Augur:分散型オラクルと予測市場プラットフォーム

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Forecast Foundation
(Dated: 2018/03/05)

Augur はトラストレスな分散型オラクルと予測市場のプラットフォームである。Augur の予測市場では、Augur のネイティブトークンである Reputation を保有しているユーザーが、現実で確認したアウトカム (outcome) にそのトークンをステークすることによってアウトカムを選択し、その見返りとしてマーケットから決済手数料 (settlement fee) を受け取る。Augur では、Reputation 保有者が正直かつ正確にアウトカムをレポートすることが、常に最も有益な行動であるようインセンティブ設計されている。トークン保有者は累進的に増加する (Reptation 支払いの) 争議保証金を提示することで、マーケットで提示された結果に対して争議 (dispute) を行うことが可能である。この保証金がある閾値に達すると、Reputation がマーケットのアウトカム毎に複数のバージョンに分割され、トークン保有者はこの分割されたいずれかのバージョンのトークンに交換しなければならない。正しく結果判定されない予測市場には誰も参加しないため、現実とそぐわない結果のバージョンの Reputation は無価値となる。そのため、トークン保有者は引き続き価値があると考えるバージョン、すなわち現実に起こった事象と合致するバージョンの Reputation を選択する。

Augur はトラストレスな分散型オラクルと予測市場のプラットフォームである。予測市場では、各個人が未来の出来事の結果を推測することができる。結果を正しく予測した者は賞金を獲得し、誤った者は失う [1–3]。予測市場の価格をもって、そのイベントが発生する可能性を正確に測定することができる [4–7]。

Augur を使用することで、非常にコストが低い予測市場でトレードが可能となる。 Augur の参加者に想定される最も大きな支出は、マーケット作成者、および、マーケットのアウトカムに対してレポートを行うユーザーに対する報酬である。そのため、競争原理よって予測市場の信用の要求、摩擦、手数料は低くなる。

予測市場は中央集権化の歴史であった。予測市場において取引を集約する最も簡単な方法は、信頼できる企業が取引の帳簿を管理することである。同様に、イベントのアウトカムを決定しトレーダーに配当を分配する最も簡単な方法は、公平で信頼できる裁判官的な人物にその役割を果たしてもらうである。しかし、集権的な予測市場には多くのリスクと限界がある。集権的な予測市場では、グローバルな規模での参加が許されず、市場の作成や取引可能な市場の種類を制限されるケースがあり、加えてトレーダーは管理者が資金を盗まず市場の結果判定を正しく行うことを信用しなくてはならない。

Augur は完全な分散型市場を目指している。Bitcoin[8] や Ethereum[9] などのトラストレスな分散型ネットワークは、私利私欲による贈賄や盗難のリスクを排除する。Augur 開発者の唯一の役割は、スマートコントラクトを Ethereum ネットワークに公開することである。Augur のコントラクトは完全に自動化されており、開発者はコントラクト上のエスクロー取引で保有されている資金を横領することや、マーケットで下された判決の制御、ネットワーク上にある取引の承認・拒否・変更・取消などはできない。Augur のオラクルによって、現実世界の情報を信頼を必要とする仲介者に依存することなくブロックチェーン上に移行させることが可能である。 Augur は世界初の分散型オラクルとなるだろう。

I. どのようにして AUGUR は動くか

Augur のマーケットは、作成 *(creation)*、トレーディング *(trading)*、レポーティング *(reporting)*、決済 *(settlement)* の 4 段階から成る。現実世界のイベントに基づき、誰でもマーケットを作成することができる。マーケット作成直後からトレーディングが始まり、すべてのユーザーは自由にマーケットで取引可能である。マーケットの元となるイベントが発生した後、イベントのアウトカムは Augur のオラクルによって決定される。アウトカムが決まれば、トレーダーはポジションをクローズし支払いを受け取ることとなる。

Augur にはネイティブトークンである Reputation(REP) がある。REP は、Augur プラットフォームで作成されたマーケットの作成者と、そのマーケットのアウトカムを報告するレポーターが使用する。レポーターは、マーケットのアウトカムの 1 つに REP をステーク *(staking)* することによって、そのマーケットへのレポートを行う。これによって、レポーターは「自身の REP をステークしたアウトカムこそが、現実で起きたアウトカムである」と宣言したことになる。各レポーターのコンセンサスは、マーケットのアウトカムを決定するための”真実 (truth)”とみなされる。あるレポーターのレポートが、コンセンサスとなったレポートと一致しなかった場合、コンセンサスと一致したレポーターに対して、一致しなかったレポーターの REP を分配する。

REP を所有し、正確なアウトカムをレポートすることにより、トークン所有者はプラットフォーム上の手数料の一部を受け取ることができる。ステークした REP に応じてその所有者に対して、Augur のマーケット手数料が平等に分配される。より多い REP を所有し正しいレポートを行うことにより、Augur のプラットフォームを安全に保った作業報酬としてより多い手数料を獲得できる。

Augur において REP は中心的な役割を果たしているが、Augur のマーケットでのトレーディングには使用されない。トレーダーはレポーティングに参加する必要が無いため、REP を保有・使用するは必要はない。

Figure 1. 予測市場のライフタイム概要

A. マーケット作成

Augur ではこれから起こるイベントについてのマーケットを作成することができる。マーケット作成者 *(maket createor)* は、イベント終了日時 *(event end time)* を設定し、イベントのアウトカムをレポートするための指名レポーター *(designated reporter)* を選択する。指名レポーターはマーケットのアウトカムを一方的に決定するものではない。コミュニティには、指名レポーターのレポート内容に対して争議を行い、訂正する機会が常に与えられる。

次に、マーケット作成者はレポーターがアウトカムを決定するために使用する判決ソース *(resolution source)* を選択する。判決ソースは単に「一般常識」でも良く、例えば、「米国エネルギー省」、bbc.com、特定の API エンドポイントのアドレス等の特定のソースでも良い。[1] そして、トレーダーの決済時にマーケット作成者に対して支払われる作成者手数料 *(creator fee)* の設定を行う (手数料についての詳細はIDを参照)。最後に、マーケット作成者は 2 つの保証金を支払う。有効性保証金 *(validity bond)* と 指名レポート不参保証金 *(designated report no-show bond)*(略して、不参保証金 *(no-show bond)*) である。

有効性保証金の支払いは ETH で行われ、この保証金はマーケットが無効 *(invalid)* 以外のアウトカムになればマーケット作成者へ返却される。[2] 有効性保証金は、明瞭なアウトカムがあり、明確に定義されたマーケットを作成する動機付けとなる。有効性保証金の金額は、直近のマーケットで無効と判定されたマーケットの割合から動的に設定される。[3]

不参保証金は、ETH によって支払われる不参 *gas* 保証金 *(no-show gas bond)* と、REP によって支払われる不参 *REP* 保証金 *(no-show REP bond)* の 2 つから構成される。これらの保証金は、そのマーケットのイベント終了日時が過ぎた最初の 3 日以内に指名レポーターがレポートを行えば、マーケット作成者に返却される。3 日以内に指名レポーターがレポートしなかった場合、マーケット作成者の不参保証金は没収され、ファーストパブリックレポート *(first public report)* でレポートをしたレポーターにその保証金が与えられる (セクションIC6を参照)。これにより、マーケット作成者は信頼性の高い指名レポーターを選択する動機付けとなり、マーケットの判決も早く下される。

不参 gas 保証金は、ファーストパブリックレポーターの gas コストを賄うために設けられた。この保証金によって、ファーストパブリックレポーターの gas コストが高すぎるためにレポーターに損益が出る、という事態を防いでいる。不参 gas 保証金は、直前の手数料期間 *(fee window)* の平均 gas コストの 2 倍が設定される。

指名レポートが行われなかった場合、不参 REP 保証金は、ファーストパブリックレポーターがレポートしたアウトカムへの追加ステークという形で与えられる。ゆえに、不参 REP 保証金を受け取ることができるのは、ファーストパブリックレポーターが正しいレポートを行った場合のみである。有効性保証金と同様、直前の手数料期間にレポートを行わなかった指名レポーターの割合に応じて、不参 REP 保証金の金額は調整される。[4]

これら一連のマーケット作成とそれに伴う必要な保証金の支払いは、単一の Ethereum トランザクションで行われる。このトランザクションが承認されれば、マーケットでのトレードが開始される。

B. トレーディング

マーケット参加者は、アウトカムのシェア *(shares)* を取引することにより、そのイベントのアウトカムを予測する。シェアのコンプリートセット *(complete set of shares)* は、そのイベントで有効なアウトカムに該当するシェアの集合で構成される [10]。コンプリートセットは、トレードを完了させるため Augur のコントラクト上にあるマッチングエンジンによって必要に応じて作成される。

例えば、A、B の 2 つのアウトカムが予想されるマーケットを考えてみよう。アリスは A のシェアに 0.7ETH を支払い、ボブは B のシェアに 0.3ETH を支払うとする。[5] まず、Augur はこれらのオーダーをマッチングし、アリスとボブから合計 1ETH を受け取り[6]、シェアのコンプリートセットを作成して、アリスに A のシェア、ボブに B のシェアを与

[1] 例えば、「WeatherUnderground で報告された、2018 年 4 月 10 日のサンフランシスコ国際空港の最高気温 (華氏) は?」というマーケットがあり、判決ソースとして https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html を指定している場合、レポーターはその URL にアクセスし、表示されている最高気温をレポートすれば良い。

[2] 無効マーケット (invalid market) とは、マーケット作成者が列挙したアウトカムのいずれも誤っているため、あるいはマーケットの文言が曖昧または主観的であるため、レポーターによって無効と判断されたマーケットのことである。IIIF を参照

[3] 詳細は Appendix.E 1を参照。

[4] 詳細は Appendix.E 2を参照。

[5] リリース初めは、Augur のマーケットでは Ethereum のネイティブこいんである Ether（ETH）が使用可能である。続くリリースで、Ethereum ネットワーク上で発行された任意のトークンをサポートし、法定通貨に固定されたトークン ("stablecoin") と同様、他マーケットのシェアも取り扱う予定である。

[6] ここでは、説明を簡単にするために 1 桁の数字である 1ETH を使用している。実際のシェアのコンプリートセットのコストはこれよりもはるかに小さい。詳細は docs.augur.net/#number-of-ticks を参照。

える。こうして各アウトカムのシェアが生成される。シェアが生成されれば、あとは自由に取引することができる。

Augur のトレード用コントラクトは、プラットフォーム上に作成された全てのマーケットのオーダーブックを保持している。新しいオーダーは誰でも作成でき、存在するオーダーに対していつでも約定することが可能である。オーダーは Augur のスマートコントラクト内にある自動マッチングエンジンにより約定される。シェアの売買要求は、オーダーブックにマッチングするオーダーが存在するならば即座に約定する。それは、既存のコンプリートセットのクローズ、または、新たなコンプリートセットの発行を含め、他参加者によるシェアの購入や売却によって遂行される。Augur のマッチングエンジンは、最悪の事態に備え、最小限のシェア、及び/または、キャッシュのみをマッチングに使用する。マッチングするオーダーが無い、または、部分的にしかオーダーを約定することができない場合、残りのオーダーは新しいオーダーとしてオーダーブックに置かれる。

オーダーはトレーダーが設定した制限価格よりも悪い価格で約定することはないが、より良い価格で約定することはある。未約定のオーダーと一部約定済みのオーダーは、オーダー作成者によりいつでもオーダーブックから削除できる。手数料は、シェアのコンプリートセットが売却された場合にのみトレーダーにより支払われる。決済手数料については、セクション IDでより詳細に述べている。

