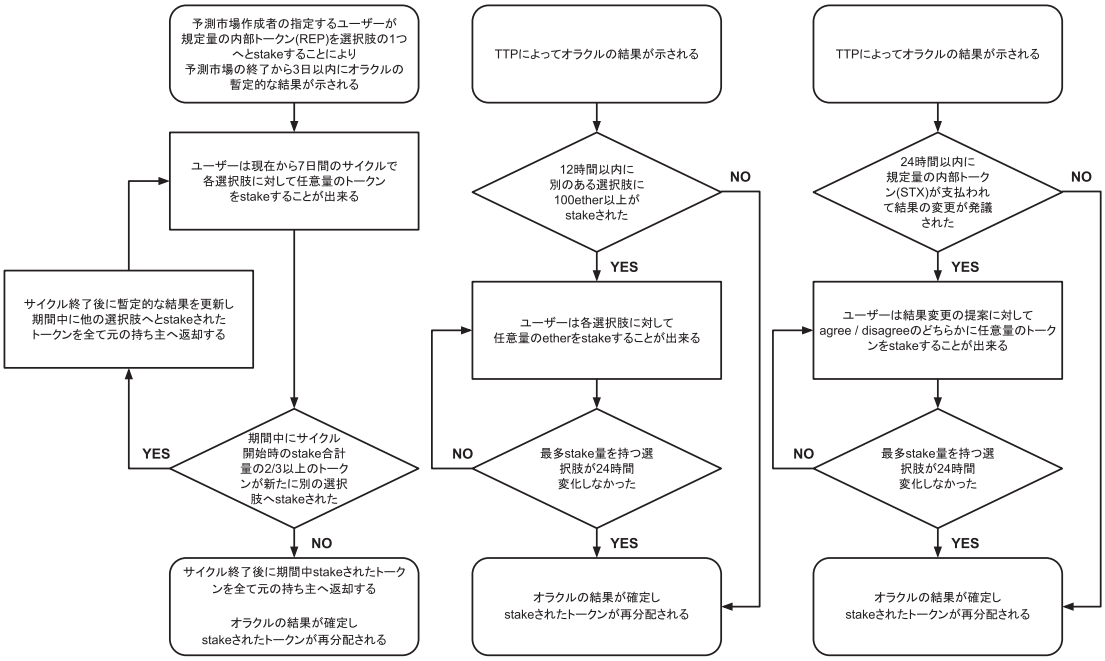
未だ分散型オラクルを備えた実用レベルのアプリケーションは公開されていないが、その実現はシステムが TTP に依存せずとも扱える情報の範囲を大幅に拡げるため重要な意義があるだろう。

しかしながら、分散型オラクルには単にトークン形式で報酬を与えるのみでは入力情報の妥当性に関して適切な検証を促せないという重要な課題が存在する。これは扱う情報の質の違いに起因している。暗号通貨の場合、合意形成を経てブロックチェーンに格納すべきは二重支払いの有無等の客観的かつ計算によって検証可能な情報だが、分散型オラクルにおけるそれは人間が主観的に時間をかけて検証する情報である[5]。主観的な情報に対する合意形成は、担当者が本当に適切な検証を行っているかを客観的に判断することが極めて難しい。例えば仮に一部の担当者が検証に必要な時間や労力を忌避してランダムに回答を返すような不誠実な行為を働いたとしても、その事実が短時間でシステム全体に認知されトークン価格が下落するかどうかは疑わしいだろう。以上の理由から、分散型オラクルでは担当者に適切な主観的検証を促す補完的なインセンティブ設計が別途求められるのである。

本稿では、このような分散型オラクルの合意形成に求められる補完的なインセンティブ設計が未だ十分に議論されていない点に着目し、現状の整理及び検討を試みる。具体的には、既存文献の調査を通じて（i）現在提案されているインセンティブ設計の整理及び問題点の指摘（ii）問題点の解決に貢献し得るピア予測法（peer prediction method）への言及の 2 点を行う。以降の構成は次の通りである。まずは次章にて現在の提案の整理と問題点の指摘を行い、次々章にてピア予測法の概要とその潜在的な可能性を論じる。そして最後に議論のまとめと今後の課題について触れる。

