

Augur: Merkezi olmayan bir kehanet ve tahmin piyasası

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Forecast Foundation
(Dated: May 24, 2018)

Augur, tahmin piyasaları için merkezi ve güven gerektirmeyen bir kehanet ve tahmin platformudur. Augur'un tahmin piyasalarının sonuçları, gözlemlenen sonuca yatırım yapan ve karşılığında piyasalardan hesap kapatma ücreti alan, Augur sisteminin tokenine sahip kullanıcılar tarafından belirlenir. Augur sistemi, doğru bilgiyi paylaşan Reputation tokeni sahiplerinin daima en kazançlı pozisyonda olacağı şekilde tasarlandı. Token sahipleri önerilen piyasa sonuçlarına itiraz etmek için Reputation tahvili kullanabilirler. Eğer bu tahvillerin boyutu belirli bir seviyeye ulaşırsa, itiraz edilmiş piyasanın her muhtemel sonucu için versiyonlara bölünür. Bu durumda token sahipleri Reputation tokenlerini bu versiyonlardan biri için takas etmelidir. Kimse doğru olmayan tahmin piyasalarına katılmayacağı için gerçeklikle uyuşmayan versiyonun itibarları değersizleşecektir. Bu nedenle token sahipleri değerli olmaya devam edecek olan tek versiyonu seçecekler; gerçekçi versiyonu.

Augur, tahmin piyasası için merkezi ve güven gerektirmeyen bir kehanet platformudur. Tahmin piyasasında, kişiler gelecekte olacak olaylarla ilgili bir tahminlerde bulunur. Doğru tahminlerde bulunanlar para kazanırken yanlış tahminde bulunanlar ise kaybeder [1–3]. Bir tahmin piyasasının değeri gelecekte bir olayın gerçekleşme ihtimali için kesin bir gösterge görevi görmesidir [4–7].

Augur yardımıyla insanlar tahminlerini düşük maliyetlerle alıp satabilecekler. Kayda değer tek maliyet, olayların sonuçlandırılma süresince rapor veren kullanıcılara ve piyasa oluşturanlara ödenecek olan paydır. Tahmin piyasalarında üyelerin birbirine duyması gereken güvenden dolayı anlaşmazlık ve ücretler serbest piyasanın düşürebileceği kadar az olacaktır.

Tarih boyunca market piyasaları tek bir merkeze dayalıydı. Alım-satımları tahmin pazarında toplamının en kolay yolu güvenilir bir temel yaratmak; benzer bir şekilde, bir olayın sonucunu belirlemenin ve yatırımcılara ödemeleri dağıtmanın en kolay yolu; piyasaların sonuçların belirleyen, tarafsız ve güvenilir bir karar merciidir. Bununla birlikte, merkezi tahmin piyasaları birçok risk ve sınırlamaya sahiptir: Küresel katılıma izin vermezler, hangi tür piyasaların oluşturulabileceğini veya ticaretinin yapılabilmesini sınırlarlar ve yatırımcıların, fonları almamaları ve piyasaları doğru bir şekilde çözmeleri için piyasa operatörüne güvenmelerini gerektirirler.

Augur, piyasaları merkezi olmayan bir yapıya taşıyarak çözmeyi planlıyor. Bitcoin[8] ve Ethereum[9] gibi merkezi olmayan ve güven gerektirmeyen ağlar, kişisel çıkarların yolsuzluk veya hırsızlığa dönme riskini ortadan kaldırır. Augur geliştiricilerinin tek rolü Ethereum ile olan bağlantıyı doğru bir şekilde kurmaktır. Kurulan bu bağlar tamamen otomatik sistem üzerine kurulmuştur; Augur geliştiricileri rehin tutulan parayı harcayamaz ya da kontrol edemezler. Aynı zamanda geliştiriciler bir ticareti onaylayamaz, reddedemez, geri alamaz ya da iptal edemezler. Augur bilginin gerçek hayattan blok zinciri piyasasına herhangi bir güvenilen aracı mekanizması olmadan taşınmasına izin verir. Bu anlamda Augur dünyanın herhangi bir merkezi olmayan ilk kehanet plat-

formudur.

I. AUGUR NASIL ÇALIŞIR

Augur piyasası 4 aşamalı bir takip sürecine sahiptir: *oluşum, ticaret, raporlama ve sonuçlandırma*. Augur sistemindeki herkes herhangi bir gerçek dünya olayına dayalı bir piyasa oluşturabilir. Ticaret piyasa oluşturulduktan hemen sonra başlar ve tüm kullanıcılar piyasada işlem yapabilir. Olay gerçekleştikten sonra olayın sonucu Augur'un kehaneti tarafından belirlenir. Sonuç belirlendikten sonra, tüccarlar pozisyonlarını kapatabilir ve ödemelerini toplayabilir.

Augur kendine ait bir tokene sahip, Reputation (REP). REP, pazar oluşturulması ve sonucu rapor edilmesi ve etkinliğin sonuçlandırılma sürecinde kullanılan bir araç. Sonucu rapor eden kullanıcılar, raporlarını olayların olası sonuçlarından birine yatırım yaparak bildirirler. Böylelikle, rapor eden kullanıcı hisselerin yer aldığı sonucun piyasanın temelindeki olayın gerçek dünya sonuçlarıyla eşleştiğini beyan eder. Bir piyasanın muhabirlerinin mutabakatı, piyasanın sonucunu belirlemek amacıyla gerçek olarak kabul edilir. Bir muhabirin piyasa sonuçlarıyla ilgili raporu diğer muhabirler tarafından varılan mutabakatla eşleşmezse, Augur, REP'i fikir birliğine varılmış sonuca yatırım yapan muhabirlere yeniden dağıtır

REP'e sahip olup ve olayların sonuçlarına ilişkin doğru raporlamaya katılarak, token sahipleri platformdaki ödemelerin bir kısmına hak kazanırlar. Her yatırılmış REP tokeni, sahibini Augur'un piyasa ücretlerinin eşit bir kısmına hak eder. Muhabirin bu platformdan alacağı pay sahip olduğu token ve doğru sonuçlandığı olaylar ile doğru orantılıdır; bu yapı düzenin daha sağlıklı ilerlemesini sağlar.

REP, Augur'un operasyonlarında merkezi bir rol oynasa da, Augur pazarlarında ticaret yapmak için kullanılmamaktadır. Raporlama sürecine katılmaları gerekmediğinden, Tüccarların hiçbir zaman REP'e sahip olmaları veya kullanmaları gerekmemektedir



Figure 1. Tahmin piyasasının basitleştirilmiş ömrü.

A. Piyasa Oluşturmak

Augur herkesin yaklaşan herhangi bir etkinlik hakkında pazar oluşturmaya izin verir. piyasa oluşturunca etkinliğin bitiş süresini ayarlar ve etkinliğin sonucunu bildirmek için bir muhabir belirler. Belirlenen muhabir pazarın sonucuna tek taraf olarak karar veremez. Topluluğun her zaman belirlenen muhabirin raporuna itiraz etme ve düzeltme fırsatı vardır.

Sonrasında piyasa oluşturunca muhabirlerin sonuçları belirlemek için kullanması gereken bir karar kaynağı seçer. Bu kaynak sadece kullanıcıların ortak bilgisi ya da Amerika Birleşik Devleti Enerji Bakanlığı, bbc.com veya resmi bir başka kaynak olabilir.¹ Muhabirler aynı zamanda içerik oluşturunca ödenecek ücreti de belirlerler. (Detaylı bilgi için ID'e bakınız). Son olarak piyasa oluşturunca iki tahvil gönderir; *geçerlilik tahvili*, ve *belirlenmiş görünmeyen tahvil* (kısaca görünmeyen tahvil de denir).

Etherium ile ödenen geçerlilik tahvili, piyasa geçersiz olarak sonuçlanmadığı sürece piyasa yaratıcısına iade edilir.² Geçerlilik tahvili, piyasa içerik oluşturunca iyi tanımlanmış olaylara dayalı, nesnel ve kesin sonuçlarla piyasalar oluşturmaya teşvik eder. Geçerlilik tahvilinin büyüklüğü, son pazarlardaki geçersiz sonuçların oranına bağlı olarak dinamik bir şekilde belirlenir.³

Görünmeyen tahviller iki çeşidi içinde barındırır: the *Görünmeyen gaz tahvili* (ETH ile ödenir) ve *görünmeyen REP tahvili* (REP ile ödenir). Atanan muhabir olayın bitiş tarihini takiben üç gün içerisinde rapor verirse görünmeyen tahviller pazar oluşturunca iade edilir. Atanan muhabir bu raporu üç günlük vakit içinde sunamaz ise piyasa oluşturunca görünmeyen tahvili kaybeder ve bu ücret olayı doğru sonuçlandıran ilk muhabire verilir. (Detaylar için IC6'e bakınız). Bu sistem, piyasa oluşturunca doğru sonucun bir muhabiri atayarak işlem sürecinin hızlı ilerlemesini sağlamaya teşvik eder.

Görünmeyen gaz tahvili ilk atanan muhabirin gaz harcamasını karşılamak için vardır. Böylece İlk muhabirin

gaz harcamasının kâr edemeyecek kadar yükselmesi engellenir. Görünmeyen gaz tahvili bir önceki ücret aralığının ortalama gaz harcamasının iki katı olarak belirlenir.

Atanan muhabirin olayı sonuçlandırmaması durumunda, görünmeyen REP tahvilleri sonucu ilk ve doğru giren muhabire verilir. Geçerlilik tahvilinde olduğu gibi görünmeyen REP tahvillerin de atanan muhabirin etkinliği sonuçlandırmaması durumunda, görünmeyen REP tahvilleri sonucu ilk ve doğru giren muhabire verilir. Geçerlilik tahvilinde olduğu gibi, REP tahvili, bir önceki ücret aralığı boyunca zamanında rapor veremeyen muhabirlerin oranına göre dinamik olarak ayarlanır.⁴

Piyasa oluşturunca piyasayı oluşturur ve tüm gerekli tahvilleri tek bir Ethereum işlemi ile gönderir. İşlem onaylandıktan sonra, piyasa açılır ve ticaret başlar.

B. Ticaret

Piyasa katılımcıları olayların sonuçları ile ilgili tahminlerini satın aldıkları hisse senetleri yoluyla bildirirler. Yapılan tahminler çerçevesinde hisse kümeleri oluşturulur. Tam bir hisse kümesi etkinliğin her olasılığından alınan hisseler ile oluşur [10]. Bu hisse kümeleri Augur'un eşleştirme motoru tarafından işlemler geldikçe otomatik olarak oluşturulur.

Örneğin, iki olasılığı olan bir pazar düşünelim A ve B. Ali A olasılığı için 0.7 ETH değerinde bir hisse satın almak isterken Bülent ise B olasılığı için 0.3 ETH değerinde bir yatırım yapmak istiyor.⁵ İlk olarak Augur Ali ve Bülent'ten aldığı ETH'leri toplayarak hisse kümesi oluşturur.⁶ Oluşturulan hisse kümesinde Ali'ye yatırdığı oranda A hissesi, Bülent'e de B hissesi verilir. Oluşan hisse senetlerinin ticareti serbest bir şekilde yapılabilir.

Augur ticaret sözleşmeleri, platformda oluşturulan her piyasa için bir sipariş defteri oluşturur. Herkes yeni bir sipariş yaratabilir veya mevcut bir siparişi eleyebilir. Siparişler, Augur'un akıllı sözleşmelerinde bulunan otomatik bir eleme motoru tarafından eşleştirilir.

¹Örneğin; eğer piyasa "10 Nisan 2018 tarihinde San Francisco Uluslararası Havalimanı'nda en yüksek sıcaklık Weather Underground tarafından kaç derece bildirildi?" şeklinde aldysa, muhabirler kolayca <https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html> adresine giderek sonucu raporlayabilirler.

²*Geçersiz piyasa*, piyasa oluşturunca listelediği sonuçların hiçbirinin doğru olmadığı, sonucun öznel olduğu ya da piyasa ifadesinin belirsiz olduğundan muhabirler tarafından geçersiz kılınan pazardır.; detaylar için III F'e bakınız.