シェアのトレードの大部分はマーケット決済前に行われると予想されるが、シェアはマーケット作成後であればいつでもトレード可能である。Augur 上のすべての資産 – アウトカムのシェア、パーティシペーショントークン、争議保証金のシェア、さらにはマーケット自体の所有権までも – は (トークン化されているという意味で) 常に譲渡可能である。

C. レポーティング

マーケットのイベント発生後は、ファイナライズし決済を開始するためにアウトカムを決定しなくてはならない。アウトカムは、Augur のオラクル (現実に起きた事実をレポートすることで利益を得る、レポーターと呼ばれる人々で構成) によって決定される。REP を所有する人は誰でも、アウトカムに対してレポーティングや争議を行うことができる。レポートがコンセンサスに合致していれば、レポーターは報酬を得られるが、合致しなければ罰金を科せられる（セクション ID3参照)。

1. 手数料期間

Augur のレポーティングシステムは、7 日間の手数料期間 *(fee windows)* が繰り返されることにより稼働する。手数料期間中に Augur によって収集された全ての手数料は、レポーティング手数料プール *(reporting fee pool)* に加算される。手数料期間の最後に、レポーティングに参加した REP 保有者に対し、このレポーティング手数料プールから支払いが行われる。レポーターは手数料期間中にステークした REP の量に比例して報酬を受け取る。ここで言うレポーティングへの参加とは、イニシャルレポートで REP をステークすること、暫定アウトカムに対して争議すること、パーティシペーショントークン *(participation tokens)* を購入することを指す。

2. パーティシペーショントークン

手数料期間中、REP 保有者は 1 attorep[7] 単位で、任意の数のパーティシペーショントークンを購入できる。手数料期間の最後に、購入したパーティシペーショントークンは REP に戻して返却され、さらに、購入したパーティシペーショントークン量に応じて、レポーティング手数料プールから手数料を獲得することができる。もし、レポーターが求められる行為 (例:レポート提出、別ユーザーのレポートに対する争議) を行わない場合は、パーティシペーショントークンを購入することで、手数料期間中に Augur に姿を現すことを意思表示できる。REP をステークすることと同様、パーティシペーショントークンの所有量に応じて、手数料期間に収集された手数料を獲得できる。

セクション IIで述べているように、REP 保有者がマーケットのフォークへの参加に備えていることは重要である。パーティシペーショントークンは、REP 保有者に少なくとも週に一度プラットフォームを監視する動機づけとなるため、その必要性が生じた場合は参加の促進に繋がる。パーティシペーショントークンを購入して手数料を手に入れる、というインセンティブがあるため、レポーティングへの参加を望まない REP 所有者に対しても、手数料期間の七日間に一度は Augur にチェックインさせる動機づけとなる。この定期的なチェックインは、Augur の利用促進、フォーク発生検知の促進となり、結果、フォークが発生した場合にユーザーの参加が促進される。

3. マーケットの状態の進行

Augur のマーケットは作成後に 7 つの状態に遷移する。Augur のマーケットの潜在的な状態、すなわち「フェーズ」は次の通り

- レポーティング前
- 指名レポーティング
- 公開レポーティング
- 次の手数料期間開始待ち
- 争議ラウンド
- フォーク
- ファイナライズ

これらの状態の関係を Figure. 2に示す。

---

[7] 1 *attorep* は 10^{-18} REP。

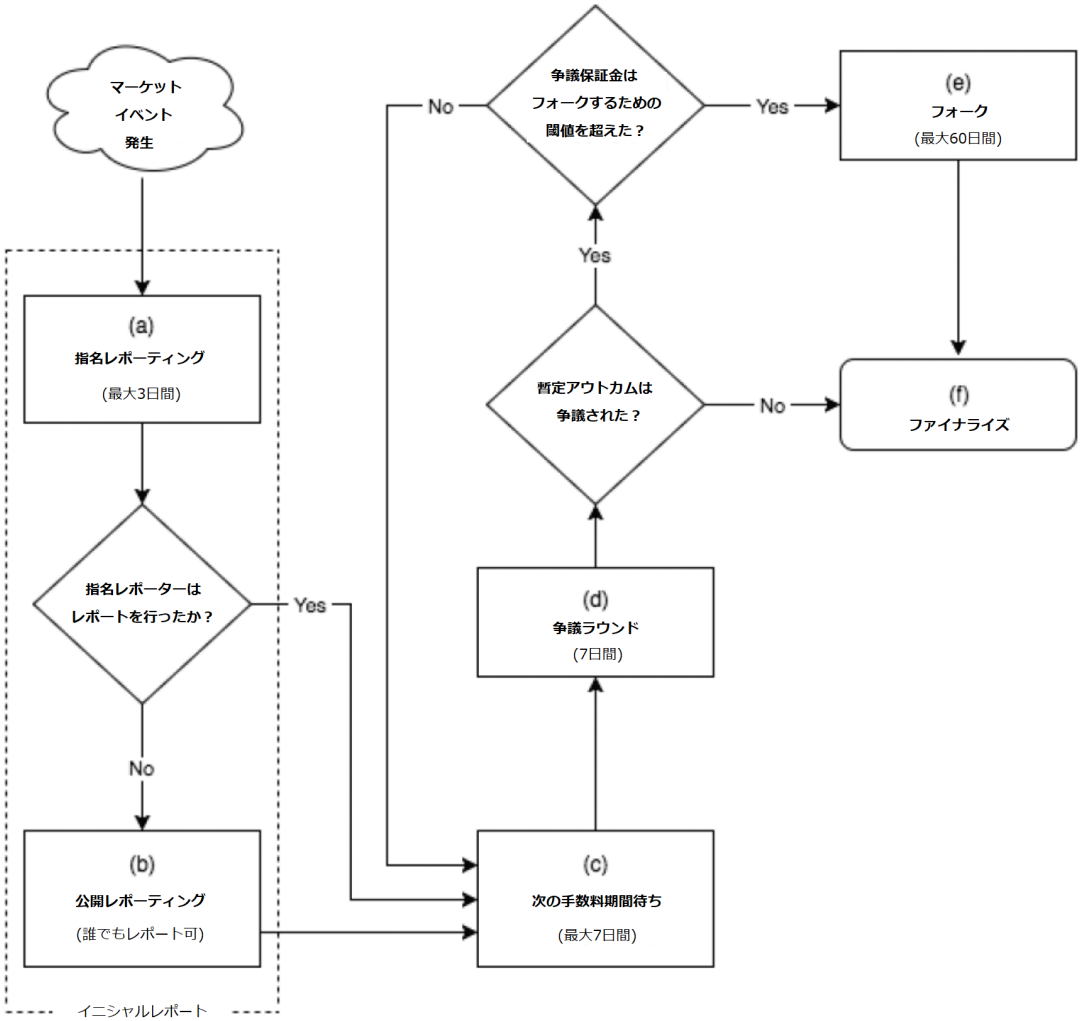

Figure 2. レポーティングフローチャート

4. レポーティング前

レポーティング前 *(pre-reporting)*、またはトレーディング *(trading)* フェーズ (Figure. 1) とは、トレード開始からマーケットのイベントが発生するまでの期間を指す。一般に、Augur のマーケットにおいて最も活発にトレードが行われる期間である。マーケットがイベント終了日時を過ぎると、指名レポーティング *(Designated Reporting)* フェーズに突入する (Figure. 2a)

5. 指名レポーティング

マーケット作成時、作成者は指名レポーターを選び、不参保証金を支払う必要がある。指名レポーティングフェーズ (Figure. 2a) では、指名レポーターはイベントのアウトカムをレポートするために 3 日間の猶予が与えられる。指名レポーターがその 3 日以内にレポートしなかった場合、マーケット作成者は不参保証金を失い、マーケットは自動的に公開レポーティング *(Open Reporting)* フェーズに移行する (Figure. 2b)。

指名レポーターがその 3 日以内にレポートを行えば、不参保証金はマーケット作成者に返却される。指名レポーターは自身がレポートしたアウトカムに対して、指名レポーターステーク[8] を支払う必要があり、仮に指名レポーターがレポートした以外のアウトカムにマーケットがファイナライズすると、指名レポーターステークは没収される。[9] 指名レポーターがレポートを行うとすぐにそのマーケットは次の手数料期間開始待ち *(Waiting for the Next Fee Window to Begin)* フェーズに移行し (Figure. 2c)、指名レポーターがレポートしたアウトカムはそのマーケットの暫定アウトカム *(tentative outcome)* となる。

[8] 指名レポーターステークの大きさについての詳細は Appendix.E 3を参照

[9] 没収されたステークは、該当の手数料期間のレポーティング手数料プールに加算され、真実をレポートしたレポーターや争議を行った者への報奨金として使用される。詳細はセクション ID 3を参照。

6. 公開レポーティング

もし、指名レポーターが割り当てられた 3 日以内にレポートできなかった場合、マーケット作成者は不参保証金を没収され、直後そのマーケットは公開レポーティング *(open reporting)* フェーズに入る (Figure. 2b)。このフェーズでは、誰でもそのマーケットに対してレポートが可能となる。指名レポーターのレポート失敗後に最初にレポートを行ったレポーターを、そのマーケットのファーストパブリックレポーター *(first public reporter)* と呼ぶ。

ファーストパブリックレポーターは、彼らが選択したアウトカムへの追加ステークという形で、没収された不参保証金を獲得する。つまり、レポートしたアウトカムがマーケットのファイナルアウトカムになった場合にのみ、不参 REP 保証金を獲得することができる。不参 gas 保証金についても同様で、ファーストパブリックレポーターがレポートしたアウトカムがマーケットのファイナルアウトカムになった場合にのみ獲得できる。

ファーストパブリックレポーターはマーケットのアウトカムをレポートする際、(没収されている不参保証金がステークされているため) 必ずしも所有する REP をステークする必要はない。このように、指名レポーターによるレポートが行われなかったマーケットは、公開レポーティングフェーズに入った瞬間誰かしらによって即時にレポートされることが期待できる。

イニシャルレポート *(initial report)* がイニシャルレポーター (指名レポーター、あるいはファーストパブリックレポーター) によって行われると、そのアウトカムはマーケットの暫定アウトカムとなり、マーケットは次の手数料期間開始待ちフェーズへと移行する (Figure. 2c)。

7. 次の手数料期間開始待ち

マーケットでイニシャルレポートが行われると、次の手数料期間開始待ちフェーズに入る (Figure. 2c)。このフェーズでは、現在の手数料期間が終了するまでレポーティングは保留状態となる。次の手数料期間が開始されると、マーケットは争議ラウンド *(Dispute Round)* フェーズに入る。

8. 争議ラウンド

争議ラウンド (Figure. 2d) は 7 日間あり、REP 保有者であればマーケットの暫定アウトカムに対して争議が行える。[10](争議ラウンド開始時の暫定アウトカムは、その後 REP 保有者による争議が無ければマーケットのファイナルアウトカムとなる)。争議とは、現在の暫定アウトカムとは異なるアウトカムに REP をステークすることである (この REP を争議ステーク *(dispute stake)* と呼ぶ)。争議ステークの合計額が、争議ラウンドで必要な争議保証金額 *(dispute bond size)* に達すれば、その争議は成功である。争議保証金額は次のようにして導出される。

A_n を、n 回目争議ラウンド開始時における、あるマーケットの全てのアウトカムの争議ステークの合計とする。ω を、この争議ラウンド開始時における、あるマーケットの暫定アウトカム以外のアウトカムとする。$S(\omega, n)$ を、n 回目争議ラウンド開始時における、ω に対する争議ステークの合計とする。すると、n 回目争議ラウンドで、暫定アウトカムに対抗してアウトカム ω で争議を成功させるために必要な争議保証金額は次の式で求められる。

$$B(\omega, n) = 2A_n - 3S(\omega, n) \tag{1}$$

争議保証金額をこのように設定した理由は、事実と異なるアウトカムに対して争議を行い、その結果争議を成功させたレポーターに対し見返りとして 50%の ROI を保証するためである (セクション II D を参照)。