2 既存の合意形成手法への評価

議論を進めるにあたり、まずは分散型オラクルにおける既存の合意形成手法を、ホワイトペーパーにて比較的詳細に内容説明を行っている 3 種類の予測市場プラットフォーム : Augur, Gnosis, Stox を例に示したい。各々の合意形成プロセスの要旨は、以下の図 1[6] が示す通りである。いずれも予測市場が終了した後に、複数の選択肢中からオラクルの結果に関する合意を得る状況が想定されている。



（a）Augur　　（b）Gnosis　　（c）Stox

図 1 分散型オラクルの合計形成プロセス

これらの中で最も以前から提案され、かつ唯一完全分散型のオラクルを志向するものが Peterson, Krug, Zoltu, Williams, & Alexander (2018) による Augur である。Augur では、ある予測市場（e.g., 1 週間後の天気は晴れか雨か）の結果は、まずは市場の作成者が予め指定した報告者が規定量の内部トークンを選択肢の 1 つ（e.g.,「晴れ」または「雨」）に stake（賭け）することによって 3 日以内に暫定的に定められる[7]。これに対し、ネットワーク参加者達が各選択肢へ任意量のトークンを stake する作業を 7 日間のサイクルで繰り返すことによって合意形成が行われる。具体的には、サイクル前に全選択肢へ stake されていたトークン総量の 2/3 がサイクル期間中に別のある選択肢へと新たに stake された場合に次サイクルで暫定的な結果が更新され[8]、1 サイクル中にどの選択肢も 2/3 の閾値を超えなかった（更新に失敗した）場合にその時点での暫定的な結果を最終的な合意と見なす[9]。期間中に stake されたトークンは暫定的な結果の更新に成功したもの以外は全てサイクル終了の度に元の持ち主へ返却されることになっており、もし最終的な合意結果が得られた場合には、その合意結果以外に stake されている全トークンが合意結果に stake していた者達の間で stake 量に比例して分配される。つまり、この設計において自身が stake していた選択肢が最終的な合意となった場合、トークン量は 1.5 倍となって返却されるのである。

Augur は完全分散型の合意形成を試みる反

面、図 1（a）で明示したプロセス以外も含めれば、観測すべき事象の発生から最終的な合意に至るまでに早くとも約 3 週間はかかるという課題を持つ。そこで Gnosis（2017a）及び Stox（2017）では、初めに中央集権型で結果を定め、必要ならば後に分散型の合意形成も行えるハイブリッド型のオラクルによる効率化を試みている。具体的に、前者では TTP からの情報をオラクルの結果と見なす一方、結果を議論し直せる期間がその後に別途設けられる。ユーザーは議論の 1 つの手段として、TTP が結果を示してから 12 時間以内に合計 100 ether を別の選択肢へ stake することで結果の変更を発議することが出来、発議後は誰もが各選択肢に任意量の ether を stake 可能となる。この時、選択肢の中で最も多く ether を集めている状態を 24 時間維持したものが最終的な合意結果と見なされ、それに stake していた者達には他の選択肢へ stake されていた ether が報酬として分配される [10]。このような選択肢中で最も多くの stake 量を持つ状態を一定期間維持することを条件とする合意形成は front-runner method と呼ばれており、後者でも採用されている。後者では、ether ではなく内部トークンを支払うことで展開される front-runner method によって事後的な議論の機会が提供され、またオラクルの結果に関する選択肢では無く発議者の提案に賛成するか否かの 2 択に対して stake が行われる点が前者との差異である。加えて、本稿の議論には大きく関わらないため図 1（c）では省略しているが、予測市場の作成者はもし当初示したオラクルの結果が後に覆された場合にはそれに伴う損失の一部を担保トークンによって補償することが求められおり、これによって適切な結果報告が促されている。

以上のように、詳細な部分は異なれども予測市場における分散型オラクルには（i）検証者達は選択肢の中から自身が支持する対象へトークンを stake する（ii）所与の条件（e.g., front-runner method）を満たす選択肢 1 つを合意結果と見なしそれに stake していた検証者達の間で他の選択肢に stake されていた全トークンを分配するという 2 点の特徴を共有するインセンティブ設計が採用されている。本稿では、Peterson et al.（2018）の表記を援用しこのような勝者総取り型の設計を staking と呼ぶこととする。このような staking は、すなわち stake したトークンが失われるリスクを通じて検証者達に信念の正直な報告を促す意図が背景にあるが、一方で著者はこれには少なくとも 3 点の問題点が存在すると考える。