³Detaylar için E1'e bakınız.

⁴Detaylar için E2'e bakınız.

⁵Başlangıçta Augur piyasasındaki ticaretlerde Ethereum'un ana sanal parası olan Ether (ETH) kullanılacak. Sonraki aşamada bu işlemlere Ethereum dışında bulunan diğer tokenler, pazarlardan satın alınmış hisse senetleri ve uygun görülen diğer tokenler dahil edilecektir.

⁶1 ETH tamamen işlem kolaylığı için kullanılmıştır. Aşında sistemde kullanılan eşleşme miktarı bundan çok daha düşüktür; detaylar için docs.augur.net/#number-of-ticks'a bakınız.

Sipariş defterinde eşleşen bir sipariş varsa, hisseleri satın alma veya satma talepleri derhal yerine getirilir. Bu işlem yeni hisse kümesi yaratarak ya da mevcut hisse kümelerini kapatarak yapılabilir. Augur'un akıllı eleme motoru her zaman risk altındaki değeri karşılamak için gereken minimum hisse miktarını ve/veya nakit miktarını seçer. Eşleşen bir sipariş yoksa veya işlem miktarı yalnızca kısmen doldurulmuşsa, kalan kısım sipariş defterine yeni bir sipariş olarak yerleştirilir.

İşlemler, tüccar tarafından belirlenen fiyattan daha kötü bir fiyat ile gerçekleştirilemez ancak daha iyi bir fiyat ile gerçekleşebilir. Tamamlanmamış ya da kısmen tamamlanmış siparişler piyasa oluşturucusu tarafından her zaman iptal edilebilir. Ücretler, sadece tüm hisse satıldığında ödenir; Anlaşma ücretleri bu bölümde daha detaylı açıklanmaktadır¹ D.

Hisse alım-satım işlemlerinin piyasa oluşmadan gerçekleşmesi daha olası gözükse de, piyasa oluştuktan sonra da işlem yapılabilir. Augur varlıklarının tamamı; hisse senetleri, tokenler, anlaşmazlık tahvillerinde hisseler ve hatta piyasalar her zaman devredilebilir.

C. Raporlama

Olay tamamlandıktan sonra, piyasanın sonuçlanması için bir sonuç belirlenmelidir. Sonuçlar kâr amacı güden, olayın gerçek sonuçlarını ortaya koyan muhabirler tarafından Augur'un kehanetiyle belirlenir. REP'e sahip olan herkes sonuçlandırma tartışmasına katılabilir. Raporlar mutabakat ile eşleşen kullanıcılar maddi olarak ödüllendirilirken, uymayanlar cezalandırılır. (Bölüm ID 3'e bakınız).

1. Ücret Aralığı

Augur'un raporlama sistemi 7 günlük bir ücret aralığından oluşur. Bu süre boyunca tüm ücretler Augur tarafından toplanır ve ücret havuzu oluşturulur. Sürecin sonunda raporlama ücreti, sonuçlandırma sonucuna katılan REP sahiplerine ödenir. REP sahipleri riske attıkları miktar oranında ödüllendirilirler. Raporlama sistemine katılım: ilk rapor süresinde yapılan yatırım, kesin olmayan sonuca itiraz ya da *katılım tokeni* satın alarak yapılabilir.

2. Katılım Tokeni

REP sahipleri sonuçlandırma sürecinde 1 attorep⁷ değerindeki katılım tokenlerinden istedikleri kadar satın alabilirler. Ücret aralığı sonunda 1'er attorep olarak

katılım tokenlerini bozdurabilirler. Eğer bir muhabir ondan beklenen eylemleri (*Örneğin*, raporlama ve başka bir üye tarafından sonuçlandırılmış rapora itiraz gibi) gerçekleştirmezse, ücret aralığına katıldığını göstermek için katılım tokeni satın alabilir. Yatırılmış REP gibi, katılım tokenleri de ücret aralığında ödenen fiyatlara orantılı olarak bozulabilir.

II'da anlatıldığı gibi, REP sahiplerinin herhangi bir ikilem durumunda pazar sonuçlandırmak için karar belirtmesi önemlidir. Katılım tokeni, REP sahiplerinin platformu en az haftada bir kere takip etmesi adına teşvik sağlar. Sonuçlandırma sürecine katılmak istemeyen REP sahipleri bile bu teşvik sayesinde Augur'u düzenli olarak kontrol ederler. Bu sayede ihtiyaç halinde REP sahiplerinin de kehanete katkıda bulunması sağlanmakla birlikte bir etkinliğin sonuçlandırılması konusunda sıkıntı yaşandığı taktirde duruma müdahil olmaları da sağlanacaktır.

3. Piyasa Aşamaları

Augur piyasaları oluşturulduktan sonra yedi olası aşamada olabilirler. Augur piyasalarının olası aşamaları şu şekildedir:

- Ticaret
- Raporlama
- Açık Raporlama
- Bekleme Aşaması (bir sonraki ücret aralığını bekleme)
- İtiraz
- Çatallaşma
- Sonuç

Bu aşamaların ilişkileri Şekil-2'de görülebilir. Fig. 2.

4. Ticaret

Ön Raporlama ya da *Ticaret* süreci (Fig. 1) piyasada ticaret başladıktan sonra ama bitmeden önce başlayan süreçtir. Genellikle, her Augur piyasası için bu süreç, en hareketli ticaret sürecidir. Olay sonuçlandıktan sonra piyasa *raporlama* sürecine girer. (Şekil. 2a).

5. Raporlama

Piyasa oluştururken, piyasa oluşturucularının bir muhabir ataması ve görünmeyen tahvil vermeleri gerekir. Atanmış raporlama sürecinde, piyasanın atanmış muhabirinin olay sonucunu raporlaması için üç günü vardır. Eğer atanmış muhabir üç gün içinde

⁷1 attorep = 10⁻¹⁸ REP.

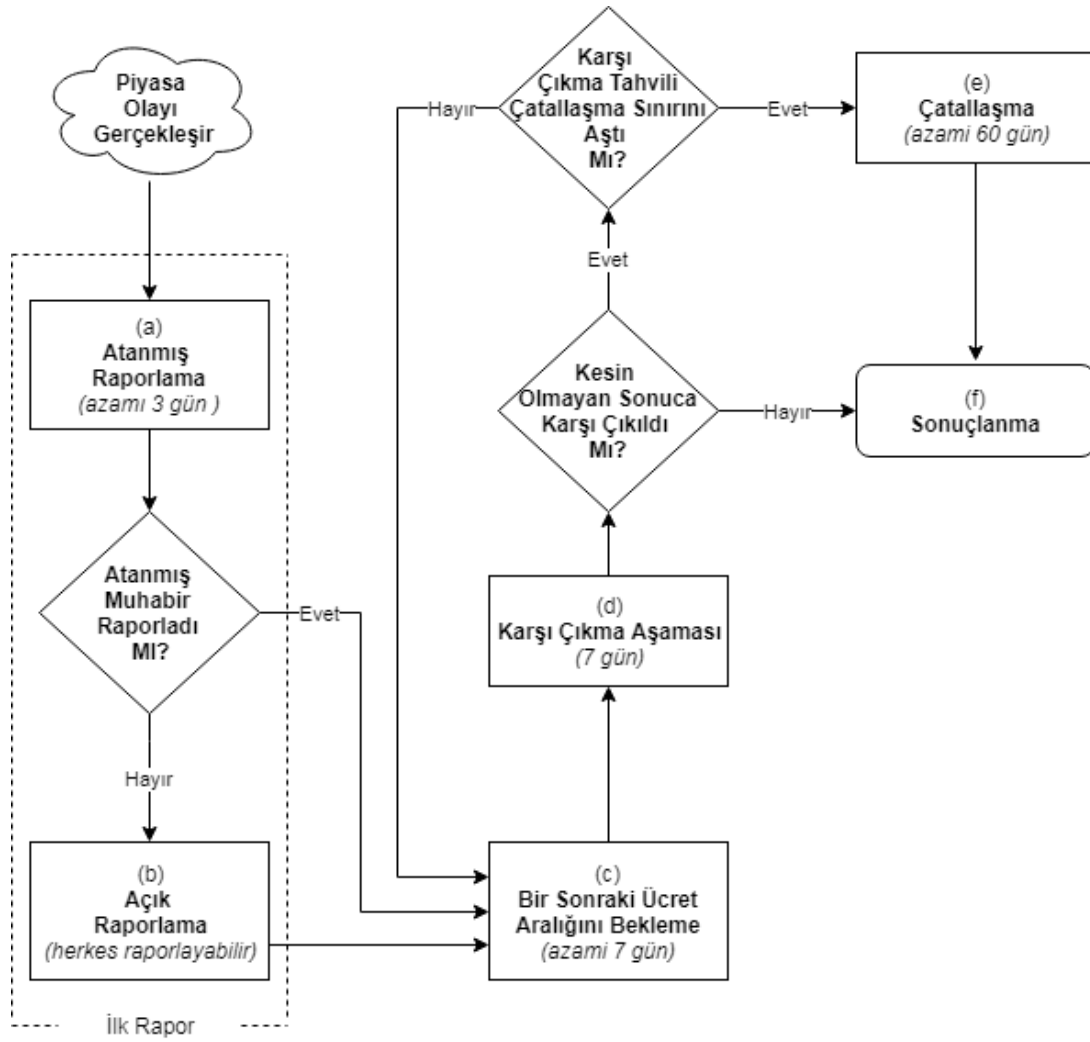


Figure 2. Raporlama akım şeması.

raporlayamazsa piyasa oluşturucusu görünmeyen tahvil üzerinde hakkını kaybeder ve piyasa otomatik olarak *açık raporlama* sürecine girer. (Şekil. 2b).

Eğer atanmış muhabir olayı zamanında raporlarsa görünmeyen tahvil, piyasa yaratıcısına geri verilir. Atanmış muhabirin, kendi tahvilini raporladığı sonuca yatırarak bildirir.⁸Eğer piyasa raporladığı sonuçta karar kılmaz ise muhabir yanlış raporladığı için hissesini kaybeder.⁹ Atanmış muhabir sonucu raporladığı anda piyasa bir sonraki süreç olan *bekleme aşamasına* girer ve raporlanmış sonuç piyasanın kesin olmayan sonucu haline gelir. (Şekil. 2c)

6. Açık Raporlama

Eğer atanmış muhabir üç gün içinde raporlayamazsa piyasa yaratıcısı görünmeyen tahvil üzerinde hakkını kaybeder ve piyasa *açık raporlama* aşamasına girer.(Fig. 2b). Piyasa açık raporlama aşamasına girdiği anda herkes piyasanın sonucunu raporlayabilir. Bu durumda sonucu ilk olarak raporlayan muhabir,*ilk kamu muhabiridir*.

Piyasanın ilk kamu muhabiri görünmeyen tahvili(atanan muhabirin kaybettiği tahvil), raporladığı sonuç üzerine hisse olarak alır. Böylece görünmeyen REP tahvilini sadece raporladığı sonuç piyasanın sonucuyla eşleşirse kazanmış olur. Eğer raporladıkları sonuç piyasanın sonucuyla eşleşirse ek olarak görünmeyen gaz tahvilini de alırlar.

İlk kamu muhabirinin piyasa sonuçlarını rapor ederken kendi REP'lerinden yatırım yapmak zorunluluğu yoktur. Bu sayede atanmış muhabirin sonuçlandıramadığı bir pazar açık raporlama aşamasına geldikten çok kısa

⁸ Atanmış muhabirin hisse büyüklüğünün bilgileri için:E3.

⁹ Kaybedilen hisse piyasanın atanmış ücret aralığının raporlama ücret havuzuna eklenir, bu mebla ilk sonuca karşı çıkan ve doğru sonucu raporlayanları ödüllendirmek için kullanılır; detaylar için D 3'e bakınız.

bir süre sonra *birileri* tarafından rapor edilebilir.

İlk sonuç rapor edildikten sonra (atanan muhabir ya da kamu muhabiri fark etmeksizin), rapor edilen sonuç piyasanın geçici sonucu haline gelir ve market bir sonraki ücret süreci beklemeye başlar(Şekil. 2c).