争議保証金は、必ずしも一人のユーザーが全額を払う必要はない。Augur のプラットフォームでは不特定多数のユーザーで争議保証金を募ることができる。誤った暫定アウトカムを見つけたユーザーは、暫定アウトカム以外のアウトカムに REP をステークすることで争議を発動できる。もし、いずれかのアウトカム (暫定アウトカム以外のアウトカム) の争議ステークが、争議保証金となりえる程十分に集まった場合、現在の暫定アウトカムに対する争議が成功したと言える。

争議が成功すると、マーケットは次の争議ラウンド、あるいは、フォーク *(fork)* 状態に移行する (Figure. 2e)。争議保証金額が全 REP の 2.5%より大きくなると、マーケットはフォーク状態となる。争議保証金額が全 REP の 2.5%より小さい場合は、争議のために新たに選択したアウトカムが暫定アウトカムとなり、マーケットは次の争議ラウンドに移行する。

争議ラウンド中、全ての争議ステークはエスクローで保持される。もし争議ステークが争議を成功させるだけの額に達しなかった場合、争議ステークは争議ラウンド終了時に争議ステークの所有者へ返却される。もし、7 日間の争議ラウンドで争議が成功しなければ、マーケットはファイナライズ *(finalized)* 状態となり (Figure. 2f)、その時の暫定アウトカムがファイナルアウトカムとなる。つまり、マーケットのファイナルアウトカムとは、争議ラウンドを経たが争議失敗に終わった暫定アウトカム、または、フォークによって決定された暫定アウトカムのことである。Augur のコントラクトはこのファイナルアウトカムを真実 *(truth)* として扱い、それに従って支払いを行う。

争議に失敗した全ての争議ステークは、争議ラウンドが終了するたびに元の所有者へ返却される。争議に成功した全ての争議ステークは、支持したアウトカムに適用され、マーケットがファイナライズされるまで (または他のマーケットでフォークが発生するまで) その状態のままとなる。(争議の成功/失敗によらず) すべての争議ステークは、現在の手数料期間にあるレポーティング手数料プール[11] の一部を受け取る。

---

[10] 争議ラウンドと手数料期間が同時期であるのは、純粋に便利性の問題である。原理的には、争議ラウンドと手数料期間の期間が異なることは可能である。

[11] 手数料期間中に収集された決済手数料と有効性保証金は、手数料期間のレポーティング手数料プールに加算される。手数料期間の最後に、レポーティング手数料プールから、手数料期間中にステークした REP 量に応じた額がユーザーに支払われる。

9. フォーク

フォーク状態 (Figure. 2e) とは特殊な状態であり、最大 60 日間続く。フォークはマーケットの判決を下すための最終手段である。非常に破壊的なプロセスであり、発生することはほぼ無いと想定している。フォークが発生するのは、あるマーケットで争議保証金が全 REP の 2.5%に達した場合である。このマーケットのことを、フォーキングマーケット *(forking market)* と呼ぶ。

フォークが開始されると、そのフォーキング期間 *(forking period)* は 60 日[12] 続く。このフォーキング期間が終わるまで、ファイナライズされていない他の全マーケットは保留状態となる。REP 保有者と (ウォレット、取引所などの) サービス提供者がフォークに対応する十分な時間が確保できるよう、フォーキング期間は通常の手数料期間よりも長く設定している。また、フォークで決定したファイナルアウトカムを争議することはできない。

全てのマーケットと全ての REP トークンは、ユニバース *(universe)* に存在する。あるユニバースに存在する REP トークンは、同一のユニバースに存在するマーケットに対してのみ、その REP トークンでレポートを行うことができる (それにより手数料を獲得できる)。Augur がローンチされた直後、全てのマーケットと全ての REP はジェネシスユニバース *(genesis universe)* に存在する。

マーケットがフォークすると、新しいユニバースが生成される。フォークでは、フォーク対象のマーケットに存在するアウトカムの数だけ、新しいチャイルドユニバース *(child universe)* が生成される (セクション ID 2で述べているように、このアウトカムには無効 (Invalid) を含む)。例えば、ある“バイナリ”マーケットでは、A、B、無効の 3 つのアウトカムがあるとする。このバイナリマーケットがフォークすると、ユニバース A、ユニバース B、ユニバース Invalid の合計 3 つのチャイルドユニバースが生成される。生成直後は、これらのユニバースは空の状態であり、マーケットや REP トークンは含まれていない。

フォークが開始されると、ペアレントユニバース *(parent universe)* は永久的にロック *(locked)* される。ロック済みユニバースでは新しいマーケットを生成することはできない。ユーザーは、ロック済みユニバースにあるマーケットのシェアをトレードすることはでき、さらにイニシャルレポートも可能であるが、このユニバースではレポートに対する報酬は払われず、マーケットもファイナライズできない。ロック済みユニバース内のマーケットや REP トークンを利用可能にするためには、REP をいずれかのチャイルドユニバースに移行しなくてはならない。

ペアレントユニバースに存在する REP を保有するユーザーは、移行先のチャイルドユニバースを選択し、その REP を移行することができる。移行は不可逆で一方向であるため、この選択は慎重に検討する必要がある。チャイルドユニバース間での REP トークンのやり取りはできない。移行とは特定のマーケットのアウトカムに対する *REP* トークンの永久的なコミットメントである。それぞれのチャイルドユニバースに移行された REP トークンは、完全に分離されたトークンとみなすべきで、ウォレットや取引所などのサービス提供者もそのように取り扱うべきである。

フォークが開始すると、フォーキング期間中にチャイルドユニバースへの移行が自由に行えるように、フォーク対象でないマーケットにステークされている全ての REP は、そのステーク状態が解除 *(unstaked)* される。[13]

フォーキング期間終了時に最も REP が移行されたチャイルドユニバースがウィニングユニバース *(winning universe)* となり、そのユニバースに対応するアウトカムがフォークしたマーケットのファイナルアウトカムとなる。ペアレントユニバースにあるファイナライズされていないマーケットは、このウィニングユニバースにのみ移行され、そこでイニシャルレポートが行われると、次の手数料期間開始待ちフェーズにリセットされる。

ペアレントユニバースからチャイルドユニバースに対してトークンを移行させるにあたり、時間制限はない。トークンはフォーキング期間後に移行されるが、これらのトークンはユニバースの勝利決定には影響を与えない。フォーキング期間中の参加を促進するため、フォーク開始から 60 日以内に REP を移行させた保有者すべてに、移行先のチャイルドユニバースで 5%の REP を追加付与する[14]。この報酬は新しい REP トークンを生成することによって支払われる。[15]

フォーク対象のマーケットのアウトカムに対して *REP* をステークしたレポーターは、フォーク中にそのポジションを変更することはできない。　ペアレントユニバースのアウトカムにステークされた REP は、そのアウトカムに対応するチャイルドユニバースにしか移行できない。例えば、争議ラウンドにおいて、あるレポーターがアウトカム A が正しいアウトカムだと信じ、アウトカム A に対する争議保証金を支払った場合、フォーク中はユニバース A にのみ、その REP を移行することが可能である。

シブリングユニバース *(sibling universe)* は完全に分離されている。　あるユニバースに存在する REP トークンで、別のユニバースにあるマーケットをレポートすることは不可能であり、それによって報酬を得ることもできない。ユーザーは、信用できないオラクルが存在するユニバースでのマーケット作成やトレードを望まないと想定されるため、事実にそぐわないユニバースでは REP によって手数料を稼げる可能性は低くなる。その結果、そのユニバースの市場価値は大きくならないだろう。フォーク後、事実にそぐわないユニバースがウィニングユニバースになるか否かに関わらず、そのユニバースに移行した REP の市場価値は失われるだろう。このことはセキュリティ上重要な結論である。この件についてはセクション IIで考察している。

---

[12] フォーキング期間は 60 日間未満になることがある。フォーキング期間は、60 日経過するか、全 REP の 50%以上がチャイルドユニバースに移行すれば終了する。

[13] 唯一の例外は、イニシャルレポーターがイニシャルレポートでステークした REP である。他マーケットでフォークが発生してもこの REP はアウトカムへのステーク状態が継続され、フォーク後に最も REP が移行されたチャイルドユニバースに自動的に移行される。

[14] これは、全体の 50%以上の REP がいずれかのチャイルドユニバースに移行したことにより、早期にフォーキング期間が終了した場合でも発生する。

[15] この REP 追加発行の効果は小さい。例えば、全体の 20%にあたる REP がフォーキング期間中に移行されたとして、これによる追加発行は全体の 1 %に過ぎず、加えてフォークは非常に稀なイベントと予想されるためである。

10. ファイナライズ

フォークが完了する、または、暫定アウトカムに対する争議が成功しない状態で争議ラウンドが 7 日経過すれば、そのマーケットはファイナライズ状態 (Figure. 2f) に入る。フォークしたアウトカムに対して争議することは不可能であり、フォークしたアウトカムはフォーキング期間終了時にファイナライズしたとみなされ、トレーダーはすぐにそのマーケットでポジションを決済することができる。マーケットがファイナライズ状態になった時、選ばれたアウトカムをファイナルアウトカム *(final outcome)* と呼ぶ。

D. マーケットの決済

トレーダーは次の 2 つの方法のいずれかによりポジションを決済することができる。一つは、所有するシェアを通貨と交換して他のトレーダーに売却する方法、もう一つは、所有するシェアをそのマーケットで決済する方法である。前述の、合計 1ETH が Augur 上でエスクロー取引された時にコンプリートセットの一部としてシェアが生成された例を思い出してほしい。[6] エスクローから 1ETH 取り出すためには、トレーダーは Augur に対してコンプリートセットを提供するか、もしくはマーケットが既にファイナライズしているならば、ウィニングアウトカムのシェアを Augur に対して提供しなくてはならない。この交換が発生した時、トレーダーがマーケットコントラクトに対して決済した、と言う。

例として、アウトカム A と B が存在する未ファイナライズのマーケットを考えてみる。アリスはアウトカム A のシェアを保有しそれを 0.7ETH で売却したいと希望しており、ボブはアウトカム B のシェアを保有しそれを 0.3ETH で売却したいと希望しているとする。まず Augur はこれらのオーダーをマッチングし、参加者から A と B のシェアを収集する。その後 Augur はアリスに 0.7ETH(実際はここから手数料が差し引かれる) を与え、ボブに 0.3ETH(同様に手数料が差し引かれる) を与える。

二つ目の例として、ウィニングアウトカムが A とファイナライズされたマーケットを考えてみる。アリスはアウトカム A のシェアを保有しその換金を希望している。アリスはそのアウトカム A のシェアを Augur に送り、1ETH(手数料が差し引かれる) を受け取る。

1. 決済手数料

Augur では、参加者がマーケットコントラクトに対して決済した時にのみ手数料が課せられる。課せられる手数料は、作成者手数料とレポーティング手数料の 2 つである。これらの手数料は両方とも決済した額に比例する。従って、アリスが 0.7ETH、ボブが 0.3ETH 受け取った上記の未ファイナライズマーケットの例では、アリスは手数料の 70%、ボブは手数料の 30%を支払う。

作成者手数料はマーケット作成時に作成者により設定され、決済時にそのマーケット作成者に支払われる。レポーティング手数料は動的に設定され (セクション II C参照)、レポーティングに参加したレポーターに支払われる。