第 1 に、検証者が任意量のトークンを stake 可能な場合、より多くのトークンを保有する者ほど合意形成の結果を容易に覆すことが出来る。この問題はトークン保有量が多いほど更なる報酬が得やすい点で proof-of-stake に基づく暗号通貨の採掘作業と同様だが、オラクルにとってより深刻なのは、少数派だった選択肢に大量のトークンを stake して結果を覆した方が結果として獲得する報酬量が増えるため、トークンを多く保有する検証者に合意形成の結果を意図的に歪めるインセンティブが存在する点だ。staking は、このような戦略的行動により検証者達の選好を正しく反映出来ない可能性が高い。

第 2 に、例え各アカウントが stake 可能な

トークン量を固定して1 人1 票に近い形式を採ったとしても、その手法は典型的な「美人投票」であり、検証者は自身の選好では無く自身が予想する他の検証者達の平均的な選好に基づいて行動してしまう。美人投票ゲームにおいて、ナッシュ均衡はこの予想に応じて変化するため選択肢の数だけ存在することが知られている[11]。つまり、この1 人1 票型 staking でも検証者達の真の選好を正しく反映した結果を導くことは出来ないのである。

第3 に、ゼロ和ゲームであるこの手法は必ずしも検証作業に参加するインセンティブがあるとは言えない。これはシンプルなモデルによっても示すことが出来る。n 名の検証者が複数の選択肢に対して共通のトークン量 t を stake し合い、最も多くのトークンを集めた選択肢1 つを合意結果とする1 人1 票型の例を考えよう。この時、合意結果に stake していた場合に得られる報酬を r、ある検証者が予想する自らの stake 先が合意結果となる確率を p と置けば、検証作業の期待報酬 $E[r]$ は $pr-(1-p)t$ と表せる。報酬量 r は具体的に、stake された全トークン $n\cdot t$ を合意結果に stake していた検証者間で分配した値から自身の stake 分である t を引いたものである。従って合意結果に stake していた検証者の人数を n^* とすれば、$r=\frac{n\cdot t}{n^*}-t=\frac{n-n^*}{n^*}t$ と表せる。この結果を $E[r]$ へ代入して式を整理すると、期待報酬に関して以下の条件が導かれる。

$$E[r]\begin{cases}>0 & (\frac{p/(1-p)}{n^*/(1-n^*)}>1)\\ =0 & (\frac{p/(1-p)}{n^*/(1-n^*)}=1)\\ <0 & (\frac{p/(1-p)}{n^*/(1-n^*)}<1)\end{cases}$$

ここで $\frac{p/(1-p)}{n^*/(1-n^*)}$ は自らの stake 先が合意結果に選ばれる確率に関する、予想と現実のオッズ比を示す。つまり、モデルにおける期待報酬はこのオッズを実際の結果より高く見積もっていた場合のみ正値を取り、結果を正しく予想する限りの期待報酬は（ゼロ和ゲームのためある意味当然だが）0 となる。さらに検証作業自体にかかる時間や労力のコストを考慮すれば、オッズを正確に予想出来た場合の期待報酬すら負値となるだろう[12]。

3 ピア予測法の潜在的有用性

前章で指摘した3 点の問題点を解決するためには、どのようなインセンティブ設計が望ましいだろうか。まず、ゼロ和ゲームを回避するためには検証の際に新規報酬トークンの発行が必要だろう。しかし例え報酬を増やして期待値を底上げした場合でも、staking の構造が残る限りは戦略的行動に対する脆弱性や美人投票の問題は解決しない。よって

- 検証者は報告作業自体の対価として新規発行された報酬トークンを受け取る。
- 自身の信念を正直に報告した検証者はより多くの報酬トークンを受け取る。

という2 点を満たす設計が分散型オラクルの実現に必要であると著者は考える。これは言わば暗号通貨の採掘を計算資源では無く人間の主観的検証を元に行う構造だが、本稿の初めに指

摘した通り主観的な検証作業は適切に行われているか否かの客観的判断が困難であるため、単純な置き換えでは後者の条件を満たすことが出来ない。そこで本章では解決策としてピア予測法の導入を提案する。以降で詳述する通り、ピア予測法はまさにこのような主観的な検証作業に対する適切な報酬配分を扱う分野である。