7. Bekleme Aşaması

Piyasa ilk raporunu aldığı anda bir sonraki ücret aralığını bekleme aşamasına girer(Şekil. 2c). Bu aşamada piyasa için raporlama yapılamaz, bir sonraki ücret aralığı beklenir ve yeni ücret aralığıyla birlikte piyasa *itiraz aşaması* girer.

8. İtiraz Aşaması

İtiraz aşaması,(Şekil. 2d) her REP sahibinin kesin olmayan sonuca itiraz fırsatının olduğu yedi günlük bir süreçtir.¹⁰ (İtiraz sürecinin başlangıcında piyasanın kesin olmayan sonucu, REP sahipleri tarafından başarılı bir şekilde karşı çıkılmazsa piyasanın kesin sonucu haline gelir.) İtiraz, piyasanın kesin olmayan sonucu dışındaki sonuçlara –itiraz hissesi adı altında- REP yatırımıyla yapılır. Bir sonuca yatırılan itiraz hissesi, geçici sonuca yatırılan hisse miktarını geçerse itiraz başarılı olur. İtiraz süreci aşağıdaki gibi bir örnekle ifade edilebilir.

Piyasanın bu itiraz aşamasının başlangıcında, bütün sonuçlara yatırılan hisselerin toplamı n olduğunu ω 'nın ise piyasanın itiraz aşamasının başlangıcında kesin olmayan sonucu dışında herhangi bir sonucu olduğunu farz edelim. $S(\omega, n)$ ise itiraz aşaması n 'nin başında ω 'ye yatırılan hisselerin toplamı olsun. Kesin olmayan durumda başarılı bir itiraz için ω 'ye yatırılması gereken hisse $B(\omega, n)$ olsun:

$$B(\omega, n) = 2A_n - 3S(\omega, n) \quad (1)$$

Tahvil boyutlarının böyle seçilmesinin nedeni başarılı bir şekilde karşı çıkan muhabirlere, yatırımlarından sabit 50% kazanç sağlamaktır.(Bölüm II D'ye bakınız).

İtiraz tahvillerinin tek kişi tarafından ödenmesine gerek yoktur. Augur platformu, katılımcıların itiraz tahvilini kitle olarak fonlamasına izin verir. Her kullanıcı, yanlış olduğunu düşündüğü kesin olmayan sonuç dışında herhangi bir sonuca REP yatırarak kesin olmayan sonuca karşı çıkabilir. Kesin olmayan sonuç dışında herhangi bir sonuç itiraz tahvilini dolduracak kadar yatırım alırsa, kesin olmayan sonuca itiraz başarılı olur.

Başarılı bir itiraz sonucunda piyasaya yeniden itiraz sürecine girer ya da çatallaşma aşamasına girer (Şekil. 2e). Eğer doldurulmuş itiraz tahvili toplam

REP'in 2.5%'ndan daha fazla ise piyasa çatallaşma aşamasına girer. Eğer doldurulmuş itiraz tahvili toplam REP'in 2.5%'ndan az ise seçilen sonuç piyasanın yeni kesin olmayan sonucu olur. Piyasa yeniden itiraz sürecine girer.

Bütün itiraz hisseleri itiraz aşamasında rehinde tutulur. Eğer bir itiraz tahvili başarısız olursa itiraz hisseleri sahiplerine iade edilir. Eğer yedi günlük itiraz aşaması sırasında hiçbir itiraz başarılı olmazsa, piyasa sonuçlanmaya girer(Şekil. 2f) ve kesin olmayan sonuç nihai sonuç olarak kabul edilir. Bir piyasanın kesin sonucu başarılı bir şekilde itiraz edilmeyen veya çatallaşmayla belirlenen sonucudur. Augur kullanıcıları kesin sonuçları gerçek sonuç olarak kabul edip uygun bir şekilde ödemelerini yaparlar. Bütün başarısız itiraz hisseleri itiraz aşamasından sonra sahiplerine iade edilir. Bütün başarılı itiraz hisseleri destekledikleri sonuca uygulanır ve piyasa sonuçlanmaya kadar (veya başka bir piyasada çatallaşma oluşana kadar) bekletilir. Bütün itiraz hisselerine (başarılı ya da başarısız) devam eden ücret aralığında alınan raporlama ücretlerinin havuzundan pay eklenir.

9. Çatallaşma

Çatallaşma aşaması (Fig. 2e) 60 güne kadar uzayabilen özel bir aşamadır. Çatallaşma piyasanın son çaresidir; aksatıcı bir süreçtir ve nadiren oluşması beklenir. Bir piyasada toplam REP'in 2.5%'ini oluşturan bir itiraz tahvili oluşması çatallaşmaya neden olur. Bu durumun olduğu piyasalar çatallaşan piyasa olarak isimlendirilir.

Çatallaşma oluştuğunda 60 günlük süreç başlar.¹¹ *forking period*. Çatallaşma süreci alışılan ödeme süreçlerinden daha uzundur çünkü platformun REP sahiplerine ve hizmet sağlayıcılarına (piyasanın bütün aktörlerine) gerekli zamanı vermesi gerekir. Bir çatallaşmanın nihai sonucuna karşı çıkılmaz. Bütün Augur piyasaları ve REP tokenleri bir evrende bulunur.

REP tokenleri sonuçları raporlamada (ve raporlama yoluyla para kazanmada) kullanılır ama bu sadece REP tokenleriyle aynı evrende yer alan piyasalar için geçerlidir. Augur açılışını yaptığı anda bütün piyasalar ve REPlar aynı ana evrende bulunacak.

Bir piyasa çatallaştığında yeni evrenler oluşur. Çatallaşmalar, çatallaşan piyasanın her olası sonucu için birer çocuk evren oluşturur. (Bu duruma, ID 2'da bahsedilen geçersiz piyasalar da dahildir.). Örnek olarak, tekil bir piyasanın 3 olası sonucu vardır: A, B ve Geçersiz. Böylece, Tekil bir çatallaşma üç çocuk evren oluşturur: Evren A, Evren B ve Geçersiz Başlangıçta bu yeni oluşturulan evrenler boştur: Piyasaları ve REP tokenleri yoktur.

¹⁰İtiraz süreci ve ücret aralığının aynı olma nedeni tamamen işlem kolaylığı sağlamaktır. Teknik olarak iki sürecin uzunluğu farklı olabilir.

¹¹Çatallaşma aşamaları 60 günden kısa olabilir. Çatallaşma aşamaları 60 gün geçtiğinde ya da ana REP'in 50%den fazlası çocuk evrene taşındığında sona erer

Çatallaşma başladığında Ebeveyn evren kalıcı olarak kilitlenir. Kilitlenen bir evrenden yeni piyasalar oluşturulamaz. Kilitli evrenlerde kullanıcılar hisse ticareti yapabilir ve piyasalar ilk raporlarını alabilirler. Fakat raporlamalar ödüllendirilemez ve piyasalar sonuçlandırılmaz. Kilitlenmiş bir evrende piyasaların ve REP tokenlerinin kullanışlı olması için öncelikle çocuk evrene taşınmaları gerekir.

Ebeveyn evrende REP tokeni bulunan kullanıcılar tokenlerini istedikleri çocuk evrene taşıyabilirler. Bu karar dikkatlice alınmalıdır, çünkü taşımalar tek yönlüdür; geri alınamaz. Tokenler çocuk evrenler arasında taşınmaz. Taşımak, REP tokenlerinin piyasanın bir sonucuna kalıcı olarak adanmasıdır. Farklı bir kardeş evrene taşınan tokenler farklı tanınır ve hizmet sağlayıcılarının da tokenleri bunu dikkate alarak listelemesi gerekir.

Bir çatallaşma başlatıldığında, yatırılmış bütün REPler çocuk evrenlere taşınabilmesi için serbest bırakılır.¹²

En çok REP taşınan çocuk evren kazanan evren olur, uyumlu olduğu sonuç ise çatallaşan piyasanın nihai sonucu olur. Ebeveyn evrenin sonuçlanmamış piyasaları sadece kazanan evrene taşınabilir ve ilk raporlamalarını almışlar ise bir sonraki ücret aralığını bekleme aşamasına alınırlar.

Ebeveyn evrenden çocuk evrene token taşımının zaman sınırı yoktur. Tokenler çatallaşma aşamasından sonra taşınabilirler ama kazanan evrenin kararlaştırılmasında rol oynamazlar. Çatallaşma sürecinde katılımı güdülemek amacıyla çatallaşmanın başlangığını takiben 60 gün içinde tokenlerini taşıyan bütün REP sahiplerine taşıdıkları çocuk evrende 5% fazladan Rep verilir.¹³ Bu ödüllendirme yeni REP basımı ile karşılanır.¹⁴

Çatallaşan piyasanın sonuçlarından birine REP yatıran muhabirler kararlarını çatallaşma devam ederken değiştiremezler. Ebeveyn evrende bir sonuca yatırılmış olan REP, sadece yatırıldığı sonuca uyumlu olan çocuk evrene taşınabilir. Örnek olarak, bir muhabir başarıya ulaşan ve A sonucunu destekleyen itiraz tahvilinin doldurulmasına yardım etmiş ise A sonucuna yatırdığı REP çatallaşma aşamasında sadece A evrenine taşınabilir.

Kardeş evrenler ayrışıklardır. Bir evrende bulunan REP tokenleri başka bir evrende olayları raporlama veya ödül kazanma için kullanılamaz. Kullanıcılar, kehaneti güvenilir olmayan bir evrende piyasa oluşturup ticaret yapmak istemeyecekleri için ve gerçeklikle uyuşmayan bir evrende bulunan REP'in sahibine ödül kazandırma

olasılığı az olacağı için bu evrenlerde bulunan REPlerin piyasa değeri kayda değer olamayacaktır. Böylece, gerçeklikle uyuşmayan evrenlere taşınan REP tokenleri, yanlış evren çatallaşmada kazansa da piyasada değersiz olacaktır. Bu durum güvenlik için çok önemlidir. Bu durumII'de açıklanmıştır.

10. Sonuçlanma

Bir piyasa, yedi günlük itiraz aşamasını kesin olmayan sonucuna başarılı bir şekilde karşı çıkılmadan geçerse veya çatallaşması sonuca ererse sonuçlanmış aşamaya girer.(Şekil. 2f) Çatallaşmanın sonucuna karşı çıkılmaz ve her zaman çatallaşma aşamasının sonunda, nihai kabul edilir. Bir piyasa sonlandırıldığında, tüccarlar hesaplarını doğrudan piyasa ile kapatabilirler. Bir piyasa sonuçlanmış aşamasına girdiğinde, seçilmiş sonucuna nihai sonuç deriz.

D. Piyasa Kapanışı

Bir tüccar hesabımı iki şekilde kapatabilir: sahip olduğu hisseleri başka bir tüccara döviz karşılığında satarak veya piyasayla hisselerini kapatarak. Hatırlarsanız bütün hisseler, 1 ETH'nin Augur'a rehin verilmesiyle ve tamamlanmış bir küme oluşmasıyla oluşturuluyordu.⁶ 1 ETH'yi rehinden çıkarmak için tüccarlar Augur'a ya tamamlanmış eşleşmeyi ya da eğer piyasa sonuçlandıysa kazanan hissedenden bir pay vermeli. Bu takasa tüccarların piyasa ile hesap kapatması denir.

Örnek olarak, olası sonuçları A ve B olan sonuçlanmamış bir piyasa düşünelim. Ayşe'nin A sonucunda 0.7 ETH'a satmak istediği hissesi olsun ve Ahmet'in de 0.3 ETH'a satmak istediği B sonucunda hissesi olsun. Öncelikle, Augur bu siparişleri eşleştirir ve katılımcılardan A ve B hisselerini toplar. Sonra Augur Ayşe'ye 0.7 ETH (ücretleri çıkarmadan), Ahmet'e 0.3 ETH (ücretlendirmeleri çıkarmadan) verir.

İkinci bir örnek olarak, kazanan sonucu A olan bir piyasa düşünelim. Ayşe'nin A hissesi var ve satmak istiyor. A hissesini Augur'a yollayıp karşılığında 1 ETH kazanır(Aslında 1 ETH - ücretlendirmeler).