2. 無効マーケットの決済

ファイナルアウトカムが無効となったマーケットでは、マーケットコントラクトに対して決済を行ったトレーダーは各アウトカムのシェア毎で同額の ETH を受け取る。つまり、もし N 個のアウトカム (無効は含まない) があり、シェアのコンプリートセットの金額が C ETH だとすると、トレーダーは一つのシェアで C/N ETH を受け取る。[16]

3. *Reputation* の再配布

マーケットがフォークすることなくファイナライズした場合、ファイナルアウトカム以外にステークされた全ての REP は没収され、その没収された REP は、ファイナルアウトカムにステークした各ユーザーに対して、そのステークした REP 量に応じて再配布される。争議保証金額は、争議でファイナルアウトカムとなるアウトカムに争議ステークとしてステークされた REP が、報酬として ROI が 50%となるように決定される。[17] この報酬は、現実の結果にそぐわない暫定アウトカムがあった場合に、レポーターが争議を発動させるための強いインセンティブとなる。

II. インセンティブとセキュリティ

REP の時価総額と Augur のフォーキングプロトコルの信頼性の間には、強い関係性がある。REP の時価総額が十分に大きく[18]、攻撃者が経済的合理性を有する場合、フォークで勝利したアウトカムは客観的現実と合致するものになるはずである。実際には、指名レポーターや争議ラウンドの仕組みを使わなくても Augur は適切に機能するであろうし、フォーキングプロセスさえあればオラクルは誠実にレポートを行うだろう。

しかし、フォークは破壊的であり時間を浪費する。フォークは一つのマーケットで判決を下すまで最大 60 日かかり、さらに 1 度に 1 つのマーケットにしか処理できない。フォーク中のマーケットが判定される 60 日の間、ファイナライズされていない他の全マーケットは保留状態となる。[19] サービス提供者はサービスの更新が必要となり、REP 保有者は REP を新しいチャイルドユニバースに移行する必要がある。それゆえ、フォークは絶対に必要な場合のみ実施されるべきである。言うなれば、フォークの実行は核兵器を使用するようなものである。

首尾よく、フォークは真実を決定するために信頼できるものであるということが定着すれば、実際にフォークせず

---

[16] もしマーケットのアウトカムが無効でファイナライズした場合、技術的制約があるためトレードを簡単に取引前の状態に巻き戻すことはできない。アウトカムのシェアはただのトークンであり、ユーザー間で直接取引することができる。つまり、ETH とシェアは Augur の制御配下に無く、マーケットが無効にファイナライズしたからといって、これらを元の所有者に返却することはできない。

[17] Appendix.Aの定理 3参照。

[18] 詳細はセクション II A参照。

[19] トレーダーはこれらのマーケット上でトレードを続行することはできるが、マーケットのファイナライズはフォーキング期間が終わるまでできない。

ともインセンティブによって参加者を正直に行動するよう促すことができる。フォークとは信頼できる脅威であり、フォークが正しい判決を下すという信念は、*Augur* のインセンティブシステムの基盤となっている。

次に、フォーキングシステムが真実を決定できるための要件について説明する。ここでは、インセンティブシステムと、そのインセンティブシステムが如何にして迅速かつ正確に全マーケットの判決を下すことを促進するかを考察する。

A. フォーキングプロトコルの完全性

ここではフォーキングプロセスの確実性と信頼可能となる条件について説明する。以下では説明を簡単にするために、フォークについて言及する場合、チャイルドユニバースは客観的現実に合致した、トゥルー (`true`) ユニバースとし、それ以外のチャイルドユニバースは事実とは異なる、フォルス (`false`) ユニバースとする。また、最も REP が移行されるチャイルドユニバースをウィニングユニバースとし、それ以外のチャイルドユニバースはルージングユニバース *(losing universe)* とする。

当然、我々はトゥルーユニバースがウィニングユニバースとなり、フォルスユニバースはルージンズユニバースになることを望んでいる。仮にフォーキングプロトコルへの攻撃が成功し、その結果、フォルスユニバースがウィニングユニバースになってしまった場合、そのフォーク対象のマーケットから (潜在的には未ファイナライズのマーケットからも) 不正な支払いが行われることになるだろう。

我々は、攻撃するために必要となる最低限のコストよりも、攻撃の成功により得られる最大利益を小さくすることで、オラクルを保護しようと取り組んでいる。このことを以下に成文化する。

1. 攻撃者の最大利益

オラクルへの攻撃が成功した場合、未ファイナライズのマーケットはフォルスユニバースに移行される。もし攻撃者がフォルスユニバースで大多数の REP をコントロールできるのであれば、未ファイナライズのマーケットを思い通りの判決結果にすることができる。最も極端なケースでは、未ファイナライズマーケットでエスクロー取引されている資金全てを攻撃者が獲得することとなる。[20]

定義 1. Augur の未ファイナライズなマーケット内でエスクローされている資金の合計額を、Augur のネイティブ未決済建玉 *(native open interest)* と定義し、I_a で示す。[21]

定義 2. Augur に対して一切レポーティング手数料を支払わないが、Augur のマーケットの判決結果に従い、自身のマーケットの判決を下すマーケットのことを、寄生的マーケット *(parasitic market)* と定義する。

定義 3. Augur のマーケットに連動して判決を下す寄生的マーケットでエスクローされている資金の合計額を、寄生的未決済建玉 *(parasitic open interest)* と定義し、それを I_p で示す。

最も極端なケースでは、攻撃者は全寄生的マーケットの全資金を獲得可能である。

観察 1. オラクルへの攻撃が成功した攻撃者の最大利益 (グロス値) は、$I_a + I_p$ である。

2. 寄生的未決済建玉の不可知性

Augur の I_a を正確かつ効率的に測定することは可能である。しかし、一般に I_p は不可知である。なぜならば、オフラインな寄生的マーケットはランダムに多数存在し、それらのマーケットの未決済建玉の額もまたランダムであるためである。攻撃者の最大利益に不可知な値である I_p を含むため、オラクルは経済的合理性を持つ者からの攻撃に対して安全であるという客観的な確信を得ることは不可能である。

しかし、実際には I_p に合理的制限があると仮定すれば、オラクルは安全であるという条件を定義できる。

3. 攻撃成功のための最小コスト

次に、オラクルを攻撃するためのコストについて考察する。REP の価格を P とする。attorep を ϵ とする[22]。現存する REP の総量 (REP の “マネーサプライ“) を M とする。フォーキング期間中にトゥルーユニバースに移行される M の割合を S とする。

すると、積 SM はフォーキング期間中にトゥルーユニバースに移行する REP の総量となり、さらに積 PM は REP の時価総額となる。

攻撃者が選択したフォルスユニバースに対して移行した REP の価格を P_f とする。$P \leq P_f$ の場合、REP を移行しないことよりも、REP をフォルスユニバースに移行することの方が有益となるため、オラクルは経済的合理性を持つ攻撃者に対して安全とは言えない。

4. 完全性

仮定 1. 攻撃者でないレポーターは、フォーク中にフォルスユニバースに *REP* を移行しないものとする。[23]

設計上、オラクルに対する攻撃を成功させるには、フォーキング期間中にトゥルーユニバースよりも多い REP をフォルスユニバースに移行する必要がある。仮定より、攻撃者のみがフォルスユニバースに REP を移行したとする。す

[20] 攻撃者はいくつかのアウトカムの全てのシェアを獲得し、強制的にマーケットをそのアウトカムにファイナライズする必要がある。

[21] これには Augur へレポーティング手数料を支払う外部市場が含まれる。

[22] 1 *attorep* は 10^{-18} REP。

[23] 偶然や不注意によって、悪意のないレポーターがフォルスユニバースに REP を移行する可能性はあるが、そのレポーターが攻撃者の共犯者か否かは判別できない。

ると、フォーキング期間中にトゥルーユニバースに移行されたREP量は、SMで示すことができる。従って、攻撃を成功させるためには、少なくとも$SM+\epsilon$ REPを移行する必要がある。単純化するためϵは無視できる程小さい値とすると、攻撃を成功させるためには少なくともSM REPを、フォルスユニバースに移行する必要がある。

攻撃者がフォーキング期間中にSM REPを移行した場合、攻撃者は移行先であるチャイルドユニバースでSM REPを受け取ると考えられる。[24] もし、攻撃者がフォルスユニバースに移行したとすると、それらのコインの価値はSMP_fとなる。故に、攻撃の成功に必要な最小コストは$(P-P_f)SM$である。

観察 2. フォーク中に、攻撃者がフォルスユニバースに移行するREPの最小量はSMであり、その移行には$(P-P_f)SM$のコストがかかる。

$S>\frac{1}{2}$の場合は、フォルスユニバースがウィニングユニバースとなるための十分なREPがトゥルーユニバース以外のユニバースに存在しないため、攻撃は不可能である点に注意してほしい。

経済的合理性のある攻撃者に対抗するため、攻撃の成功に必要な最小コストよりも最大利益の方が小さい場合、オラクルは客観的現実に一致するアウトカムを選択するだろう。観察1、2より、$S>\frac{1}{2}$、または、$I_a+I_p<(P-P_f)SM$を満たす限り、必ずこの状況となる。このことから以下の完全性の公式定義が得られる。

定義 4. (完全性の性質) フォーキングプロトコルは、$S>\frac{1}{2}$、または、$I_a+I_p<(P-P_f)SM$、であれば常に完全性がある。

上記の不等式から、フォーキングプロトコルの完全性とREPの時価総額PMの関係性を求めることができる。

定理 1. *(*時価総額の安全性定理*)* フォーキングプロトコルに完全性があるための必要十分条件は、以下である。

1. $S>\frac{1}{2}$、または
2. $P_f<P$、かつ、*REP*の時価総額が$\frac{(I_a+I_p)P}{(P-P_f)S}$より大きい。

Proof. フォーキングプロトコルに完全性があると仮定すると、定義より、$S>\frac{1}{2}$または$I_a+I_p<(P-P_f)SM$である。$I_a+I_p<(P-P_f)SM$とすると、$I_a+I_p\geq 0$かつ$SM>0$であるため、$P_f<P$である. $I_a+I_p<(P-P_f)SM$よりPMを求めると、$\frac{(I_a+I_p)P}{(P-P_f)S}<PM$となり、一方向目が証明された.