ピア予測法は、proper scoring rules[13] と呼ばれるメカニズムデザインからの派生であり、確率的な事象を予測する際の回答に対し報酬の指標となるスコアを付与することで検証者達に信念の正直な報告を促すことを目的としている。一般的なスコアリングルールは $R(x \mid p_x)$ と表せる。ここで p_x は事象 x に関して検証者が報告した発生確率であり、よって $R(x \mid p_x)$ は発生確率を p_x と報告した事象 x が実際に起きた場合に獲得するスコアを意味している。スコアリングルールは、報告 p_x と検証者の信念とが一致する正直な申告が獲得スコアの期待値を最大化する場合には proper、さらにそれが期待値最大化の唯一の選択肢である場合には strictly proper とされる。この時、単純に報告した確率に応じてスコアを与える線形スコアリングルール $R(x \mid p_x) = p_x$ では proper にならないことが良く知られている。例えば松原（2016）では晴れか雨の 2 択を予測する天気予報の例を用いてこれを簡潔に説明している。2 択の予測において、検証者が事象 x に対して抱く真の信念を p^*_x とすれば、p_x と報告した場合に獲得するスコアの期待値は $p^*_x p_x + (1-p^*_x)(1-p_x)$ となる。この場合 $p^*_x > \frac{1}{2}$ である限り、検証者にとっての期待スコアは $p_x = 1$ と虚偽報告を行った際に最大化されてしまう[14]。これに対し strictly proper となる代表例の 1 つは、対数スコアリングルール $R(x \mid p_x) = \ln p_x$ である。先の例に当てはめると期待値は $p^*_x \ln p_x + (1-p^*_x) \ln (1-p_x)$ となり、p_x に関する 1 階の条件を導出することで $p_x = p^*_x$ が獲得スコアを最大化する唯一の報告であることが判るだろう。その他にも二次（quadratic）スコアリングや球体（spherical）スコアリング等、strictly proper となるルールは多く提案されている。

以上の議論は事象 x が発生したか否かが後に客観的な結果として明らかになる前提だったが、例えば学術論文の査読やオンラインのレビューサイト、そして分散型オラクルがそうであるように、予測対象の結果が最終的に明示されない検証作業も存在する。再び天気予報の例を用いるならば、TTP が後に結果を明らかにする天気を予測するならばスコアリング可能である一方、当日に検証者達が観測した天気の分類に関する合意形成（e.g., 一瞬小雨が降ったかも知れない場合を晴れとするか雨とするか）には各々の主観的な見解しか存在しないため $R(x \mid p_x)$ で表現されるスコアリングルールは適用することが出来ない[15]。そこでピア予測法を初めて示した Miller, Resnick, & Zeckhauser（2005）は、検証者の報告では無く、検証者の報告によって更新される他の検証者の報告に関する事後確率分布へのスコアリングを提起した。この概念は、事象 x が確率的にシグナル s を発すると仮定し、それを受け取った検証者達の報告によって x のタイプを推測するモデルによって定式化される。具体的に、Miller et al.（2005）は（i）事象 x のタイプと各タイプが発するシグナル s はそれぞれ所与の事前確率分布に従う[16]（ii）

事前確率分布は検証者間の共有知識である（iii）事前確率分布は検証者の報告内容に応じて更新されるという 3 点を仮定した上で検証者 i に対する以下のスコアリングルールを提案している。

$$R\left(s_j \mid a_i\left(s_i\right)\right)$$

ここで a_i はシグナル s_i を受け取った検証者 i による報告であり、よって $R\left(s_j \mid a_i\left(s_i\right)\right)$ は自分が a と報告した後に別の検証者 j がシグナル s を受け取る場合の獲得スコアを表す。スコアリング対象は s_j の事後確率分布 $p\left(s_j \mid a_i\left(s_i\right)\right)$ であるため、対数スコアリングを採用するならば $R\left(s_j \mid a_i\left(s_i\right)\right) = \ln p\left(s_j \mid a_i\left(s_i\right)\right)$ である [17]。Miller et al.（2005）は、$R\left(x \mid p_x\right)$ のケースで strictly proper とされたスコアリングルールがこの場合でも正直な報告 $a_i\left(s_i\right) = s_i$ を促せる旨を示すと共に、検証者達が他者の受け取るシグナルを直接観測出来ないより現実的な世界、つまり $R\left(a_j\left(s_j\right) \mid a_i\left(s_i\right)\right)$ 環境下の同時報告ゲームにおいて全員が正直に報告する戦略 $a_i\left(s_i\right) = s_i, \forall i$ が狭義ナッシュ均衡に含まれることを明らかにした。直感的に言えば、検証者達それぞれが「自分がこれから報告する内容が他者の報告に与える影響次第でスコアが決まる」という前提を共有した上で相手の出方を読み合う限り、彼らは全員受け取ったシグナルを正直に報告し得る。このように、既存のスコアリングルールを他者との比較に基づくゲームへと拡張することで、客観的な結果が存在しない検証作業でも有用なスコアの導出を可能にした点がピア予測法の新規性なのである。