1. Hesap Kapatma Ücretleri

Augur, sadece piyasa katılımcıları piyasa anlaşmasıyla hesap kapattıklarında ücret alır. Bu süreçte Augur piyasa oluşturma ücreti ve raporlama ücretini katılımcıların ödedikleri ücret oranında keser. Örneklendirmek gerekirse; yukarıdaki sonuçlandırılmamış hesap kapatma örneğinde; Ayşe 0.7 ETH aldığı için ücretlerin 70%'ini, Ahmet 0.3 ETH aldığı için ücretlerin 30%'unu öder.

Yukarıda alınan ücretlerden; Piyasa oluşturma ücreti piyasayı oluşturan kullanıcıya, Raporlama ücreti ise ra-

¹²Tek istisnası ilk muhabirin raporlarken yatırdığı REPTir. Bu REP ilk rapor edilen sonuçta yatırılmış halde kalır ve çatallaşmayı kazanan çocuk evrene otomatik olarak taşınır.

¹³Bu durum, toplam REP'in 50% sinin çocuk evrenlerden birine taşınmasıyla çatallaşma aşamasının erken bitmesinde bile geçerlidir.

¹⁴Bu paranın REP havuzuna katılmasının etkisi azdır. Örnek olarak, eğer var olan toplam REP'in 20%'si çatallaşma aşamasında taşınırsa, bu fazlalık REP kaynağında 1%'lik bir artışa neden olurdu. Ayrıca, çatallaşmalar nadir olmaları için tasarlandı.

porlama sürecine katkıda bulunan muhabirlere verilir. (Bu oran dinamik olarak belirlenir)(Detaylar için; II C)

2. Belirsiz Piyasaların Sonuçlanması

Piyasa belirsiz olarak sonuçlandığında, piyasa anlaşmasıyla hesaplarını kapatan tüccarlar her sonucun hisseleri için eşit miktarda ETH alırlar. Eğer piyasanın N sayısında bir olası sonucu var ise (geçersiz sonucu saymaz isek) ve eşleşmiş hisselerin değeri C ETH ise tüccarlar piyasada kapattıkları her hisse için C/N değerinde ETH alırlar.¹⁵

3. Reputation Dağılımı

Bir piyasa çatallaşma olmadan sonuçlanırsa, piyasanın nihai sonucu dışında herhangi bir sonuca yatırılmış REPlar piyasanın nihai sonucuna yatırım yapan kullanıcılara, yatırdıkları REP'e orantılı olarak dağıtılır. İtiraz tahvilinin boyutu, başarıyla karşı çıkan kullanıcılara 50% kâr sağlayacak şekilde seçilir.¹⁶ Böylece, yanlış/kesin olmayan sonuçlara itirazları için kullanıcılar teşvik edilmiş olur.

II. TEŞVİKLER VE GÜVENLİK

Piyasanın REP değeri ile Augur'un çatallaşma protokolünün bütünlüğü arasında güçlü bir ilişki vardır. Eğer piyasanın REP değeri yeterince yüksek ise¹⁷ ve saldırganlar ekonomik olarak makul iseler çatallaşmanın sonucunun gerçeklikle uyuşması gerekir. Aslına bakılırsa Augur'un atanmış muhabirler ve itiraz aşamaları olmadan çalışmaları olasıdır. Sadece çatallaşma aşaması kullanılırsa, kâhinin doğruyu bildirmesi gerekir.

Ancak, çatallaşmalar aksatıcı ve zaman harcayan süreçlerdir. Bir çatallaşma 60 günde bir piyasayı çözebilir ve aynı anda birden fazla piyasayı çözemez. Çatallaşmanın 60 günü içerisinde sonuçlanmamış bütün piyasalar beklemeye almır.¹⁸ Hizmet sağlayıcıları REPlarını güncellemeli, REP sahipleri ise taşımalı. Bu nedenle, çatallaşmalar sadece gerektiğinde kullanılmalı. Çatallaşma nükleer çözümdür.

Neyse ki, çatallaşmaların hakikati bulmak için kullanılabileceği anlaşıldığında, güdülemelerle kullanıcılar

çatallaşmaya ihtiyaç olmadan dürüst davranmaya teşvik edileceklerdir. *Çatallaşmanın güvenilirliği ve çatallaşmanın doğru biteceğine kullanıcıların inancı, Augur'un güdüleme sisteminin mihenk taşlarıdır.*

Bundan sonra, çatallaşma sisteminin hangi şartlarda doğruya ulaştırmasına güvenilebileceğinden bahsedeceğiz. Ondan sonrasında ise; güdüleme sisteminden ve piyasaları nasıl hızlı ve doğru sonuçlara ulaştırmaya teşvik ettiğinden bahsedeceğiz.

A. Çatallaşma Protokolünün Bütünlüğü

Burada çatallaşma işleminin bütünlüğünden ve hangi şartlarda güvenilebileceğinden bahsedeceğiz. Kolaylık için, gerçeklikle uyumlu olan çocuk evrene doğru evren, uyumlu olmayan her evrene yanlış evren diyeceğiz. Çatallaşma sürecinde en çok REP alan evrene kazanan evren ve diğer bütün evrenlere kaybeden evren diyeceğiz.

Doğal olarak, doğru evrenin hep kazanan evren, yanlış evrenlerin hep kaybeden evrenler olmasını isteriz. Yanlış evren kazanan evren olduğunda çatallaşma protokolüne başarıyla saldırıldı deriz. Böyle olduğunda çatallaşan piyasaya ve sonuçlanmamış her piyasaya ödemeler yanlış yapılır.

Kâhini korumaya yaklaşımımız başarılı bir saldırının kazancını kayıplarından düşük tutmaktır. Bu yaklaşımımızı aşağıda resmileştirdik

1. Bir Saldırganın Azami Kazancı

Başarılı bir saldırgan sonuçlanmamış bütün piyasaların bir Yanlış evrene taşınmasına neden olur. Eğer saldırgan bir Yanlış evrende REP'in çoğunu kontrol ediyorsa, sonuçlanmamış bütün piyasaları istediği sonuca zorlayabilir. En aşırı durumda, o piyasalarda rehin tutulan bütün tahvilleri de ele geçirebilir.¹⁹

Tanım 1. I_a ile olarak gösterdiğimiz Augur'un yerel açık faizi, Augur'un sonuçlanmamış piyasalarında rehin duran bütün hisselerin değeridir.²⁰

Tanım 2. Augur'a raporlama ücreti ödemeyen, ama Augur'un yerel piyasalarından biriyle aynı sonuca ulaşan piyasalar parazit piyasa olarak tanımlanır.

Tanım 3. I_p olarak gösterdiğimiz parazit açık faizi, sonuçlanmamış Augur piyasaları ile uyumlu çözülen bütün parazit piyasalarda rehin tutulan sermayelerin toplamının değeri olarak tanımlanır.

En ekstrem durumda, bir saldırgan, parazit piyasalarda Augur'un sonuçlanmamış yerel piyasalarıyla uyumlu sonuçlanan bütün hisseleri de ele geçirebilir.

¹⁵Eğer piyasa geçersiz sonuçlanırsa, teknik limitler nedeniyle alışverişler sonuçlanamaz. Sonuçların hisseleri sadece kullanıcılar arasında kullanılan tokenlerdir; bu nedenle, ETH ve hisseler Augur'un kontrolünde değildir ve eğer piyasa geçersiz sonuçlanırsa geri verilemez

¹⁶Ek A'da 3 üçüncü teoriye bakınız A.

¹⁷Detaylar için II A'da bölüm II'ye bakınız.

¹⁸Tüccarlar bu piyasalarda ticaretlerine devam edebilirler ama bu piyasalar çatallaşma süreci bitene kadar sonuçlanmaz.

¹⁹Bu durumun gerçekleşmesi için saldırganın bir sonucun tüm hisselerini ele geçirmesi ve piyasayı o sonuca zorlaması gerekir.

²⁰Augur'a raporlama ücreti ödeyen dış piyasalar da dâhildir.

Gözlem 1. Augur'un kehanetine başarılı bir şekilde saldıran bir saldırganın azami (brüt) kârı $I_a + I_p$ olur.

2. Parazit Açık Faiz Bilinemez.

Augur tutarlı ve etkili olarak I_a 'yı hesaplayabilir. Ancak, I_p genel olarak bilinemez çünkü birçok çevrimdışı parazit piyasa, her biri gelişigüzel bir şekilde var olabilir. Saldırganın azami kazancı büyüklüğü bilinmeyen I_p 'yi de içereceğinden dolayı, kehanetin ekonomik olarak makul saldırılara karşı güvenli olduğuna emin olunamaz.

Ancak, I_p 'nin uygulamada bağlı olduğunu iddia edebilirsek, o zaman kehanetin güvende olduğu şartları tanımlayabiliriz.

3. Başarılı Bir Saldırının Asgari Maliyeti

Kehanet sistemine saldırmanın masrafını hesaplayalım. P , REP'in değeri olsun. $\epsilon =$ bir attorep²¹. M ise REP'in toplam para arzı, S ise M 'nin çatallaşma sürecinde evrene taşınacak kısmı olsun.

Böylece SM , çatallaşma sürecinde doğru evrene taşınan bütün REP'i temsil eder ve piyasanın ürünü PM de piyasanın REP tavanı olur.

P_f , saldırganın seçtiği yanlış evrene taşınan REP olsun. Eğer $P \leq P_f$ olsaydı kehanet ekonomik olarak makul saldırganlara karşı güvenli olmazdı çünkü yanlış evrene REP taşımak ile hiç taşımamak arasında kâr farkı olmazdı.

4. Bütünlük

Varsayım 1. Saldırgan olmayan muhabirler bir çatallaşmada asla bir yanlış evrene REP taşımaz.²²

Kehanet, başarılı bir saldırının yapılması için çatallaşma aşamasında yanlış evrene doğru evrenden çok REP taşınması gerekecek şekilde tasarlandı. Varsayımsal olarak, sadece saldırgan bir yanlış evrene REP taşıyabilir. SM , raporlama sürecinde doğru evrene taşınan REP miktarıdır. Böylece bir saldırganın başarılı olabilmesi için en az $SM +$ taşınması lazım. Kolaylık için, önemsiz olanları görmezden gelip başarılı bir saldırı için taşınmadan önce $SM + \epsilon$ değeri olan SM REP'in bir yanlış evrene taşınması gerektiğini söyleyelim.

Eğer bir saldırgan çatallaşmanın raporlama aşaması sırasında SM REP taşırırsa, taşıdığı evrende SM REP

alacaktır.²³ Eğer saldırgan bir Yanlış evrene taşırırsa o sanal paraların değeri $SM P_f$ olur. Böylece, saldırganın asgari masraf $(P - P_f)SM$ olur.

Gözlem 2. Çatallaşma sırasında başarılı bir saldırganın bir Yanlış evrene taşınması gereken REP miktarı SM 'dir, bunun saldırganın masrafı $(P - P_f)SM$ 'dir.

Eğer $S > \frac{1}{2}$ ise bir saldırı imkânsız hale gelir çünkü doğru evrenin dışındaki bir yanlış evrene galibiyet sağlayacak kadar REP yoktur.

Ekonomik olarak makul saldırganlara karşı bırakıldığında, kâhin, eğer saldırma masrafı azami kazançtan fazla ise gerçeklikle uyumlu olan sonuçlara çözümleyecektir. 1. ve 2.incelemedeki $S > \frac{1}{2}$ ya da $I_a + I_p < (P - P_f)SM$ durumuna bakarak bunu anlayabilir. Bu bize bütünlüğün resmi tanımını verir..

Tanım 4. (Integrity Property) $S > \frac{1}{2}$ ya da $I_a + I_p < (P - P_f)SM$ olduğunda çatallaşma protokolü bütünlük içindedir.

Yukarıdaki eşitsizlik, çatallaşma protokolü bütünlüğü ile REP'in piyasa değeri arasında ilişkiyi göstermek için PM için* çözülebilir.