次に、$S>\frac{1}{2}$、または、$P_f<P$かつ$\frac{(I_a+I_p)P}{(P-P_f)S}<PM$とする。$S>\frac{1}{2}$の場合、定義よりフォーキングプロトコルに完全性がある。さらに、$P_f<P$かつ$\frac{(I_a+I_p)P}{(P-P_f)S}<PM$の場合、$I_a+I_p$を求めると、$I_a+I_p<(P-P_f)SM$となるため、逆方向も証明された。 □

[24]実際には、フォーク開始から60日以内に移行するとボーナスとして5%付与されるため、チャイルドユニバースで受け取るREPは、$1.05SM$ REPとなる。ここでは考察を簡単にするため、5%のボーナスは無視する。詳細はAppendix.Cを参照。

B. 仮定とその帰結

トレーダーは、虚偽のレポートが行われるユニバースではトレードを望まないと考えられる。また、マーケット作成者は、トレーダーが存在しないユニバースではマーケットの作成を望まないと考えられる。このようなマーケットやトレードが存在しないユニバースでは、REP保有者に対していかなる配当も提供されない。故に、フォルスユニバースに移行されたREPは市場価値を失い、これを$P_f=0$でモデル化する。

フォーキング期間中に、存在するREPの少なくとも20%はトゥルーユニバース移行すると考えられるため、これを$S\geq\frac{1}{5}$でモデル化する。また、ネイティブ未決済建玉の50%に及ぶ寄生的未決済建玉に対応するため、$I_a\geq 2I_p$とする。

これらの前提の下、定理1より、REPの時価総額がネイティブ未決済建玉の7.5倍以上であれば、フォーキングプロトコルに完全性があるといえる。[25]

C. 時価総額ナッジ

AugurはREPの価格に関する情報を、現実世界で起こる他の情報と同じ手法、つまりAugurのマーケットから取得する。これにより、Augurは自身でREPの時価総額を算出することができる。また、Augurは現在のネイティブ未決済建玉を取得することもできるため、Augurの完全性要件を満たすための時価総額が決定できる。

全てのユニバースにおいて、そのユニバース開始時のレポーティング手数料は1%である。もし現在の時価総額が目標値よりも低い場合、レポーティング手数料は自動的に増加する (ただし33%を超過することはない) ことで、REPの価格に対して上昇圧力を、新たなネイティブ未決済建玉に対しては下降圧力をかける。反対に、現在の時価総額が目標値よりも高い場合、トレーダーがシステムを安全に保つための手数料を必要以上に支払わなくていいよう、レポーティング手数料は自動的に減少する (ただし0.01%を下回ることはない)。

レポーティング手数料は次のようにして決定する。直前の手数料期間でのレポーティング手数料をr、目標の時価総額をt、現在の時価総額をcとすると、現在の手数料期間のレポーティング手数料は、$\max\left\{\min\left\{\frac{t}{c}r,\frac{333}{1000}\right\},\frac{1}{10{,}000}\right\}$となる。

D. フォークの脅威を活用する

前述したように、フォークとは破壊的でマーケットをファイナライズするためには時間を要する。全てのマーケットをフォークで判決するのではなく、フォークの脅威を有効に活用してマーケットの判決を行う。

争議でファイナルアウトカムに賛成票を投じた場合、争議ステークに対して50%のROIが報酬として得られるこ

[25]代替的な仮説とその帰結については、Appendix.B参照。

とを思い出してほしい。[26] フォーク発生時、事実と異なるアウトカムにステークされた REP は無価値となり、反対に、事実と一致するアウトカムにステークされた REP はチャイルドユニバースで 50%以上の REP が報酬として与えられる。それゆえにフォークに突入すれば、事実と異なるアウトカムを争議して正しいアウトカムに賛成票を投じた REP 保有者は常には優位性があり、事実と異なるアウトカムに賛成票を投じた REP 保有者の REP は経済的価値を失うだろう。

我々は、このような背景から、事実と異なる全ての暫定アウトカムは必ず争議の対象になると確信している。

III. 潜在的問題と危険性

A. 寄生的マーケット

寄生的マーケットとは、Augur に対してレポーティング手数料の支払いはないが、ネイティブな Augur のマーケットの判決結果に従い判決を下すマーケットであった。寄生的マーケットは手数料の支払い対象となるレポーターは存在せずに Augur と同様のサービスを低い手数料で提供できる。これはフォーキングプロトコルの完全性に深刻な影響を及ぼす可能性がある。特に、Augur にあったトレードの関心を寄生的マーケットが奪う場合、Augur のレポーターが受け取るレポーティング手数料は少なくなるだろう。これは REP 時価総額の下降圧力となる。REP 時価総額が低すぎるとフォーキングプロトコルの完全性は危険にさらされる (定理 1)。その結果、寄生的マーケットは Augur の長期生存性を脅かす可能性があり、Augur はこのことには激しく抵抗しなくてはならない。

この寄生的マーケットに対する最善の防衛策の一つは、Augur 上で寄生的マーケットを稼働させた際の報酬を最小限に抑えるために、(オラクルの完全性を持続させつつも) プラットフォームである Augur でのトレーディングをできるだけ安くすることである。

B. 未決済建玉のボラティリティ

ポピュラーなスポーツイベント期間中にみられるような、大きく、急で、予測できない未決済建玉の増加は、フォーキングプロトコルの完全性の要件である時価総額の急激な増加につながる (定理 1)。その時点の時価総額が時価総額要件に満たない場合、経済的合理性を持つ攻撃者によって誤った判決に導くためのフォークが引き起こされる危険性がある。これを防ごうと Augur は時価総額を上昇させようと試みるが (セクション II C参照)、これらの試みは反動的であり 7 日間の手数料期間毎に 1 回しか調整されない。

しかしながら注目すべき点は、未決済建玉の急激な増加を目の当たりにしている投機家は、この時価総額の反動ナッジを見越して REP を購入する可能性があり、その結果、おそらくフォーキングプロトコルの完全性が脅かされなくなるまで時価総額が上昇する。従って、攻撃者はオラクルの脆弱な期間を利用して攻撃を成功させるだけの十分な時間は取れないだろう。

[26] ファイナルアウトカムに一致するユニバースに存在する REP で測定される件については、Appendix.Aの定理 3を参照。

C. 不整合あるいは悪意のある判決ソース

マーケット作成時、作成者はレポーターがアウトカムを決定するための判決ソースを選択する。もしマーケット作成者が不整合または悪意のある判決ソースを選択した場合、正直なレポーターは資金を失う可能性がある。

例えば、セレナというマーケット作成者が、アウトカム A、B の 2 つあるマーケットを作成し、判決ソースとして彼女のウェブサイト attacker.com を選択、指名レポーターに彼女自身を設定したとする。マーケットのイベント終了後、指名レポーターである彼女はアウトカム A をレポートし、attacker.com の内容をアウトカム B が正しいアウトカムであるかのように書き換える。正直なレポーターは attaker.com をチェックするとイニシャルレポートが正しくないと認識した後、最初の争議ラウンドで暫定アウトカムに対する争議を起こし、その争議の結果、首尾よくアウトカム B が正しいという結果になったとする。その後セレナは attacker.com の内容をアウトカム A が正しいアウトカムであるかのように書き換え、マーケットは 2 回目争議ラウンドに突入する。再度、レポーターは attacker.com をチェックし、暫定アウトカムであるアウトカム B は正しくないと認識するため、その争議は成功し、アウトカム A が正しいという結果になる。セレナはマーケットがファイナライズするまでこれを繰り返す。このような行為によって、マーケットがどのように判決を下しても正直なレポーターは資金を失うこととなる。

この攻撃にはいくつかのバリエーションが存在する。このようなマーケットはフォークを引き起こす原因となり、全ての REP 保有者が REP の移行先となるチャイルドユニバースを選択する作業が発生するため、単純に疑わしい判決ソースのマーケットを無視するだけでは不十分である。レポーターは疑わしい判決ソースのマーケットに対して警戒を続けなくてはならない。そのようなマーケットはレポーターが連携して、確実に無効にファイナライズするよう、公の場で特定されなくてはならない。

D. オラクルへの自己言及型クエリ

Augur のオラクルの未来における行動を予測するマーケットは、オラクル自身の行動に望ましくない影響を及ぼす可能性がある [11]。例えば、“2018 年 12 月 31 日以前の 3 日間のレポート期間において、いずれかの指名レポーターがレポート提出を行わないか?”というマーケットを考えてみる。このマーケットにおける No への賭けは、指名レポーターが意図的にレポートを行わないインセンティブとなる。また、もし指名レポーターが不参保証金を補填可能なほど安価な Yes のシェアを買い占めることができるならば、その指名レポーターは意図的にレポートを行わないだろう。

REP の時価総額が十分に大きければ (定理 1)、このオラクルに対する自己言及型クエリがフォーキングプロトコルの完全性を脅かすものにはならないだろう。しかし、マー

ケットのファイナライズの遅延を引き起こし、Augur のパフォーマンスを悪化させる可能性がある。マーケットは正しくファイナライズされるが、こういった挙動は破壊的で望ましくない。

E. フォーク参加の不確実性

フォーク期間中にどれぐらいの REP がトゥルーユニバースに移行されるかを事前に知ることはできないため、オラクルが完全性を持つのに十分な時価総額であるか (定理 1) を事前に知ることはできない。私たちのフォーキングプロトコルの完全性に対する信仰は、フォーク期間中に正直な参加者が最低何名集まるかという仮定に対する信仰ほど強くはない。フォーキング期間中に少なくとも 20%の REP がトゥルーチャイルドユニバースに移行すると仮定しているが、この保証はない。

Augur のフォークは、次の点でブロックチェーンのフォークとは大きく異なる。ブロックチェーンの場合フォーク後であれば、ペアレントチェーンのコイン所有者はフォークしたチェーンのコインを含め、両方のコインを所有することになる。リプレイアタックを無視すると、ブロックチェーンのフォークはユーザーに対してほとんどリスクがない。これ対して Augur のフォークの場合、REP を保有するユーザーはその REP をペアレントユニバースからたった一つのチャイルドユニバースに移行しなくてはならない。REP をコンセンサスを得たユニバース以外に移行した場合、その REP は全ての価値を失うだろう。よって、フォーキング期間中の REP の移行は、どのチャイルドユニバースがコンセンサスを得たか明確になるまで、ユーザーを危険にさらす。そのリスクはフォーキング期間中の参加を阻害する可能性がある。

このリスクを補い、フォーキング期間中に参加を促進するために、フォーク開始から 60 日以内に REP を移行した全 REP 保有者に対して、移行先のチャイルドユニバースで 5%の REP を付与する (セクション I C 9参照)。しかし、この 5%のボーナスがリスクを補うのに十分な数字であり、フォーキング期間中の参加を促すものであるかは定かではない。

F. 不明瞭あるいは主観的なマーケット

Augur のマーケットは、イベントのアウトカムを客観的に知ることができる場合にのみ、その使用に適している。 – 例えば、不明瞭または主観的なマーケット、あるいはアウトカムがイベント終了日になってもわからないようなマーケット – これらのマーケットは、Augur のプラットフォームに適していないため、無効とレポートされるであろう。マーケットが無効と判決されれば、トレーダーには全てのアウトカムで平等な金額が支払われる。スカラーマーケットであればマーケットの最高価格と最低価格の中間の金額が支払われる。

あるレポーターはアウトカム `A` が正しい、別のレポーターはアウトカム `B` が正しいと確信するような、レポーターの判断が割れてしまうマーケットもあり得る。例えば 2006 年に TradeSports は、2006 年 7 月末までに北朝鮮が領空外に着弾する弾道ミサイルを発射するか、という予測市場を公開した。2006 年 7 月 5 日、北朝鮮は領空外への弾道ミサイル着弾を成功させ、このイベントは米国政府の情報筋と世界中のメディアから幅広くレポートされた。しかし、TradeSports の契約にあった 米国国防総省による認定は無かった。Tradesports はこの契約の条件が満たされていないとの結論を下し、それに応じて支払いを行った。[27]

のケースでは、– ミサイルの発射予測 –というマーケットの魂は満たされたが、– 米国国防総省が発射を認めるか– というマーケットの字義は満たされなかった。TradeSports は集権化されたウェブサイトであり、一方的にマーケットのアウトカムを宣言することができた。同じことが Augur で起きた場合、マーケットがどのように判定されるべきかという考え方は REP 保有者それぞれで異なり、各自の考えに従って REP をステークするだろう。最悪の場合、複数のチャイルドユニバースの REP に価値が付くようなフォークとなるだろう。

ACKNOWLEDGMENTS

有益なご意見、ご提案をしていただいた Abraham Othman、Alex Chapman、Serena Randolph、Tom Haile、George Hotz、Scott Bigelow、Peronet Despeignes に感謝します。

[1] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspectives*, 18(2):107–126, 2004.
[2] James Surowiecki. *The Wisdom of Crowds*. Anchor, 2005.
[3] R. Hanson, R. Oprea, and D. Porter. Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, 60(4):449–459, 2006.
[4] D.M. Pennock, S. Lawrence, C.L. Giles, and F.A. Nielsen. The real power of artificial markets. *Science*, 291:987–988, 2001.
[5] C. Manski. Interpreting the predictions of prediction markets. *NBER Working Paper No. 10359*, 2004.
[6] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. *NBER Working Paper No. 10359*, 2005.
[7] S. Goel, D.M. Reeves, D.J. Watts, and D.M. Pennock. Prediction without markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 357–366. ACM, 2010.
[8] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*, 2008.