Miller et al.（2005）以降のピア予測法は、モデルの仮定を緩めつつより実用的なメカニズムを示す方向で議論が発展している。例えば検証者達が観測対象のタイプとシグナルに関する事前確率分布を共有しているという強い仮定に対しては、Witkowski and Parkes（2012）がシグナルを報告する前に他者の事前確率分布に対する予測も報告者に課す手法を、そして Radanovic and Faltings（2013）がシグナル報告と同時に他者が観測したシグナルの予測を報告者に課す手法をそれぞれ提案している。また Miller et al.（2005）の欠点として、検証者達が結託して全く同じ回答を表明する行為もナッシュ均衡に含まれる点がしばしば指摘されている。複数の均衡が存在し得る点でこのままでは staking の美人投票問題と同様だが、これは Jurca and Faltings（2007）及び Jurca and Faltings（2009）により、比較対象とする他者の数を複数に増やすことを通じた対策が示されている。さらに、最近では検証作業に費やす労力をモデルへ明示的に反映させる試みも Dasgupta and Ghosh（2013）や Liu and Chen（2016）らによって成されている。前者では各検証者に複数の観測対象への報告を課し、個別の報酬計算に他の観測対象に対して行った報告も用いることで彼らに労力を割いた正直な報告を促す手法が、後者ではピア予測法を繰り返し行うことで各検証者の報告の質と努力水準を探りつつ最適な報酬を導出する手法がそれぞれ提案されている。

ピア予測法が持つ上記の研究背景及び議論の発展は、この手法が本章初めに記した 2 つの条件を満たすインセンティブ設計を分散型オラクルにもたらす可能性を示唆している。すなわち、作業の対価として担当者全員に報酬トークンを発行しつつその配分をピア予測法のスコア

に準じて重み付けすることで、適切な検証作業への規律付けが期待出来る。先述の通りモデルの詳細な検討は本稿で扱う範囲外だが、この達成に向けた設計案としては、例えばある検証作業に対して予め求める報告数と発行トークン量が規定されており、その情報を把握する検証者達から先着順で報告を集める形式等が考えられるだろう[18]。このように、ピア予測法と分散型オラクルとの間にはシナジーが存在し、その導入はこれまで困難だった人間の主観的な検証作業に基づく採掘メカニズムの実現に大きく貢献するはずである。

4 おわりに

本稿では、分散型オラクルの合意形成に対するピア予測法の潜在的有用性を示した。主観的な検証作業を伴う性質上、分散型オラクルにはトークン形式の報酬を補完するインセンティブ設計が別途求められるが、現在専ら採用される各選択肢へトークンを賭け合う staking の手法には（i）大量のトークン保有者による戦略的行動に対して脆弱である（ii）美人投票となり検証者の真の選好を反映出来ない（iii）ゼロ和ゲームのため検証作業に参加するインセンティブが弱いという 3 点の問題が少なくとも存在する。これらは、全ての検証担当者へ報酬トークンを発行しつつも、自身の報告が更新する他者の報告に関する事後確率分布に基づき報酬量を決定するピア予測法を用いて各々への分配を重み付けすることにより解決する可能性がある。報酬トークンとピア予測法の組み合わせにより、分散型オラクルはシステム全体と個別の検証作業の両面から望ましくない行動を予防し、結果として計算資源では無く人間の主観的な検証作業に基づく採掘メカニズムの実現が期待出来るだろう。