Teorem 1. (Market Cap Security Theorem) Çatallaşma protokolünün bütünlük arz etmesi için ancak ve ancak:

1. $S > \frac{1}{2}$, ya da

2. $P_f < P$ olması ve REP'in piyasa değerinin $\frac{(I_a + I_p)P}{(P - P_f)S}$ 'dan daha büyük olması gerekir.

Proof. Çatallaşma protokolünün bütünlük arz ettiğini varsayalım. Sonra tanım gereği $S > \frac{1}{2}$ ya da $I_a + I_p < (P - P_f)SM$. $I_a + I_p < (P - P_f)SM$ olduğunu varsayalım. $I_a + I_p \geq 0$ ve $SM > 0$ olduğundan dolayı, $P_f < P$ sonucuna ulaşıyoruz. Sonrasında $I_a + I_p < (P - P_f)SM$ 'yı PM ile çözersek, $\frac{(I_a + I_p)P}{(P - P_f)S} < PM$ sonucunu buluruz. Bu da bizim ilk gidiş yolumuzun doğruluğunu ispatlar.

Şimdi de $S > \frac{1}{2}$ olduğunu varsayalım, ya da $P_f < P$ and $\frac{(I_a + I_p)P}{(P - P_f)S} < PM$. If $S > \frac{1}{2}$, bu durumda çatallaşma bütünlük arz eder. Eğer $P_f < P$ ve $\frac{(I_a + I_p)P}{(P - P_f)S} < PM$ ise $I_a + I_p$ ile bu denklemi çözdüğümüzde $I_a + I_p < (P - P_f)SM$ sonucuna ulaşırı ve bu sonuç çatallaşma protokolünün bütünlük arz ettiğini gösterir. \square

B. Varsayımlarımız ve Sonuçları

Tüccarların, muhabirlerin yalan söylediği bir Augur evreninde ticaret yapmak istemeyeceklerine

²¹ 1 attorep = 10^{-18} REP.

²² Kötü niyeti olmayan muhabirlerin yanlışlıkla veya umursamazca Yanlış evrene REP taşımaları mümkündür. Ancak bu tarz davranışlar saldırganla iş birliğiyle ayırt edilemez.

²³ Gerçekte, saldırgan çatallaşmanın ilk 60 gününde REP taşıdığı için %5 primiyle beraber çocuk evrende 1.05SM REP kazanırdı ama kolaylık için bunu görmezden geldik. %5 ödüllendirme konuşması için en C'ye bakınız C.

inıyoruz. Ticaretlerin olmadığı bir evrende piyasa oluşturmalarının ödeme yapıp piyasa oluşturmak istemeyeceklerine de inanıyoruz. Piyasasız ve ticaretsiz bir evrende REP, sahibine kâr sağlamaz. Bu nedenle, yanlış bir evrene taşınan REP'in kayda değer bir alım gücü olmayacağına inanıyoruz. Bu durumu böyle gösteriyoruz: $P_f = 0$.

Var olan REP'in en az 20% sinin çatallaşma aşamasının raporlama sürecinde doğru sonuca taşınacağını beklemenin mantıklı olduğunu düşünüyoruz and bunu böyle gösteriyoruz: $S \geq \frac{1}{5}$. Ayrıca yerel açık faizin 50%'si kadar parazit açık faizi barındırmaya razıyız. Böylece, $I_a \geq 2I_p$ olur.

Bu varsayımlar bağlamında, Theorem 1 1 bize REP'in piyasa değeri, yerel açık faizin 7.5 katı olduğunda çatallaşma protokolünün bütünlüğe sahip olduğunu gösterir.²⁴

C. Piyasa Bonusu

Augur, REP'in değerini gerçek dünya hakkında her bilgiye ulaşma yoluyla alır: bir Augur piyasasıyla. Böyle Augur REP'in piyasa değerini hesaplayabilir. Augur güncel açık faizi de hesaplayabilir ve böylece tutarlılığın sağlanması için hangi piyasa değerinin hedeflenmesi gerektiğini belirler.

Her evren 1% raporlama ücreti ile başlar. Eğer güncel piyasa değeri hedefin altındaysa raporlama ücretleri otomatik olarak yükseltilir (ama asla 33%'den fazla olmaz). Böylece REP'in değeri artmaya ve yerel açık faiz azalmaya zorlanır. Eğer yürürlükte olan piyasa değeri hedefin üstündeyse, raporlama ücretleri otomatik olarak azaltılır (ama 0.01% in altına düşürülmez). Böylece Tüccarlar sistemi güvenli tutmak için ödemeleri gerekenin üstünü ödemek zorunda kalmazlar.

Raporlama ücretleri şu şekilde hesaplanır: r bir önceki ücret aralığında raporlama ücreti olsun, t hedeflenen piyasa değeri olsun ve c güncel piyasa değeri olsun. Böylece yürürlükte olan raporlama ücret aralığının raporlama ücreti $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10,000}\right\}$ ile hesaplanabilir.

D. Çatal Tehdidi

Yukarıda bahsedildiği gibi, çatallaşmalar piyasaların sonuçlanması için aksatıcı ve yavaş yöntemlerdir. Her piyasayı sonuçlandırmak için çatallaşma kullanmak yerine, Augur piyasaları etkili bir şekilde sonuçlandırmak için çatallaşma tehdidini kullanır.

Bir sonuca marketin nihai sonucuyla karşı çıkan

her hissenin 50% getirisi olacağını hatırlayın.²⁵ Bir Çatallaşma gerçekleştiğinde, piyasanın yanlış sonuçlarına yatırılan REPlar değerlerini kaybederler. Piyasanın doğru sonucuna yatırılan bütün REPlar piyasanın doğru sonucuyla uyumlu olan çocuk evrende (çatallaşmanın sonucuna bakmaksızın) 50% daha fazla REP ile ödüllendirilir. Bu nedenle, eğer çatallaşmaya zorlanırsalar, doğru sonuçların lehine yanlış sonuçlara karşı çıkan REP sahipleri her zaman kârlı çıkarlar. Yanlış sonuca yatırım yapan REP sahipleri, REPlarının bütün ekonomik değerini kaybettiğini görürler

Bu durumun bütün kesin olmayan yanlış sonuçlara karşı çıkılmasını garantilediğine inanıyoruz.

III. POTANSİYEL SORUNLAR VE RİSKLER

A. Parazit Piyasalar

Parazit piyasalar, Augur'a raporlama ücreti ödemeyen ama Augur'un yerel piyasalarıyla uyumlu bir şekilde sonuçlanan piyasalardır. Parazit piyasaların ödüllendireceği muhabirleri olmadığından Augur'un hizmetinin aynısını daha ucuza sunabilirler. Bu Augur'un çatallaşma protokolünün bütünlüğü için ciddi sorunlar teşkil edebilir.

Özellikle, parazit piyasalar ticaret faizini Augur'dan çekerlerse Augur'un muhabirleri raporlama ödemelerinden daha az kazanır. Bu durum REP in piyasa değerini aşağıya çeker. Eğer REP'in piyasa değeri çok düşerse, çatallaşma protokolünün bütünlüğü tehlikeye atılır (Theorem 11). Sonuç olarak, parazit piyasalar Augur'un uzun vadeli kullanımını tehlikeye atarlar ve şiddetle karşı çıkılmalıdır.

Parazit piyasalara karşı en iyi savunmamız, parazit piyasa sahibi olmanın kârını düşük tutmak için Augur platformunda ticareti (kehanetin bütünlüğünü devam ettirerek) tutabildiğimiz kadar düşük tutmaktır.

B. Açık Faizin Dalgalanması

Açık faizde büyük, ani ve beklenmedik artmalar - popüler spor etkinliklerinde görülenler gibi- çatallaşma protokolünün bütünlüğü için piyasa değerinin ani yükselişi için ihtiyaca neden olurlar. (Theorem 1). Gereken piyasa değeri, piyasa değerini geçtiğinde ekonomik olarak makul davranan saldırganların yanlış sonuçlandırmak için çatallaşmaya neden olması riski ortaya çıkar. Augur böyle durumlarda piyasa değerini yükselmeye itelesen de, bu itelemeler tepkiseldir ve 7 günlük bir süre içinde sadece bir kez düzenlenirler (see Section II C)

²⁴ Alternatif varsayım ve neticeler için B'e bakınız.

²⁵ Evrendeki mevcut REP miktarı sonucu etkileyebilir; detaylar için: 3 A.

Açık faizin ani artışını fark eden vurguncular piyasa değerinin tepkisel itelenmesi beklentisiyle REP alabilirler, böylece, REP'in piyasa değeri belki de çatallaşma protokolünün tehditten kurtulana kadar yukarı çekilir. Bu yüzden, kehanetin zayıf kaldığı süre, bir saldırganın zayıflığı istismar etmesi için yeterince uzun olmayabilir.

C. Tutarsız veya Kötü Niyetli Sonuç Kaynakları

Piyasa yaratımı sırasında, olayın sonucunu belirlemek için muhabirlerin kullanabileceği bir çözüm kaynağı seçerler. Eğer piyasa yaratıcısı tutarsız ya da kötü niyetli bir çözüm kaynağı seçerlerse, dürüst muhabirler para kaybedebilir.

Örnek olarak, diyelim ki piyasanın A ve B sonuçları var ve piyasa yaratıcısı, Serena, çözüm kaynağı olarak kendi sitesi, *attacker.com*'u seçti. Piyasanın olay bitiş süresinden sonra, Serena (aynı anda atanmış muhabir olarak) A sonucunu raporlar ve *attacker.com*'u güncelleyip B sonucunun doğru sonuç olduğunu gösterir. *attacker.com*'a bakan dürüst muhabirler ilk raporun yanlış olduğunu görüp ilk itiraz aşamasında başarılı olarak kesin olmayan sonuca B sonucuyla karşı çıkarlar. Serena *attacker.com*'u yeniden günceller ve A sonucunun doğru sonuç olduğunu gösterir ve piyasa ikinci itiraz aşamasına girer. Muhabirler tekrar *attacker.com*'u kontrol edip kesin olmayan B sonucunun yanlış olduğunu görürler ve başarılı bir şekilde karşı çıkarlar. Serena, piyasa sonuçlanana kadar bu davranışına devam edebilir. Piyasa nasıl sonuçlanırsa sonuçlansın bazı dürüst muhabirler para kaybederler.

Bu saldırının farklı türleri olabilir. Şüpheli çözüm kaynakları olan piyasaları görmezden gelmek yeterli değil, eğer bu piyasalardan birisi bir çatallaşmaya neden olursa, bütün REP sahiplerinin REPlerini taşımak için bir çocuk evren seçmeleri gerekir. Muhabirler şüpheli çözüm kaynaklarına sahip olan piyasalara karşı tetikte olmalı. Muhabirlerin, bu piyasaları geçersiz olarak sonlandırmak için işbirliği yapıp bu piyasaların alenen tanımlanmaları gerekir.

D. Self-Referential Oracle Queries

Augur'un kâhininin gelecekteki davranışları üzerine ticaret yapan piyasaların kâhinin üzerinde olumsuz etkileri olabilir [11]. Örnek olarak, "Atanmış muhabirlerden birisi 31 Aralık 2018'den önce üç günlük raporlama sürecinde rapor vermede başarısız olacak mı?" sorusu üzerine ticaret yapan bir piyasa düşünelim. Hayır sonucuna yatırılan bahisler atanmış muhabirleri rapor vermemeye teşvik edebilir. Bir atanmış muhabir ucuz fiyata yeterince Evet hissesi alıp görünmeyen tahvil kaybını karşılayabilirse, rapor vermeyebilir.

Eğer piyasanın REP değeri yeterince yüksek ise özgönderimsel kâhin sorguları çatallaşma sürecinin bütünlüğü için tehdit oluşturmaz (Theorem 1). Yine de,

piyasaların sonuçlanmasını geciktirerek Augur'un performansını olumsuz bir şekilde etkileyebilirler. Piyasalar doğru sonuçlanırdı ama bu tür davranışlar yine de ak-satıcılar ve sakıncalıdır.