[27] 詳細は、`https://en.wikipedia.org/wiki/Intrade#Disputes` を参照。

[9] V. Buterin. A next generation smart contract and decentralized application platform. *https://github.com/ethereum/wiki/wiki/White-Paper*, 2013.

[10] J. Clark, J. Bonneau, E.W. Felten, J.A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS '14: Proceedings of the 10^{th} Workshop on the Economics of Information Security*, June 2014.

[11] A. Othman and T. Sandholm. Decision rules and decision markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, pages 625–632. International Foundation for Autonomous Agents and Multiagent Systems, 2010.

[12] J. Peterson and J. Krug. Augur: a decentralized, open-source platform for prediction markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014.

Appendix A: ファイナライズ所要時間と再配布

まず初めに、表記法、定義、観察について述べる。

定義 5. 任意のマーケット M において、M のアウトカム空間 (またはアウトカム一式) を、Ω_M とする。

定義 6. $n \geq 1$、かつ、$\omega \in \Omega_M$ の時、n 回目争議ラウンド開始時のアウトカム ω への争議ステーク総額を、$S(\omega, n)$ とする。これには、前の争議ラウンドで ω に賛成票を投じた全ての争議保証金を含む。

定義 7. $n \geq 1$、かつ、$\omega \in \Omega_M$ の時、n 回目争議ラウンド開始時の ω を除いた Ω_M の全アウトカムへの争議ステーク総額を、$S(\overline{\omega}, n)$ とすると、次の式が成り立つ。

$$S(\overline{\omega}, n) = \sum_{\substack{\gamma \in \Omega_M \\ \gamma \neq \omega}} S(\gamma, n)$$

定義 8. $n \geq 1$ の時、n 回目争議ラウンド開始時の M の全アウトカムに対する争議ステークを A_n とすると、次の式が成り立つ。

$$A_n = \sum_{\omega \in \Omega_M} S(\omega, n)$$

観察 3. 以上から、$A_n - S(\omega, n) = S(\overline{\omega}, n)$ が成立する。

定義 9. $n \geq 1$ の時、n 回目争議ラウンド開始時の暫定アウトカムを $\hat{\omega}_n$ とする。例えば、$\hat{\omega}_1$ はイニシャルレポーターによってレポートされたアウトカムである。

定義 10. $n \geq 1$、かつ、$\omega \neq \hat{\omega}_n$ の時、n 回目争議ラウンドでアウトカム ω を争議で成功させるために必要な争議保証金額を、$B(\omega, n)$ とする。

$\omega \neq \hat{\omega}_n$ の時、n 回目争議ラウンドでアウトカム ω を争議で成功させるために必要な争議保証金額は、式 1より、$B(\omega, n) = 2A_n - 3S(\omega, n)$ である。

観察 4. n 回目争議ラウンドでアウトカム ω を争議で成功させるための争議保証金が集まった場合、$S(\omega, n+1) = B(\omega, n) + S(\omega, n)$ が成り立つ。これはつまり、n 回目争議ラウンド終了時点においてアウトカム ω での争議が成功した場合、このアウトカム ω に対する争議ステークのみが、次の争議ラウンドでアウトカム ω の争議ステークとして適用されるということを意味する。

観察 5. 全ての $\omega \neq \hat{\omega}_n$ において、$S(\omega, n-1) = S(\omega, n)$ が成り立つ。つまり、アウトカム ω を争議で成功させるための争議保証金が集まらなければ、次回の争議ラウンド開始時にアウトカム ω の争議ステークは加算されない。これは、失敗した争議の争議ステークは争議ラウンド開始時にユーザーに返却されるためである。

観察 6. 全ての $n \geq 2$ において、$A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$ が成り立つ。これは、ある争議ラウンド開始時における全アウトカムの争議ステークの合計は、前回の争議ラウンド開始時の争議ステークの合計とその争議ラウンドで争議に成功した争議保証金の和であることを意味する。これ以外のすべての争議ステークは、前回の争議ラウンド終了時にユーザーに返却される。

補助定理 2. $n \geq 2$ において、$S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$ である。

Proof. $n \geq 2$ である n 回目争議ラウンドに突入した場合、$n-1$ 回目争議ラウンドのアウトカム $\hat{\omega}_{n-1}$ は、$\hat{\omega}_n$ として争議されるはずである。式 1より、争議保証金の大きさは $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$ である。これに観察 3を用いると、次のように書き換えられる。

$$B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = 2S(\overline{\hat{\omega}_n}, n-1) \quad \text{(A1)}$$

$n-1$ 回目争議ラウンドにおいて争議保証金は目標額に達成しているため、観察 4の式は $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$ と書き換えられる。観察 5より、争議ラウンドが $n-1$ から n に変わっても $\overline{\hat{\omega}_n}$ に対する争議ステークに変化が無いことが分かり、$2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$ と書き換えられる。これらの式を、式 A1に代入すると、$S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$ が導出される。 □

定理 3. 他のマーケットのフォークにより中断される場合を除き、争議でファイナルアウトカムに賛成票を投じた *REP* 保有者は、自身が投じた争議ステークに対して *50%* の *ROI(*これはファイナルアウトカムに一致するユニバースに存在する *REP* で計算される*)* で報酬を受け取る。

Proof. フォークでファイルアウトカムとなったアウトカムに争議保証金を投じた全てのユーザーは、その争議ステークがチャイルドユニバースに移行された時に、(フォーク中にコインが作成されることによって) その争議ステークに対して 50%のリターンを得る。従って、対象のマーケットでフォークが発生する場合は即座に真であると言える。

次に、、他のマーケットのフォークによるレポーティング中断は無く、自身のマーケットもフォークが発生せずにファイナライズした場合を考える。

$n \geq 2$ である n 回目争議ラウンド終了時にマーケットがファイナライズし、そのマーケットのファイナルアウトカムが ω_{Final} であったとする。これは、n ラウンド目の暫定アウトカムは ω_{Final} であり、n ラウンド目でアウトカムの争議は行われなかったことを意味する。言い換えると、$\hat{\omega}_n = \omega_{\text{Final}}$ であり、補助定理 2より、$S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$ である。

n ラウンド終了時にマーケットがファイナライズすると、いずれのアウトカムに対しても争議ステークが加算されることはないため、上記の等式において、マーケットのファイナルアウトカムへの争議ステーク合計は ω_{Final} であり、それ以外のアウトカムへの争議ステーク合計は $\overline{\omega_{\text{Final}}}$ である。ファイナルアウトカムへの争議ステークが、それ以外のアウトカムの争議ステークの 2 倍と等しいことに注意してほしい。

Augur は、ω_{Final} への争議ステーク量に比例して、ファイナルアウトカム以外への争議ステークを再配布する。ゆえに、争議で ω_{Final} に賛成票を投じたユーザーは、ステークした REP に対して 50%の ROI で報酬を受け取る。 □

次に、マーケットがファイナライズに必要とする争議ラウンドの最大回数を考察する。最大の争議ステークで争議ラウンドが開始され、ω が非暫定アウトカムである時、式 1は最小値となる。補助定理 2より、最大の争議ステークである非暫定アウトカムは、直前の争議ラウンドでは暫定アウトカムであった。ゆえに、$n \geq 2$ である n 回目争

議ラウンドで争議を成功させるための争議保証金の最小値は、$B(\hat{\omega}_{n-1}, n)$ である。

言い換えると、同じ 2 つのアウトカムが交互に争議を繰り返す場合、争議保証金の増加は**最も遅くなる**。このことから、マーケットがフォークを開始するために必要な争議ラウンドの回数は、同じ 2 つのアウトカムが交互に争議を繰り返す場合に**最大となる**。同じ 2 つのアウトカムが交互に争議を繰り返すケースの争議ラウンドの最大数を求めれば、フォーク開始までにマーケットが取り得る最大の争議ラウンド数を求めることができる。これを考察してみよう。

全ての争議保証金は、前回の争議ラウンドの暫定アウトカムに対してその額を満たし、同じ 2 つのアウトカムが交互に争議を繰り返し、そのアウトカムの一つを $\hat{\omega}_1$、もう一つを $\hat{\omega}_2$ とする。

観察 7. 同じ 2 つのアウトカムが交互に争議を繰り返す場合、$n \geq 3$ において、$\hat{\omega}_n = \hat{\omega}_{n-2}$ が成り立つ。

定義 11. イニシャルレポート中に、$\hat{\omega}_1$ にステークされた REP を d とする。この状況では、各ラウンドの暫定アウトカムは既知であるため、争議保証金の表記を単純化できる。n 回目ラウンドで必要とされる争議保証金を B_n とすると、$B_1 = 2d$ であり、$n \geq 2$ において $B_n = B(\hat{\omega}_{n-1}, n)$ である。このことは以下の読解の助けとなるであろう。

観察 8. 同じ 2 つのアウトカムが交互に争議を繰り返すケースでは、$n \geq 3$ において、$S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ が成り立つ。(すなわち、争議に成功した際の争議保証金は同じアウトカムに争議ステークとして加算されていく。)

補助定理 4. 同じ *2* つのアウトカムが交互に争議を繰り返す場合、$n \geq 3$ を満たす全ての n で、以下が成立する。

1. $S(\hat{\omega}_{n-1}, n) = \frac{2}{3}B_{n-1}$
2. $A_n = 2B_{n-1}$ かつ
3. $B_n = 3d2^{n-2}$

Proof. (n の帰納法による)

同じ 2 つのアウトカムが交互に争議を繰り返すケースを考える。

(基底ケース) 定義と式 1より次が成り立つ。

- $S(\hat{\omega}_1, 1) = d$, $S(\hat{\omega}_2, 1) = 0$, $A_1 = d$, and $B_1 = 2d$
- $S(\hat{\omega}_1, 2) = d$, $S(\hat{\omega}_2, 2) = 2d$, $A_2 = 3d$, and $B_2 = 3d$
- $S(\hat{\omega}_1, 3) = 4d$, $S(\hat{\omega}_2, 3) = 2d$, $A_3 = 6d$, and $B_3 = 6d$

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$ であるため、$n = 3$ の場合、補助定理の 1 番目の式は成り立つ。

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$ であるため、$n = 3$ の場合、補助定理の 2 番目の式は成り立つ。

$B_3 = 6d = 3d2^{3-2}$ であるため、$n = 3$ の場合、補助定理の 3 番目の式は成り立つ。

したがって、この補助定理は n=3 の基底ケースにおいて真である。

(帰納法) この補助定理が、$3 \leq n \leq k$ である全ての n において成り立つと仮定すると、$n = k + 1$ の場合に成り立つことを示せばよい。すなわち以下が成立することを示せばよい。