冒頭で記した通り分散型オラクルは本稿執筆時点において未だ実用レベルのアプリケーションが公開されておらず、故にその合意形成手法に対する議論もほとんど行われていない。またピア予測法とのシナジーについて言及している研究も著者の知る限りでは存在しない。こうした状況の下、現在提案されている手法の問題点を明らかにすると共にその問題解決に貢献し得るピア予測法の有用性を示した点は、ブロックチェーン周辺のインセンティブ設計に特化したメカニズムデザイン[19]という新たな学問分野の発展に貢献するという意味で学術的意義がある。他方で、本稿はピア予測法の潜在的有用性を示唆するに留まっており、既存の設計に対する代替モデルを提示するまでには至っていない。従って、ピア予測法を採用した具体的なインセンティブ設計を定式化し、staking に基づく既存手法と比較した場合の優位性を厳密に検証することが今後の重要な課題である。

最後に、将来報酬トークンとピア予測法の組み合わせを試みる際に考慮すべき 2 点の課題について記したい。第 1 に、もし何らかの外生的ショックによりトークンの価格が下落すると、ピア予測法による報酬の重み付けは適切なレビューを促すインセンティブとしての効果を発揮出来なくなる。この場合、入力情報に対す

る検証作業が不十分となるため分散型オラクル全体の質が下がり、その結果トークン価格が更に下落するという悪循環に陥ってしまう。このような問題を解決するためには、ビットコインにおける採掘難易度調整のような価格安定化のための何らかのメカニズムが必要となるだろう。第2に、検証作業へのインセンティブとして担当者への報酬が必要である一方、際限の無い新規トークン発行はインフレーションを引き起こす可能性がある。staking の場合には新規発行を伴わないものの、既述の通りゼロ和ゲームでは検証に参加するインセンティブが不足する。つまり、分散型オラクルにおいてシステムの持続性と適切な検証作業の促進は基本的にトレードオフの関係にある。以上の問題に取り組むには、ビットコインにおける半減期のような報酬を新規発行しつつもその総供給量を固定するメカニズムが求められるだろう。

註

1 すなわち、proof-of-work に基づき後に正統と見なされる新規ブロックを作成した採掘者。

2 経済学の文脈において、これはプリンシパル＝エージェント問題として捉えることが出来る。ビットコインによる採掘者への報酬は、例えば経営者に対する規律付けとしてストックオプションのような業績連動型の報酬を与える手法に相当するだろう。

3 スマートコントラクトという用語は Szabo（1997）によって提唱されたが、ブロックチェーンの文脈においてはより狭義に用いられることが多い。ブロックチェーンの文脈におけるスマートコントラクトに関しては、例えば Hileman and Rauchs（2017）, p11, pp57-60. を参照せよ。

4 ブロックチェーンの文脈におけるオラクルという用語に関しては、著者の知る限りでは未だ学術的な定義付けが成されていない。従ってこの用語の概念については、例えば次のようなウェブページ : [Blockchain Oracles: online], [Ethereum and Oracles: online]、及び後に示す予測市場のホワイトペーパー群 : Peterson et al.（2018）, Gnosis（2017a）, Stox（2017）等を参照せよ。

5 分散型オラクルに関する議論では、例えば[Oraclize: online] 等 TTP からの情報が伝送の過程で改ざんされていないことをブロックチェーン上で証明するための技術についてもしばしば扱われるが、本稿では人間が検証を行う際のインセンティブ設計に議論の対象を絞っている点に留意されたい。

6 それぞれホワイトペーパーを元に著者作成。

7 もしこの報告者が観測すべき事象の発生から 3 日以内に回答しなかった場合には、代わりにネットワーク参加者全員が回答可能となり、最初に成された回答が暫定的な結果となる。

8 著者が読む限り 1 サイクルの間に複数の選択肢が 2/3 の閾値を超えた場合の対処は Peterson et al.（2018）には明記されていない。しかし、先に 2/3 を獲得した選択肢を次サイクルの暫定的な結果とする解釈が自然だろう。

9 もし最初のサイクルで全く stake が行われなかった場合には、初めの暫定的な結果が最終的な合意となる。

10 Gnosis（2017a）において 100 ether が stake されて以降の仕組みは Ultimate Oracle と呼ばれている。ただし、同年 12 月に発表されたホワイトペーパー Gnosis（2017b）においてはこの Ultimate Oracle を含むオラクルの設計全般に関する議論が削除されている点は留意する必要がある。