E. Belirsiz Çatallaşma Katılımı

Bir çatallaşmada ne kadar REP'in Gerçek evrene taşınacağını bilemeyiz. Bu nedenle piyasa değerinin kehanetin bütünlüğünü sağlayacak kadar yüksek olup olmayacağını bilemeyiz. Çatallaşma protokolünün bütünlüğüne inancımız, dürüst katılımın alt sınırı hakkında varsayımlarımıza inancımızdan daha güçlü olamaz. Bütün REP'in en az 20%'sinin doğru çocuk evrene taşınacağını tahmin ediyoruz, ama bunu garantileyemeyiz.

Augur çatallaşmaları başka blok zincirlerinin çatallaşmalarından önemli bir yönden ayrılır: bir blok zinciri çatallaşmasından sonra, ebeveyn zincirde bir sanal paraya sahip olan kullanıcı iki çatallaşmada bir sanal paraya sahip olur. Tekrarlama saldırılarını görmezden gelirse, blok zinciri çatallaşmaları kullanıcılara az risk arz eder. Ancak bir Augur çatallaşmasından sonra, ebeveyn evrende bir tokene sahip olan bir kullanıcı sanal parasını çocuk evrenlerden sadece birisine taşıyabilir. Eğer kullanıcı mutabakat evreninden başka bir evrene tokenlerini taşırlarsa, tokenleri tüm değerini kaybedebilir. Bu nedenle, çatallaşma sürecinde henüz hangi çocuk evrenin mutabakata ulaştığını bilmeden REP taşımak kullanıcılar için risklidir. Bu risk, tartışmalı çatallaşmalarda kullanıcıların katılımdan caydırabilir.

Çatallaşma aşamalarında katılma teşvik için, çatalın başlangıcını takiben 60 gün içerisinde REPlerini taşıyan token sahipleri, REPlerini taşıdıkları çocuk evrende 5% ilave token alırlar (Bölüm IC9'ye bakınız). Fakat, bu 5%'lik primin, çatallaşma aşamasında riski karşılamak ve katılma teşvik etmek için yeterli olup olmayacağını önceden bilemeyiz.

F. Belirsiz veya Öznel Piyasalar

Sadece nesnel olarak bilinebilen sonuçları olan olaylar Augur piyasalarında kullanıma uygundur. Eğer muhabirler bir piyasanın platformda çözüme ulaşmaya uygun olmadığını düşünürlerse (belirsiz olduğu için, öznel olduğu için veya sonucun olay bitiş tarihinde bilinmediği için) piyasanın Geçersiz olduğunu raporlamalıdır. Eğer bir piyasa Geçersiz olarak sonuçlanırsa, tüccarlar her sonuç için eşit değerlerde geri ödemelerini alırlar; sayısal piyasalar için, tüccarlar piyasanın azami ve asgari değerinin tam ortasında ödemelerini geri alırlar.

Bazı muhabirlerin A sonucunun doğru olduğuna ve diğer muhabirlerin B sonucunun doğru olduğuna emin oldukları bir piyasa düşünmek kolay. Örnek olarak, 2006'da Tradesports kullanıcılarının, Kuzey Kore'nin Temmuz 2006'dan önce hava sahasının dışına balistik

füze atıp atamayacağı konusunda bahis oynamasına izin verdi. 5 Temmuz 2006'da Kuzey Kore, başarılı bir şekilde hava sahasının dışına düşen bir balistik füze attı, olay dünya medyası tarafından yaygın olarak rapor edildi ve birçok ABD devlet kaynağı tarafından doğrulandı. Ancak Tradesports şartnamesinde gerekçe olan ABD Savunma Bakanlığı olayı doğrulaması gerçekleşmedi. Tradesports şartnamenin gerekçelerinin gerçekleşmediğine karar verdi ve uygun bir şekilde ödeme yaptı.²⁶

Bu, piyasanın ruhunun gerçekleştiği (füzenin atılışının tahmin etmek) ama şartların gerçekleşmediği(atılışın ABD savunma bakanlığı tarafından doğrulanması) bir vaka. Merkezi bir site olan Tradesports tek taraflı bir

şekilde piyasanın sonucuna karar verebildi. Eğer böyle bir durum Augur piyasalarından birinde gerçekleşirse, REP sahiplerinin piyasanın nasıl sonuçlanacağı hakkında farklı düşünceleri olabilir ve uygun bir şekilde REPlarını yatırabilirler. En kötü halde, bir çatallaşma gerçekleşir..

IV. TEŞEKKÜRLER

Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow ve Peronet Despeignes'e faydalı geribildirimleri ve önerileri için teşekkür ederiz.

-
- [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.
 - [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 10th 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.

²⁶Detaylar için <https://en.wikipedia.org/wiki/Intrade#Disputes> 'bakınız.

Appendix A: Sonuçlandırma & Yeniden Dağıtım

Bazı formüllerle, tariflerle ve incelemelerle başlayalım.

Tanım 5. M piyasası için; Ω_M , M 'nin sonuçlar dizisi olsun ..

Tanım 6. $n \geq 1$ ve $\omega \in \Omega_M$ için, $S(\omega, n)$ itiraz aşaması n için ω sonucunda hisselerin tamamı olsun. Bu, geçmişte of ω sonucu için başarılı olan itiraz tahvillerini de içerir.

Tanım 7. $n \geq 1$ ve $\omega \in \Omega_M$, $S(\bar{\omega}, n)$ tüm sonuçların hisse miktarı olsun Ω_M hariç ω itiraz aşamasının başındaki n :

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

Tanım 8. $n \geq 1$, A_n tüm sonuçlardan gelecek hisse miktarı olsun M itiraz aşamasının başındaki n :

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

Gözlem 3. Formülü takiben $A_n - S(\omega, n) = S(\bar{\omega}, n)$.

Tanım 9. $n \geq 1$ için; let $\hat{\omega}_n$ itiraz aşamasındaki geçici gider n . Örneğin; $\hat{\omega}_1$ ilk muhabir tarafından verilen başlangıç raporu olur.

Tanım 10. $n \geq 1$ ve $\omega \neq \hat{\omega}_n$ olduğu itiraz aşamasında n sırasında ω lehine bir itiraz tahvili doldurulursa; $B(\omega, n)$ oluşur. Bu itiraz aşaması n sonundaki başarılı itiraz hissesi, ω ise uygulanan tek yeni hissedir.

$\omega \neq \hat{\omega}_n$ olduğu itiraz aşamasında n sırasında ω sonucu lehine bir itiraz tahvili doldurmak için gereken hisse miktarının denklem ile verildiğini hatırlayın. Eq. 1, $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Gözlem 4. Eğer itiraz aşaması n sırasında ω sonucu lehine bir itiraz tahvili doldurursa; $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Bu durumda n sürecinin sonunda ω kadar bir itiraz başarılı sayılmış olur.

Gözlem 5. Bütün $\omega \neq \hat{\omega}_n$, $S(\omega, n-1) = S(\omega, n)$ denklemleri için. Eğer ω sonucu lehine bir itiraz tahvili doldurulmamışsa, bir sonraki itiraz aşamasının başlangıcında ω sonucuna ilave hisse eklenmez. Bunun nedeni, itiraz aşaması sonucunda başarısız itiraz hisselerinin kullanıcılara geri verilmesidir.

Gözlem 6. Bütün $n \geq 2$, $A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$ değerleri için. Böylece, bir itiraz aşaması başlangıcında bütün sonuçlarda bulunan hisseler, bir önceki itiraz aşamasının başlangıcındaki hisseler ve bir önceki itiraz aşamasında başarılı olan itiraz hisseleridir. Diğer bütün hisseler bir önceki itiraz aşaması sonunda kullanıcılara geri verilir.

Önsav 2. $S(\hat{\omega}_n, n) = 2S(\bar{\hat{\omega}_n}, n)$, $n \geq 2$ için.

Proof. İtiraz aşamasının n olduğu, $n \geq 2$ ile bu aşamada olan bir durum düşünelim. İtiraz aşaması boyunca $n-1$ sırasında $\hat{\omega}_{n-1}$ değerine karşılık verebilmeli. $\hat{\omega}_n$. Verilen denkleme göre Eq. 1, bu itiraz tahvilinin boyutu $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$ olmalı. Çeşitli incelemelerle bu tekrardan yazılabilir. 3

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

İtiraz aşaması $n-1$ noktasında başarıyla tamamlandı. Verilen denklemi incelersek4, bu denklemi sağladığını görürüz. $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. incelemeler 5 yatırılan toplam miktarın $\hat{\omega}_n$ ilk iki aşamada değişmediğini $n-1$ to n , $2S(\hat{\omega}_n, n-1) = 2S(\bar{\hat{\omega}_n}, n)$. böylece bu değer, Eq. A1 son denklemde buraya girdiğini görüyoruz. $S(\hat{\omega}_n, n) = 2S(\bar{\hat{\omega}_n}, n)$. \square

Teorem 3. Piyasa, bir başka piyasada oluşan çatallaşma tarafından sekteye uğramazsa, bir sonuca, piyasanın nihai sonucu lehine başarıyla karşı çıkan REP sahipleri itiraz hisselerinden 50%kâr alacak (piyasanın nihai sonucuyla uyuşan çocuk evrenin REPiyle hesaplanır).

Proof. Çatallaşma sırasında, çatallaşan piyasanın nihai sonucunun itiraz tahvili başarıyla dolduran bütün kullanıcılar, sonuçla uyumlu olan çocuk evrene taşıdıklarında itiraz hisselerinden 50% kâr (sanal paralar çatallaşma sırasında basılır) kazanırlar. Böylece, söz konusu piyasanın çatallaşmaya neden olduğu durumda, teori doğrudur.

Şimdi, söz konusu piyasanın çatallaşma gerçekleşmeden çözümlenmesi ve raporlamanın başka bir piyasanın çatallaşmasıyla bölünmemesi durumunu düşünelim.

Piyasanın nihai sonucu ω_{Final} olsun ve $n \geq 2$ itiraz aşamasında n sonucunda da piyasanın sonuçlandığını varsayalım. n süreci için geçici olmayan sonuç: ω_{Final} , ve bu denkleme başarılı bir itiraz gerçekleşemedi. n . Başka bir deyişle: $\hat{\omega}_n = \omega_{\text{Final}}$. Lemma'yı kullanırsak 2 bilgisine ulaşırız. $S(\omega_{\text{Final}}, n) = 2S(\bar{\omega_{\text{Final}}}, n)$.

Piyasa n aşaması sonunda herhangi bir sonuca hisse eklenmeden çözümlendiği için, yukarıdaki denklem piyasanın nihai sonucunda bulunan kesin hisse miktarını ω_{Final} ve piyasanın diğer sonuçlarının hisselerinin toplamını $\bar{\omega_{\text{Final}}}$ gösterir.

Piyasanın nihai sonucunda, diğer sonuçların tam olarak iki katı kadar hisse olduğuna dikkat edin. Augur nihai olmayan bütün sonuçların hisselerinin tamamını, (yatırdıkları REP ile orantılı olarak) nihai sonuca yatırım yapan kullanıcılara dağıtır. Bu nedenle ω_{Final} lehine bir itiraz tahvilini başarıyla dolduran bütün kullanıcılar yatırdıkları REPTen 50% kâr kazanırlar. \square

Sonra, bir piyasayı çözümlemek için gereken azami itiraz aşaması sayısını düşünelim. ω itiraz aşamasını en fazla hisseyle başlatan kesin olmayan sonuç olarak seçildiğinde denklem Eq. 1 küçülür. 2 en büyük hisseye sahip olan kesin olmayan hissenin bir önceki itiraz aşamasının kesin olmayan sonucu olduğunu ifade eder. Bu nedenle $n \geq 2$ olduğu itiraz aşamasının n sırasında

başarıyla doldurulabilecek en küçük itiraz tahvilinin boyutu; $B(\hat{\omega}_{n-1}, n)$ olu.