(a) $S(\hat{\omega}_k, k+1) = \frac{2}{3}B_k$

(b) $A_{k+1} = 2B_k$ かつ

(c) $B_{k+1} = 3d2^{k-1}$

まず、(a) が成り立つことを証明する。観察 8より

$$S(\hat{\omega}_k, k+1) = S(\hat{\omega}_k, k-1) + B_{k-1}$$

である。観察 7より、上記は以下の式に書き換えられる。

$$S(\hat{\omega}_{k-2}, k+1) = S(\hat{\omega}_{k-2}, k-1) + B_{k-1}$$

仮定より、右辺の $S(\hat{\omega}_{k-2}, k-1)$ を $\frac{2}{3}B_{k-2}$ に置き換えると以下となる。

$$S(\hat{\omega}_{k-2}, k+1) = \frac{2}{3}B_{k-2} + B_{k-1}$$

仮定より、B_{k-2} を $3d2^{k-4}$ とし、B_{k-1} を $3d2^{k-3}$ に置き換えると以下となる。

$$S(\hat{\omega}_{k-2}, k+1) = d2^{k-1}$$

観察 7より、右辺を書き換えると以下となる。

$$S(\hat{\omega}_k, k+1) = d2^{k-1}$$

仮定とこれら上記の等式により、$S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$ が言えるため、(a) が成り立つことが証明できた。

次に、(b) が成り立つことを証明する。観察 6より以下が成り立つ。

$$A_{k+1} = A_k + B_k$$

仮定より、$A_k = 2B_{k-1}$ であるため以下となる。

$$A_{k+1} = 2B_{k-1} + B_k$$

仮定より、$B_{k-1} = 3d2^{k-3}$ であるため、右辺を単純化すると以下となる。

$$A_{k+1} = 3d2^{k-2} + B_k$$

仮定より、$B_k = 3d2^{k-2}$ であるため、右辺を書き換えると以下となる。

$$A_{k+1} = 2B_k,$$

以上で (b) が成り立つことが証明された。

最後に (c) が成り立つことを証明する。式 1より以下が言える。

$$B_{k+1} = 2A_{k+1} - 3S(\hat{\omega}_k, k+1)$$

観察 8より、$S(\hat{\omega}_k, k+1)$ は $S(\hat{\omega}_k, k-1) + B_{k-1}$ であるため以下となる。

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_k, k-1) + B_{k-1}\right)$$

観察 7より、$\hat{\omega}_k = \hat{\omega}_{k-2}$ であるため以下となる。

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

観察 6より、$A_{k+1} = A_k + B_k$ であるため以下となる。

$$B_{k+1} = 2\left(A_k + B_k\right) - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

仮定より、$A_k = 2B_{k-1}$ かつ $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$ であるため以下となる。

$$B_{k+1} = 2\left(2B_{k-1} + B_k\right) - 3\left(\tfrac{2}{3}B_{k-2} + B_{k-1}\right)$$

仮定より、$B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ かつ $B_{k-2} = 3d2^{k-4}$ である。これらを代入し単純化すると以下となる。

$$B_{k+1} = 3d2^{k-1}$$

以上で (c) が成り立つことが証明され、補助定理が証明された。 □

定理 5. 他マーケットのフォーク発生による妨げが無ければ、与えられたマーケットがファイナライズまたはフォーク発生するまでに最大 *20* 回の争議ラウンドを経る可能性がある。

Proof. 与えられたマーケットは、他のマーケットのフォーク発生による妨げが無いと仮定する。前述の通り、同じ 2 つのアウトカムが交互に争議を繰り返す場合、フォークを発生させる争議ラウンドの回数は最大となる。補助定理 4の 3 番目の式より、この状況において n 回目ラウンドで暫定アウトカムを争議で成功させるために必要な争議保証金額は、$3d2^{n-2}$ である。この時、d はイニシャルレポートでステークされた REP である。

REP は 1100 万 REP 存在し、少なくともこの全 REP の 2.5%が争議保証金として集まればフォークが発生する。つまり、争議保証金が 275, 000 REP 集まればフォークは発生する。また、イニシャルレポートでステークされる REP の最小額は 0.35 REP[28] であるため、$d \geq 0.35$ REP である。

以上から、$n \in \mathbb{Z}$ における $3(0.35)2^{n-2} > 275{,}000$ を求めると、$n \geq 20$ となる。従って、マーケットがファイナライズあるいはフォーク発生するまでに最大 20 回の争議ラウンドを経る可能性があると言える。 □

Appendix B: もう一つの前提とその結果

以下のことを思い出してほしい。

- S は、フォーク期間中にトゥルーユニバースに移行した REP の割合である。
- P は、トゥルーユニバースに移行した REP の価格である。
- P_f は、攻撃者が選択したフォルスユニバース (Flase universe) に移行した REP の価格である。
- I_a は、Augur のネイティブ未決済建玉である。
- I_p は、寄生的未決済建玉である。

Augur では、目標の時価総額に到達するために、S、P_f、I_p についてある前提を設けている。その前提とは、フォーキング期間中に存在する REP の最低 20%がトゥルーユニバースへ移行され、フォルスユニバースに移行した REP の価値はほとんど無くなり、寄生的未決済建玉は多くてもネイティブ未決済建玉の半分である、という前提である。言い換えると、$S \geq 0.2$、$P_f = 0$、$I_a \geq 2I_p$ である。これらの前提の下、定理 1より、REP の時価総額がネイティブ未決済建玉の 7.5 倍以上あれば、フォーキングプロトコルに完全性があると言える。

実際にオラクルの完全性を保つためにどれほどの時価総額が必要かを、S、P_f、I_p を使って推測することができる。便宜上、以下のシナリオを挙げて推測する。

シナリオ 1. フォーキング期間中、存在する REP の 50%以上がトゥルーユニバースに移行された場合。このシナリオでは、P_f と I_p は全く考慮する必要がない。$S > \frac{1}{2}$ であるから、時価総額に関係なくフォーキングプロトコルに完全性があると言える。つまり、攻撃者が攻撃を成功させるための十分な REP が市場に流通していないということである。

シナリオ 2. フォーキング期間中、存在する REP の 48%がトゥルーユニバースに移行され、寄生的マーケットは存在せず、フォルスユニバースに移行された REP は無価値である場合。このシナリオでは、$S = 0.48$、$I_p = 0$、$P_f = 0$ となる。この想定の下では、フォーキングプロトコルが完全性を保つために、REP の時価総額はネイティブ未決済建玉の 2 倍より大きくなければならない。

シナリオ 3. フォーキング期間中、存在する REP の 20%がトゥルーユニバースに移行され、寄生的未決済建玉はネイティブ未決済建玉と等しく、フォルスユニバースに移行された REP の価値がトゥルーユニバースに移行された REP の 5%である場合。このシナリオでは、$S = 0.2$、$I_p = I_a$、$P_f = 0.05P$ となる。この想定の下では、フォーキングプロトコルが完全性を保つため、REP の時価総額はネイティブ未決済建玉の 10.5 倍より大きくなければならない。

シナリオ 4. 期間中、存在する REP の 5%がトゥルーユニバースに移行され、寄生的未決済建玉はネイティブ未決済建玉の 2 倍あり、フォルスユニバースに移行された REP の価値がトゥルーユニバースに移行された REP の 5%である場合。このシナリオでは、$S = 0.05$, $I_p = 2I_a$, and $P_f = 0.05P$ となる。この想定の下では、フォーキングプロトコルが完全性を保つために REP の時価総額はネイティブ未決済建玉の 63 倍より大きくなければならない。

Appendix C: フォーキングプロトコルの完全性に対する早期移行ボーナスの効果

考察を簡単にするため、フォーキングプロトコルの完全性を述べる際に、5%の早期移行ボーナスと attorep を意味する ϵ については考慮していなかった。ここでは、この 2 つを考慮して定理 1を再検討する。

[28] Appendix.E 2及び E 3参照

前述した通り、フォーキング期間中にトゥルーユニバースに送信された REP の量は SM で示される。よって、攻撃者がその攻撃を成功させるには、価値が $(SM+\epsilon)P$ である、$SM+\epsilon$ 以上の REP をフォルスユニバースに移行しなくてはならない。

フォーキング期間中に、攻撃者がフォルスユニバースに $SM+\epsilon$ REP を移行した場合、攻撃者は移行先のチャイルドユニバースで $1.05(SM+\epsilon)$ REP を受け取る。P_f の定義より、この移行されたコインの価値は、$1.05(SM+\epsilon)P_f$ である。よって攻撃するための最低コストは、$(SM+\epsilon)P - 1.05(SM+\epsilon)P_f$ となり、この式は $(SM+\epsilon)(P-1.05Pf)$ と表すことができる。

前述した通り、攻撃者の最大利益 (グロス値) は I_a+I_p である。ゆえに、$S>\frac{1}{2}$、または以下の式を満たす場合にフォーキングプロトコルに完全性があると言える。

$$I_a + I_p < (SM+\epsilon)(P-1.05P_f) \tag{C1}$$

この不等式から時価総額である PM を求めると、フォーキングプロトコルが完全性を有するための必要十分条件は以下となる。

1. $S>\frac{1}{2}$ または
2. $1.05P_f < P$ かつ、REP の時価総額が $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$ より大きい

以上から、時価総額の必要条件に対する早期移行ボーナスと ϵ の影響は極めて小さいと言える。

Appendix D: フォークの最小コストに対する早期移行ボーナスの影響

フォーク中の参加を促進するため、保有する REP をフォーク開始から 60 日以内に移行した者に対して、移行先のチャイルドユニバースで 5%の REP を付与する。この報酬は REP を新規発行することで支払われる。

フォークを開始するためのコストが低すぎると、このボーナスは意図しないインセンティブになってしまう。特に、攻撃者がフォークを開始するコストよりも、付与される 5%の REP ボーナスの方が多い場合、フォークが頻発することが予想される。この攻撃を**インフレーションミルキング攻撃** *(inflation milking attack)* と呼び、この攻撃でオラクルのレポートの正確性が損なわれることは無いが、破壊的なフォークが繰り返されることが予想される。

このような事態を防ぐため、Augur では 5%の REP ボーナスで得られる利益の最大値よりも、フォーク開始のコストの方が大きいことを確認しておく必要がある。そのため以下では、意図しないインセンティブを防ぐためにフォーク開始に必要なコストの下限を求める。

フォーク前の REP 価格を P_0、フォーク前の REP 価格を P_1 とする。フォーク前の REP 供給量 (マネーサプライ) を M_0、フォーク後の REP 供給量を M_1 とする。フォーク期間中にトゥルーユニバースに移行した M_0 の割合を S とする。フォーク開始のために経済的に焼却した REP(つまりフォルスユニバースとなったアウトカムにステークされた REP) の量を b とする。ここでは、$b>1$ とする。

このセクションではより保守的な考察を行うため、フォーキング期間中に移行された全ての REP は攻撃者の支配下にあるとする。さらに (攻撃コストを最小限にするために) フォーキング期間中に移行された全ての REP はトゥルーユニバースに移行したと仮定する。