11 美人投票の概念は、現在では平均値に $p \in (0,\ 1]$ をかけた値を予想し合う数当てゲーム *p-Beauty Contest Game* として一般化されている（e.g., Moulin（1986）, Nagel（1995））。ナッシュ均衡が選択肢の数だけ存在する状態は、単純に平均値を当てる $p = 1$ のケースに限定される点に注意せよ。

12 検証作業に必要なコストを c と仮定した場合、モデルにおける期待報酬は $E[r] = p\,(r - c) - (1 - p)\,(t + c)$ となる。これに対して同様に r を代入して式を整理すると、$E[r] = 0$ が成立するための条件は $\frac{p/(1-p)}{n^*/(1-n^*)} = \frac{1}{1-p}\,\frac{t+c}{t} - p$ となり、右辺は必ず 1 よりも大きくなることが判る。

13 Proper scoring rules に関しては、例えば Gneiting and Raftery（2007）によるサーベイを参照せよ。

14 松原（2016）では、報告者が $p^*_x = \frac{3}{4},\ 1 - p^*_x = \frac{1}{4}$ という信念を持つ場合、正直な報告 $p_x = \frac{3}{4}$ に対する期待スコアが $\frac{5}{8}$、虚偽報告 $p_x = 1$ に対する期待スコア $\frac{6}{8}$ という具体的な数値例を用いてこれを示している。

15 Stox（2017）pp 53-55. では proper scoring rule について言及しているが、これはオラクルが機能している状態を仮定した上で

の予測市場への参加者達に対するスコアリングである点に注意せよ。

[16] すなわち 2 択の天気予報でシグナルも対応する 2 種類のみである場合には p（x = 晴れ）; p（x = 雨）; p（s = 晴れ | x = 晴れ）; p（s = 雨 | x = 晴れ）; p（s = 晴れ | x = 雨）; p（s = 雨 | x = 雨）が所与の事前確率として定義される。

[17] 天気予報の例をこれに当てはめるならば s_i = 晴れの時に正直に報告する場合の期待スコアは p（s_j = 晴れ | s_i = 晴れ）ln p（s_j = 晴れ | a_i（s_i）= 晴れ）+ p（s_j = 雨 | s_i = 晴れ）ln p（s_j = 雨 | a_i（s_i）= 晴れ）反対に雨と虚偽報告する場合の期待スコアは p（s_j = 晴れ | s_i = 晴れ）ln p（s_j = 晴れ | a_i（s_i）= 雨）+ p（s_j = 雨 | s_i = 晴れ）ln p（s_j = 雨 | a_i（s_i）= 雨）と表せる。

[18] 検証者達が同時では無く順番に報告を行う形式は Miller et al.（2005）においてもモデルの拡張例として言及されている。

[19] この試みは、近年 *cryptoeconomics* と呼ばれている。Ethereum 開発者達を中心に提唱されている造語であり、その定義や議論展開については、例えば Davidson, De Filippi, & Potts（2016）を参照せよ。

参考文献

松原繁夫 . 2016.“マルチエージェントシステムにおける経済学的アプローチ”. 計測と制御 , 55 巻 11 号 pp 948-953.

Blockchain and Oracles.“Blockchain and Oracles”. BlockchainHub. https://blockchainhub.net/blockchain-oracles/. Accessed on April 2 2018.

Buterin, Vitalik. 2014.“A Next-Generation Smart Contract and Decentralized Application Platform”. Available at: https://whitepaperdatabase.com/ethereum-eth-whitepaper/. Accessed on 25 March 2018.

Dasgupta, Anirban and Arpita Ghosh. 2013.“Crowdsourced Judgement Elicitation with Endogenous Proficiency”. WWW13, pp 1–17.

Davidson, Sinclair, Primavera De Filippi, Jason Potts. 2016“Economics of blockchain”. Available at: https://ssrn.com/abstract=2744751. Accessed on 21 August 2018.

Ethereum and Oracles.“Ethereum and Oracles”. Ethereum Blog. https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/. Accessed on April 2 2018.

Gneiting, Tilmann, and Adrian E. Raftery. 2007.“Strictly proper scoring rules, prediction, and estimation”. Journal of the American Statistical Association 102.477（2007）, pp 359-378.

Gnosis. 2017a.“Gnosis Whitepaper – 05.04.2017”. Available at: https://whitepaperdatabase.com/gnosis-gno-whitepaper/. Accessed on 3 May 2018.