Başka bir deyişle, itiraz tahvilinin en yavaş dolduğu zaman, aynı iki sonuca tekrar tekrar birbirileri lehine karşı çıkıldığı zamandır. Bununla birlikte, bir piyasanın çatallaşması için gereken itiraz aşamalarının sayısı, aynı iki sonuca tekrar tekrar lehine karşı çıkıldığı zaman azamiyete ulaşır. Bu nedenle, bir çatallaşma gerçekleşmeden herhangi bir piyasanın geçirebileceği azami itiraz aşaması sayısını, birbirleri lehine tekrar tekrar karşı çıkılan kesin olmayan sonuçların olduğu bir vakada gerçekleştirebilecek azami itiraz aşaması sayısını bularak tespit edebiliriz. Şimdi bu vakayı inceleyelim.

Her başarılı itiraz tahvilinin bir önceki itiraz aşamasının kesin olmayan sonucunun lehine doldurulduğunu varsayalım. Sonra, birbirleri lehine tekrar tekrar karşı çıkılan kesin olmayan sonuçlar $\hat{\omega}_1$ ve $\hat{\omega}_2$ olsun.

Gözlem 7. Aynı iki sonuca tekrar tekrar birbirileri lehine karşı çıkıldığı vakalarda, $\hat{\omega}_n = \hat{\omega}_{n-2}$ tümü için $n \geq 3$.

Tanım 11. İlk rapor sırasında $\hat{\omega}_1$ 'e yatırılan hisse miktarını d ile gösterelim. Çünkü her aşama için kesin olmayan sonucu bu durumda biliyoruz. İtiraz tahvili boyutları için formülümüzü basitleştirebiliriz. Her $n \geq 2$ için; $B_1 = 2d$ and $B_n = B(\hat{\omega}_{n-1}, n)$ n tahvil boyutu için kısa bir tahvil B_n tanımlayalım.

Gözlem 8. Her geçici sonuca tekrar tekrarkarşı çıkılabilir, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ for $n \geq 3$. (Her başarılı itiraz tahvili aynı başlığa eklenir..)

Önsav 4. Aynı iki sonuca tekrar tekrar birbirileri lehine karşı çıkıldığı vakada $n \geq 3$ için n

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

Proof. (n üzerinden tümevarım ile;)

Aynı iki sonuca tekrar tekrar birbirileri lehine karşı çıkıldığını varsayalım.

(Temel Durum) Tarif ve denklem. 1 ile aşağıdaki tespitlerde bulunabiliriz;

- $S(\hat{\omega}_1, 1) = d$, $S(\hat{\omega}_2, 1) = 0$, $A_1 = d$, 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 $B_3 = 6d$

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, Böylece ilk ön sav doğrudur. $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, $n = 3$ değeri için ikinci önsav doğrudur.

$B_3 = 6d = 3d2^{3-2}$, $n = 3$ değeri için bu denklemde de önsav doğrudur.

$n = 3$ durumu için tüm denklemler doğru bir yargıya ulaştığı için önsav doğrudur.

(Tümevarım) Önsavın bütün n için doğru olduğunu varsayalım, öyle $3 \leq n \leq k$. Önsavın $n = k + 1$ için doğru olduğunu göstermek istiyoruz. Böylece,

- (a) $S(\hat{\omega}_k, k + 1) = \frac{2}{3}B_k$
- (b) $A_{k+1} = 2B_k$ and
- (c) $B_{k+1} = 3d2^{k-1}$

Önce A kısmı aşağıdaki inceleme ile ispatlanır. 8:

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

İnceleme 7'yi tekrar yukarı yazabiliriz:

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

Tümevarım yöntemiyle $S(\hat{\omega}_{k-2}, k - 1)$ 'değerini $\frac{2}{3}B_{k-2}$ olarak denklemin sağ tarafına yerleştirerek aşağıdaki sonuca ulaşırız:

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

Tümevarım yöntemiyle B_{k-2} değerini $3d2^{k-4}$ ve B_{k-1} olarak yazabiliriz $3d2^{k-3}$:

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

Sol tarafa 7 uygularsak:

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

Son olarak yukarıdaki denklem ve tümevarım hipotezi yardımıyla; $S(\hat{\omega}_k, k + 1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. This proves part (a).

Sonrasında 6 ile B kısmını ispatlıyoruz:

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

Tümevarım yöntemiyle, $A_k = 2B_{k-1}$:

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

Tümevarım sonrası $B_{k-1} = 3d2^{k-3}$, sağ tarafta sadeleştirme yapabiliriz işlem kolaylığı adına.

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

Tümevarım uygularsak, $B_k = 3d2^{k-2}$ değerini denklemin sağına

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

yazabiliriz, bu da B aşamasını kanıtlar.

Son olarak 1:ile C aşamasını kanıtlıyoruz.

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

İncelersek 8 şeklinde yazabiliriz $S(\hat{\omega}_k, k + 1)$ as $S(\hat{\omega}_k, k - 1) + B_{k-1}$:

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

İncelersek 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

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

İncelersek ??, $A_{k+1} = A_k + B_k$:

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

Tümevarım yöntemiyle, $A_k = 2B_{k-1}$ and $S(\hat{\omega}_{k-2}, k - 1) = \frac{2}{3}B_{k-2}$:

$$B_{k+1} = 2(2B_{k-1} + B_k) - 3(\frac{2}{3}B_{k-2} + B_{k-1})$$

Tümevarım yöntemiyle, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ and $B_{k-2} = 3d2^{k-4}$ sonucuna ulaştıktan sonra gerekli işlem ve sadeleştirmeyi yaparsak:

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

Bu da C önsavının da doğruluğunu ispatlar. \square

Teorem 5. *Eğer başka bir piyasanın çatallaşmaya neden olmasından dolayı aksamazsa, bir piyasa sonuçlanmadan veya çatallaşmaya neden olmadan en fazla 20 itiraz aşamasından geçebilir.*

Proof. Belirli bir piyasanın, başka bir piyasanın çatallaşmaya neden olmasıyla aksamaya uğramadığını varsayalım. Sonra, yukarıda gösterildiği gibi, bir piyasanın çatallaşmaya neden olması için gereken itiraz aşaması sayısının aynı iki sonuca tekrar tekrar birbirileri lehine karşı çıkıldığında azamiyete ulaştığını biliyoruz. Önsavın 3. kısmı bize, bu durumda n aşamasında kesin olmayan sonuca başarıyla itiraz için gereken itiraz tahvilinin boyutunun, ilk rapora yatırılan hisse miktarının d ile gösterildiği $3d2^{n-2}$ ile verildiğini gösterir.

Çatallaşmaların, en az bütün REP'in 2.5%'i boyutunda bir itiraz tahvilinin başarılı bir şekilde doldurulmasıyla başladığını ve 11 milyon REP'in var olduğunu biliyoruz. Böylece, çatallaşmalar 275,000 REP boyutunda bir itiraz tahvili doldurulduğunda başlarlar. $d \geq 0.35$ REP olduğunu da, ilk raporda minimum hissenin 0.35 REP olduğunu da biliyoruz 27.²⁷

$3(0.35)2^{n-2} > 275,000$ işlemi $n \in \mathbb{Z}$ $n \geq 20$ sonucunu veriyor. Böylece, en fazla 20 itiraz aşamasından sonra piyasanın ya çözüleceğini ya da çatallaşmaya neden olacağını garanti edebiliriz.. \square

Appendix B: Alternatif Varsayımlar & Sonuçları

Hatırlatacak olursak;

- S çatallaşma aşamasında çocuk evrene taşınan bütün REP'in miktarıdır
- P Doğru evrende REP'in değeridir
- P_f saldırganın seçtiği bir yanlış evrene taşınan REP'in değeridir.
- I_a Augur'un yerel açık faizidir
- I_p parazit açık faizdir

Augur, piyasa değerine ulaşmak için; S , P_f ve I_p hakkında belli varsayımlarda bulunur. Özellikle, Augur bütün REP'in en az 20%'sinin çatallaşma aşamasında doğru evrene taşınacağını varsayar. Bir Yanlış evrene taşınan REP'in göz ardı edilemez bir değeri olmaya caktır ve parazit açık faizi yerel açık faizin en az yarısı olacaktır. Başka bir deyişle $S \geq 0.2$, $P_f = 0$ ve $I_a \geq 2I_p$. Bu varsayımlar altında, Theorem 1 bize REP'in piyasa değerinin yerel açık faizin 7.5 katından fazla olduğunda çatallaşma protokolünün bütünlüğünün olduğunu gösterir.

S , P_f ve I_p hakkında kendi varsayımlarınızla; kehanetin pratikte bütünlüğünün olması için piyasa değerinin ne kadar olması gerektiği hakkında kendi sonuçlarınıza varabilirsiniz. Rahatlığınız için size birkaç senaryo listeledik.

Senaryo 1. Mevcut REP'in 50%'inden fazlası çatallaşma aşamasında doğru evrene taşınır. Bu durumda P_f ve I_p 'nin önemi kalmaz çünkü $S > \frac{1}{2}$, piyasa değeri ne olursa olsun çatallaşma protokolünün bütünlüğü vardır. Bir saldırganın başarılı olması için piyasada yeterince REP kalmamıştır.

Senaryo 2. Mevcut REP'in 48%'i çatallaşma aşamasında doğru evrene taşınır, parazit piyasalar yoktur ve bir yanlış evrene yollanan REP'in değeri yoktur. Bu $S = 0.48$, $I_p = 0$, ve $P_f = 0$. Bu durumda, çatallaşma protokolünün güvenilir olması için REP'in piyasa değeri yerel açık faiz'in iki katından fazla olmalıdır.

Senaryo 3. Mevcut REP'in 20% 'si çatallaşma aşamasında doğru evrene taşınır, parazit açık faizi yerel açık faize eşittir ve bir yanlış evrene taşınan REP'in değeri doğru evrene taşınan REP'in 5%'i kadardır. Bu durumda, $I_p = I_a$, ve $P_f = 0.05P$. Bu durumda, çatallaşma protokolünün bütünlüğünün olması için REP'in piyasa değeri yerel açık faizin 10.5 katından fazla olmalıdır.

Senaryo 4. Mevcut REP'in sadece 5% 'i çatallaşma aşamasında doğru evrene taşınır, parazit açık faiz yerel açık faizin iki katıdır ve bir Yanlış evrene taşınan REP'in değeri doğru evrene taşınan REP'in 5%'i kadardır. Bu

²⁷Detaylar için; E2 ve E3

durumda, $S = 0.05$, $I_p = 2I_a$ ve $P_f = 0.05P$. Bu durumda, çatallaşma protokolünün bütünlüğünün olması için REP'in piyasa değeri yerel açık faizin 63 katından fazla olmalıdır.

Appendix C: Erken Taşıma Priminin Çatallaşma Protokolünün Bütünlüğüne Etkisi

Kolaylık için, çatallaşma protokolünün bütünlüğünü anlatırken 5% erken taşıma primini ve küçük bir terimi* görmezden geldik. Burada, görmezden geldiğimiz bu iki etkeni göz önünde bulundurarak Teori 1'i tekrar gözden geçireceğiz.

Önceden yaptığımız gibi, raporlama aşaması sırasında doğru evrene yollanan REP miktarı SM ile gösterilir. Böylece, bir saldırganın başarılı olması için taşınmadan önce değeri $(SM + \epsilon)P$ olan en az $SM + \epsilon$ REP'i bir yanlış evrene taşınması gerekir.

Önceden yaptığımız gibi, raporlama aşaması sırasında doğru evrene yollanan REP miktarı SM ile gösterilir. Böylece, bir saldırganın başarılı olması için taşınmadan önce değeri $(SM + \epsilon)P$ olan en az $SM + \epsilon$ REP'i bir yanlış evrene taşınması gerekir. Eğer bir saldırgan çatallaşmanın raporlama aşamasında bir yanlış evrene $SM + \epsilon$ taşırsa, taşıdığı çocuk evrende $1.05(SM + \epsilon)REP$ alır. P_f tarifine göre, bu tokenlerin değeri $1.05(SM + \epsilon)P_f$ ile belirlenir. Böylece, saldırganın asgari masrafı $(SM + \epsilon)P - 1.05(SM + \epsilon)P_f$ 'dır, $((SM + \epsilon)(P - 1.05P_f))$ ile de gösterilebilir.