ここでは、SM_0 はフォーキング期間中に移行された REP の量を表し、$(1-S)M_0$ はフォーク期間中に**移行されなかった** REP の量を表す場合、以下の等式が成り立つ。

$$M_0 = SM_0 + (1-S)M_0 \tag{D1}$$

SM_0 REP がフォーキング期間中に移行された場合、$0.05SM_0$ REP が新規発行される。従って、以下の等式が成り立つ。

$$M_1 = 1.05SM_0 + (1-S)M_0 \tag{D2}$$

新規発行の影響にのみ着目し、簡略化するために、フォーク前後で時価総額に変化はないものとすると[29]、以下の等式が成り立つ。

$$P_0M_0 = P_1M_1 \tag{D3}$$

式 D1、D2 を式 D3に代入し単純化すると以下となる。

$$P_1 = \frac{20P_0}{20+S} \tag{D4}$$

フォーク開始と早期移行ボーナスによって攻撃者が得られる利益 (グロス値) は、移行後の REP 価格から、移行前の REP 価格を減算することで求められる。式で表すと以下となる。

$$1.05SM_0P_1 - SM_0P_0 \tag{D5}$$

式 D4 を式 D5 に代入すると、攻撃者が得られる利益 (グロス値) を別の式で表すことができる。

$$1.05SM_0\frac{20P_0}{20+S} - SM_0P_0 \tag{D6}$$

b は、フォーク開始のために経済的に焼却した REP の量であるため、フォーク開始のコストは bP_0 である。ゆえに、以下の不等式が成立する限り、フォーク開始のコストを支払ってもなお、それを補うだけの早期移行ボーナスを得ることとなる。

$$0 < 1.05SM_0\frac{20P_0}{20+S} - SM_0P_0 - bP_0 \tag{D7}$$

$P_0>0$、かつ、$S\neq -20$ であるため、b が以下の場合、攻撃者は利益を上げることができる。

$$b < \frac{21M_0S}{S+20} - M_0S \tag{D8}$$

---

[29] これは保守的な考え方である。実際には、フォーク後の時価総額は減少すると思われる

よって、早期移行ボーナスによる意図しないインセンティブを避けるためには以下の式を満たす必要がある。

$$b \geq \frac{21M_0S}{S+20} - M_0S \tag{D9}$$

S の取り得る値が $[0,1]$ であることを考慮すると、式D9の右辺の値は $S = 2\sqrt{105} - 20 \approx 0.4939$ の場合に最大となる。よって、フォーキング期間中に存在する全 REP の内、約 49.39%が移行されると、攻撃者の利益は最大となる。より考察を保守的にするために、S はこの値を使用する。[30]

式 D9に $S = 0.4939$ を代入すると、$b \geq 0.012197M_0$ となる。従って、フォーク開始の必要コストが、存在する REP の 1.2197%以上である場合、インフレーションミルキング攻撃の実施は無益なものとなる。

フォークが開始されるのは、少なくとも存在する REP の 2.5%に相当する争議保証金が集まった後であることを思い出してほしい。例として、アウトカム ω の争議保証金が集まり、フォークが開始される場合を考える。アウトカム ω はトゥルーまたはフォルスのいずれかであるとする。

アウトカム ω がフォルスの場合、少なくとも存在する REP の 2.5%がフォルスアウトカムにステークされたということであり、結果としてこれらの REP は経済的に焼却されることとなる。従って、アウトカム ω がフォルスであれば、インフレーションミルキング攻撃の実施は無益であると言える。

アウトカム ω がトゥルーの場合、補助定理 2より、少なくとも存在する REP の 1.25%がフォルスアウトカムにステークされており、これらの REP は経済的に焼却される。従って、アウトカム ω がトゥルーの場合もインフレーションミルキング攻撃の実施は無益である。

以上から、フォーク開始には少なくとも存在する REP の 2.5%に相当する争議保証金が必要であると言える。

Appendix E: 保証金額の調整

有効性保証金、不参 REP 保証金、指名レポーターステーク (designated reporter stake) は、直前の手数料期間における参加者の挙動に基づいて動的に調整される。ここでは、これらの値をどのようにして調整するかを説明する。

まず、関数 $f : [0,1] \to [\frac{1}{2}, 2]$ を次のように定義する。[31]

$$f(x) = \begin{cases} \frac{100}{99}x + \frac{98}{99} & \text{for} \quad x > \frac{1}{100} \\ 50x + \frac{1}{2} & \text{for} \quad x \leq \frac{1}{100} \end{cases} \tag{E1}$$

この関数 f は、以下のサブセクションで説明しているように、調整用の倍数として利用する。直前の手数料期間において、不適切な挙動が丁度 1%の割合で発生した場合、各保証金の値は変わらない。1%より小さければ保証金の値は最小で二分の一減少し、逆に 1%より大きければ最大 2 倍増加する。

1. 有効性保証金

ローンチ後に迎える初回の手数料期間では、有効性保証金は 0.01ETH に設定される。その後、直前の手数料期間でマーケットの 1%超が無効でファイナライズされた場合、有効性保証金は増加する。逆に、直前の手数料期間でマーケットの 1%未満が無効でファイナライズされた場合、有効性保証金は減少する (ただし 0.01ETH を下回ることはない)。

厳密には、直前の手数料期間において無効にファイナライズしたマーケットの割合を ν、直前の手数料期間での有効性保証金額を b_v とすると、現在の手数料期間における有効性保証金の最大値は、$\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$ となる。

2. 不参 REP 保証金

ローンチ後の初回の手数料期間では、不参 REP 保証金は 0.35 REP に設定される。有効性保証金と同様、不参 REP 保証金も (指名レポーターが期限内にレポートしない割合が)1%を基準として上下に調整される。下限値は 0.35 REP である。During the very first fee window after launch, the no-show REP bond will be set at 0.35 REP. As with the validity bond, the no-show REP bond is adjusted up or down, targeting a 1% no-show rate with a floor of 0.35 REP.

厳密には、直前の手数料期間において期限内に指名レポーターによりレポートされなかったマーケットの割合を ρ、直前の手数料期間での不参 REP 保証金額を b_r とすると、現在の手数料期間における不参 REP 保証金の最大値は $\max\{0.35, b_r f(\rho)\}$ である。

3. 指名レポーターステーク

ローンチ後の初回の手数料期間では、指名レポーターステークは 0.35 REP に設定される。指名レポーターステークは、直前の手数料期間における指名レポーターが行った誤ったレポート (マーケットのファイナルアウトカムと異なったレポート) の数によって動的に調整される。

厳密には、直前の手数料期間において誤ったレポートを行った指名レポーターの割合を δ、直前の手数料期間での指名レポーターステーク額を b_d とする。すると、現在の手数料期間における指名レポーターステークの最大値は $\max\{0.35, b_d f(\delta)\}$ である。

Appendix F: 設計の変更

我々は三年に及ぶ研究と様々な反復作業により、現在の Augur の設計にたどり着いた。この設計内容はかつてのホワイトペーパー [12] の内容からは大幅に変更されている。ここでは 3 つの重要な変更とその根拠について説明する。

[30] 実際には、フォーキング期間に攻撃者以外の REP の移行を防ぐことはできないため、S の値は攻撃者が理想とする約 0.4939 を超える可能性がある。しかし、ここでは最悪のシナリオを想定するために、$S = 0.4939$ とした。

[31] この式は、実働するマーケットからのデータ採取後に変更される可能性がある。

1. レポーティング手数料

旧設計では、マーケット作成者がレポーターと 50/50 で分け合うトレーディング手数料を設定していた。現設計では、マーケット作成者とレポーターに支払われる手数料はそれぞれ独立しており、レポーターの手数料はシステムを安全に保つため Augur 自身によって動的に調整される。

レポーターに支払われる手数料は、フォーキングプロトコルの安全性に直接作用する REP 価格に対して影響を及ぼす (定理 1)。もしレポーターに支払われる手数料が低すぎる場合、オラクルの完全性は危険にさらされる。反対に、レポーターに支払われる手数料が高すぎる場合、寄生的マーケットが増加する恐れがある。従って、レポーターに支払われる手数料はマーケット作成者が任意に決定するのではなく、Augur の安全性を維持するために動的に調整することが重要である。

マーケット作成者にレポーターの手数料を決定させないことによって、マーケット作成者同士の最低手数料を巡る競争から、レポーターを (結果として、フォーキングプロトコルの完全性も) 守ることになる。良質なマーケットとレポーティングは、それぞれ独立して評価され報酬が与えられるべきである。価格競争でレポーター手数料を道連れに引き下げることなく、マーケット作成者手数料のみゼロに向かうことを可能にするだろう。

2. トレーディング手数料

旧設計では、トレーダーが取引を行う都度、手数料を徴収することを想定していた。新設計では、トレーダーがマーケットコントラクトと直接決済した場合のみ手数料を徴収する。この変更は、一つには Augur がオフライン取引を管理できないという理由がある。マーケットアウトカムのシェアはただのトークンであり、これらはユーザー間で自由に取引できる。手数料徴収を全取引で行うことは不可能であるため、トレーダーがマーケットコントラクトと直接決済した場合のみ Augur は手数料を徴収する。このアプローチによる副産物は、トレーダーが支払う平均手数料が減り、Augur の競争力が向上することである。

3. ユニバース

旧設計では、REP の “バージョン” は一つだけであり、その供給量は固定されていた。現設計では、REP は多数の異なるバージョン (ユニバース) にフォーク可能であり、フォークしたそれぞれのバージョンは元のバージョンよりも REP の量が増減する可能性がある。フォーク参加者に対するチャイルドユニバースへの早期移行ボーナスによって、ペアレントユニバースよりもチャイルドユニバースの方が REP 量が多くなる可能性がある。

フォークによって生成された新しい REP はそれぞれ独自の価格と合計量を持つ異なるトークンであり、サービス提供者はそれらをそのように扱うべきである。Augur の最初のローンチでは、まさに現在存在しているように、一つのユニバース (ジェネシスユニバース) と一つの REP のバージョンのみが存在する。しかし、フォークが発生すると一つだけだった REP のバージョンは複数のバージョンに分かれる。例えば、アウトカムに `A` と `B` があるマーケットがフォークする場合、REP-`A`、REP-`B`、REP-`Invalid`、という新しいトークンが生成される。この時点で、REP を取り扱うウォレットと取引所は、(理論上) サポート可能な 4 種類の異なる REP のバージョン – REP-`genesis`(この時点ではロックされている REP のオリジナルバージョン)、REP-`A`、REP-`B`、REP-`Invalid` – を取り扱えることとなる。[32]

各チャイルドユニバースの REP 供給量は、そのチャイルドユニバースへの REP 移行量と移行実施日時によって異なる。フォーク中の REP の移行では、どのチャイルドユニバースがコンセンサスを達成したのかが明確になるまで、ユーザーは小さい (がゼロではない) 危険にさらされ (セクション III E参照)、この危険はフォーキング期間中のユーザー参加を妨げる可能性がある。フォーキング期間中の参加を促すため、ユーザーはこの危険を補償されなくてはならない。

フォーキング期間中に参加しなかったユーザーはペナルティとして所有している REP を失う可能性があった。実際、旧設計は “使用するか失うか” という、まるで不正確なレポートを行ったレポーターを罰するかのような、不参加ユーザーを罰するメカニズムがあった。しかし、不参加ユーザーを罰することは重大なユーザビリティ問題を引き起こす。不参加ユーザーを罰することは、ウォレットと顧客の REP を預かる取引所にとって問題である。なぜならば、フォークが発生した場合、取引所はいずれかのチャイルドユニバースに顧客の REP を移行する必要があり、さもなければその預かる REP の一部を失ってしまうためだ。[33]

不参加を罰する代わりに、フォーキング期間中に移行したユーザーに対して、移行先のチャイルドユニバース内で 5%のボーナスを与えることにした。REP の 4.762%(あるいはこれ以上) がルージングユニバースに移行する – この内 1.25%から 2.5%はすでに争議ステークとしてコミット済み – と、全てのチャイルドユニバースの REP 合計量がペアレントユニバースの REP 合計量よりも小さくなる。

---

[32]実際には、ユーザーにフォークへの参加を促し、その後フォークによる判決結果に従い単純にウィニングユニバースをサポートすることが、サービス提供者にとって最も簡単な方法 (さらにユーザーに対しても最も破壊的でない方法) であると気付くだろう。

[33]実際問題として、再配布のみでフォークの報酬を実現するためにスマートコントラクトのコードを非常に複雑にする必要があった。コントラクトのコードの複雑化はセキュリティ上のリスクが高まるため、可能な限り単純な実装を試みた。