Gnosis. 2017b.“Gnosis Whitepaper 22 December 2017”. Available at: https://gnosis.pm/resources/default/pdf/gnosis-whitepaper-DEC2017.pdf. Accessed on 3 May 2018.

Hileman, Garrick, Michel Rauchs. 2017.“Global Blockchain Benchmarking Study”. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224. Accessed on 24 March 2018.

Jurca, Radu and Boi Faltings. 2007.“Collusion-resistant, incentive-compatible feedback payments”. Proceedings of the 8th ACM conference on Electronic commerce, pp 200-209.

Jurca, Radu and Boi Faltings. 2009.“Mechanisms for making crowds truthful”. Journal of Artificial Intelligence Research, 34（1）, pp 209–253.

Liu, Yang and Yiling Chen. 2017.“Sequential Peer Prediction: Learning to Elicit Effort using Posted Prices”. AAAI, pp 607-613.

Miller, Nolan, Paul Resnick, Richard Zeckhauser. 2005.“Eliciting informative feedback: The peer-prediction method”. Management Science, 51, pp 1359–1373.

Moulin, Herve. 1986. Game Theory for the Social Sciences（2nd ed.）. New York: NYU Press.

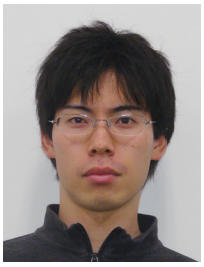
Nagel, Rosemarie. 1995.“Unraveling in Guessing Games: An Experimental Study”. American Economic Review, 85（5）, pp 1313-1326.

Nakamoto, Satoshi. 2008.“Bitcoin: A Peer-to-Peer Electronic Cash System”. Available at: https://bitcoin.org/bitcoin.pdf. Accessed on 24 March 2018.

Oraclize.“Oraclize - blockchain oracle service, enabling data-rich smart contracts”. Oraclize limited. http://www.oraclize.it/. Accessed on April 2 2018.

Peterson, Jack, Joseph Krug, Micah Zoltu, Austin, K. Williams, Stephanie Alexander. 2018.“Augur: a Decentralized Oracle and Prediction Market Platform”. Available at:

http://www.augur.net/whitepaper.pdf. Accessed on 8 January 2018.
Radanovic, Goran and Boi Faltings. 2013. “A Robust Bayesian Truth Serum for Non-Binary Signals”. AAAI13, pp 833–839.
Stox. 2017. “Stox Platform for Prediction Markets whitepaper v03”. Available at:
https://resources.stox.com/stox-whitepaper.pdf. Accessed on 3 May 2018.
Szabo, Nick. 1997. “Formalizing and securing relationships on public networks”. First Monday 2.9.
Witkowski, Jens and David C Parkes. 2012. “Peer Prediction Without a Common Prior”. Proceedings of the 13th ACM Conference on Electronic Commerce, pp 964-981.



伊東　謙介（いとう・けんすけ）
［生年月］1991/12
［出身大学または最終学歴］東京大学学際情報学府社会情報学コース博士課程在籍

A Potential Utility of Peer Prediction Method to Consensus Building on Decentralized Oracle Systems

Kensuke ITO*

In this paper, we pointed the potential utility of *peer prediction method* to the existing consensus building in decentralized oracle systems where participants aim to verify the validity of input information to blockchain without relying on a trusted third party (TTP). This is important because, despite the recent expectation of implementing decentralized oracle systems, few discussions have dealt with the incentive design for their consensus building, much less the synergy with peer prediction method. Specifically, we mentioned the followings through the survey of preceding studies: (i) the current predominant method of *staking* that allows validators to bet the reward tokens has the limitations such as a vulnerability to strategic behavior and a lack of incentive to participate in the verification, (ii) these problems could be solved by peer prediction method which determines the amount of rewards based on the posterior probability distribution on the report of others updated by one's own report. Peer prediction method can encourage validators to perform proper verification while supplementing the token-based rewards, and thereby can contribute to the realization of the mining mechanism based on subjective review instead of computational resources. On the other hand, several obstacles still remain to propose a practical incentive design, such as the fluctuation of token price that would prevent peer prediction from incentivizing proper verification.

Ph.D. student, Graduate School of Interdisciplinary Information Studies, The University of Tokyo.

Key Words : *Decentralized Oracle, Peer Prediction Method, Blockchain, Consensus Building, Mechanism Design.*