Önceden bahsedildiği gibi, bir saldırganın azami (brüt) kârını $I_a + I_p$ ile bulabiliriz. Böylece çatallaşma protokolünün bütünlüğünün olduğunu ne zaman $S > \frac{1}{2}$ ya da:

$$I_a + I_p < (SM + \epsilon)(P - 1.05P_f) \quad (C1)$$

Yukarıdaki eşitsizliği piyasa değeri için çözerken, PM , çatallaşma protokolünün bütünlüğünün olduğunu ancak ve ancak:

1. $S > \frac{1}{2}$ ya da
2. $1.05P_f < P$ ve piyasa değerinin daha büyük olduğu durumda görürüz $\frac{P(I_a + I_p - \epsilon(P - 1.05P_f))}{S(P - 1.05P_f)}$

Görüldüğü üzere erken taşınmanın piyasa değeri üzerindeki etkisi bir hayli düşük.

Appendix D: Taşıma Priminin Bir Çatallaşmanın Asgari Masrafına Etkisi

Çatallaşma aşamalarında katılma teşvik için, Çatallaşmanın başlangıcını takiben 60 gün içerisinde REPlarını taşıyan token sahipleri, REPlarını taşıdıkları çocuk evrende 5% ilave token kazanırlar. Bu ödül para enflasyonu ile ödenir.

Eğer çatallaşma başlatma masrafı çok düşük ise, bu prim ters teşvike dönüşebilir. Özellikle, bir saldırganın 5%lik primden kazancını çatallaşma başlatma masrafından daha fazla ise, çatallaşmaların mümkün olduğunca sık gerçekleşmesini bekleriz. Enflasyon sağma saldırısı ismini verdiğimiz bu saldırı kâhinin yanlış rapor vermesine neden olmaz, ancak aksatıcı çatallaşmaların sıklıkla gerçekleşmesine neden olur.

Bu davranışı önlemek için Augur'un, 5% enflasyon priminden azami kazancın çatallaşma başlatma masrafından daha az olduğundan emin olması gerekiyor. Burada, bu ters teşviki önlemek için daha düşük bir çatallaşma başlatma ücret sınırı türetiriz.

P_0 çatallaşmadan önce REP değeri olsun ve P_1 çatallaşmadan sonra REP değeri olsun. M_0 çatallaşmadan önce para arzı olsun ve M_1 çatallaşmadan sonra para arzı olsun. S çatallaşma aşamasında doğru evrene taşınan M_0 oranı olsun. b, çatallaşmanın başlaması için ekonomik olarak yakılan (bir Yanlış sonucu yatırılmış) REP olsun; $b > 1$ olduğunu varsayıyoruz..

Bu bölüm çerçevesinde, çatallaşma aşamasında taşınan bütün REP'in saldırgan tarafından kontrol edildiğini ve çatallaşma aşamasında taşınan bütün REP'in doğru evrene (böylece saldırı masrafı asgariye indirilir) taşındığı basit varsayımında bulunacağız.

Bu bilgiden hareketle, SM_0 çatallaşma aşamasında taşınan REP, $(1 - S)M_0$ ise çatallaşma aşamasında taşınmayan REP olur.

$$M_0 = SM_0 + (1 - S)M_0 \quad (D1)$$

Çatallaşma aşamasında toplam SM_0 REP taşındığında, $0.05SM_0$ 'lık bir enflasyon oluşur.

$$M_1 = 1.05SM_0 + (1 - S)M_0 \quad (D2)$$

Enflasyonun etkileri üzerine odaklanıyoruz ve kolaylık için çatallaşmadan sonra piyasa değerinin çatallaşmadan önce piyasa değeriyle aynı olacağını varsayıyoruz²⁸:

$$P_0M_0 = P_1M_1 \quad (D3)$$

D1 ve D2 yerine D3 koyarak sadeleştirirsek;

$$P_1 = \frac{20P_0}{20 + S} \quad (D4)$$

Saldırganın çatallaşma oluşturmaktan ve erken taşıma primini kullanmaktan (brüt) kazancı, Taşımadan sonra REP'inin değeri - taşınmadan önce REP'inin değeridir.

$$1.05SM_0P_1 - SM_0P_0 \quad (D5)$$

D4'i D5'ün yerine koyarak saldırganın (brüt) kazancı için alternatif bir ifade elde ederiz.

$$1.05SM_0 \frac{20P_0}{20 + S} - SM_0P_0 \quad (D6)$$

²⁸Bunun makul olduğunu düşünüyoruz. Uygulamada Piyasa değerinin alçalmasını bekliyoruz.

b 'nin bir çatallaşmanın başlaması için ekonomik olarak yakılması gereken REP olduğunu hatırlayın, Böylece, bir çatallaşma başlatmanın masrafı bP_0 'olur. Bu nedenle, ne zaman aşağıdaki denklem gerçekleşirse o zaman erken taşıma priminden faydalanmak için çatallaşma masrafını ödemeye değer.

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

$P_0 > 0$, ve $S \neq -20$ olduğunu incelersek b bilinmeyenini çözebilir ve saldırının karlı olduğunu görürüz.

$$b < \frac{21M_0S}{S+20} - M_0S \quad (D8)$$

Ters teşviki önlemek için, Augur şartları aşağıdaki gibi düzenlemelidir:

$$b \geq \frac{21M_0S}{S+20} - M_0S \quad (D9)$$

S 'in $[0, 1]$ aralığına kısıtlandığına dikkat ederek $S = 2\sqrt{105} - 20 \approx 0.4939$ olduğunda D9 eşitsizliğinin sağ tarafının değerinin azami hale getirildiğini görürüz. Yani, bu saldırı var olan bütün REP'in 49.39%'u çatallaşma aşamasında taşındığı zaman en karlı halindedir. Sadelikten yana davranırsak, bu değeri S için kullanırız.²⁹

D9 'u $S = 0.4939$ yerine koyarak $b \geq 0.012197M_0$ 'u elde ederiz. Bu nedenle, bir çatallaşmayı başlatma masrafı var olan REP'in en az 1.2197% ise enflasyon sağma saldırısı karlı olmaz

Bir çatallaşmanın, en az bütün REP'in 2.5%'i boyutunda bir itiraz tahvilinin başarılı bir şekilde doldurulması ile başladığını hatırlayın. ω sonucu lehine böyle bir tahvilin doldurulduğunu ve çatallaşmanın başladığını varsayalım. ω sonucu ya doğrudur ya da yanlıştır.

Eğer ω sonucu yanlış ise, var olan bütün REP'in en az 2.5%'i yanlış bir sonuca yatırıldı ve bu nedenle ekonomik olarak yakıldı demektir. Bu nedenle ω yanlış olduğunda enflasyon sağmak karlı değildir.

Eğer ω sonucu doğru ise, Önsav 2 bize var olan REP'in(toplamda) en az 1.25%'i yanlış sonuçlara yatırıldı ve ekonomik olarak yakıldı demektir. Bu nedenle ω doğru olduğunda enflasyon sağmak karlı değildir.

Bu nedenle çatallaşma başlangıcı en az bütün REP'in 2.5%'i boyutunda bir itiraz tahvilinin başarılı bir şekilde doldurulmasını gerektirir.

Appendix E: Tahvil Büyüklüğü Ayarlamaları

Geçerlilik tahvili, görünmez REP tahvili ve atanmış muhabir hissesi bir önceki ödeme aralığı sırasında

katılımcıların davranışlarına göre dinamik olarak ayarlanır.

Burada, bu değerleri nasıl ayarladığımızı tarif ettik $f : [0, 1] \rightarrow [\frac{1}{2}, 2]$ by:³⁰

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

f fonksiyonu aşağıdaki altbölümelerde tanımlandığı gibi, bu ayarlamalarda kullanılan katsayıya karar vermek için kullanılır. Kısaca, eğer davranış bir önceki ücret aralığında tam olarak %1 kadar tekrarlandıysa tahvil boyutu aynı kalır. Eğer daha az sıklıkla tekrarlandıysa tahvil boyutu yarıya indirilir. Eğer daha fazla sıklıkla tekrarlandıysa tahvil boyutu iki katı kadar artırılır.

1. Geçerlilik Tahvili

Başlangıçtan sonra ilk ücret aralığı sırasında geçerlilik tahvili 0.01 ETH olarak belirlenir. Sonra, eğer bir önceki ücret aralığında sonuçlanmış piyasaların 1%'inden fazlası geçersiz ise geçerlilik tahvili artırılır. Eğer bir önceki ücret aralığında sonuçlanmış piyasaların 1%'inden azı geçersiz ise geçerlilik tahvili azaltılır (ama asla 0.01 ETH-den az olmaz.)

Özellikle, bir önceki ücret aralığında geçersiz olan sonuçlanmış piyasaların oranı ν bir önceki ücret aralığında geçerlilik tahvilinin miktarı b_ν olsun. Böylece yürürlükte olan aralıkta tahvil boyutu azami $\max\{\frac{1}{100}, b_\nu f(\nu)\}$ olur.

2. Görünmeyen REP Tahvili

Başlangıçtan sonra ilk ücret aralığı sırasında, görünmeyen REP tahvili 0.35 REP olarak belirlenir. Geçerlilik tahvilinde olduğu gibi görünmeyen REP tahvili, taban değeri 0.35 REP olan 1%'lik bir görünmeyen oran hedeflenerek azaltılır veya çoğaltılır.

Özellikle, ρ bir önceki ücret aralığında atanmış muhabirleri zamanında raporlayamamış olan piyasaların oranı olsun ve b_ρ bir önceki ücret aralığında görünmeyen tahvil miktarı olsun. Yürürlükte olan ücret aralığı için görünmeyen REP tahvilinin miktarı azami $\max\{0.35, b_\rho f(\rho)\}$ olur

3. Belirlenmiş uhabir Hissesi

Başlangıçtan sonra ilk ücret aralığı sırasında, atanmış muhabir hissesi 0.35 REP olarak belirlenir. Atanmış muhabir hissesi olarak kaç muhabirin bir önceki ücret

²⁹Pratikte, saldırgan çatallaşma aşamasında diğer katılımcıların kendi REPlerini taşımalarını engelleyemez ve bu nedenle S 'in ideal bulduğu 0.4939 değerini geçeceğini garantileyemez. Ancak, en kötü durum senaryosuna karşı savunma yaptığımız için $S = 0.4939$ 'u kullanıyoruz.

³⁰Bu formül canlı piyasadan deneysel veri elde edildiğinde değişebilir.

aralığında hatalı olduğuna(nihai sonuçla uyumlu olmadığına) göre dinamik olarak ayarlanır.

Özellikle, bir önceki ücret aşaması sırasında yanlış olan atanmış raporların oranı δ ve bir önceki ücret aralığı sırasında atanmış muhabir hissesi b_d olsun, sonra yürürlükte olan ücret aralığı için atanmış muhabir hissesi azami is $\max\{0.35, b_d f(\delta)\}$ olur.

Appendix F: Tasarım Değişiklikleri

Augur'un güncel tasarımına üç yıllık araştırma ve tekrarlamayla ulaştık. Bu süreçten ortaya çıkan tasarım, kağıt üzerindeki tasarımdan önemli ölçüde farklıdır [12]. Burada, önemli üç değişikliği ve mantığını anlatacağız.

1. Raporlama Ücretleri

Eski tasarımda, piyasa yaratıcısı muhabirlere yarı yarıya bölünecek bir ticaret ücreti belirliyordu. Güncel tasarımda piyasa oluşturucusunun ücreti ve muhabirlerin ücreti bağımsızdır ve muhabirlerin ücretleri sistemi güvenli tutmak Augur tarafından dinamik olarak ince ayarlanır.

Muhabirlere ödenen ücretler REP'in değerini etkiler, bu durumun çatallaşma protokolü üzerinde doğrudan etkisi vardır (Theorem 1). Eğer muhabirlere ödenen ücretler çok düşük ise kehanetin bütünlüğü riske girer. Eğer muhabirlere ödenen ücretler çok yüksek ise parazit piyasaların tehdidi artar. Bu nedenle, muhabirlere ödenen ücretlerin piyasa yaratıcılarının gelişigüzel ayarlaması yerine dinamik olarak ayarlanması Augur'un güvenliğinin sağlanması için önemlidir.

Muhabirlerin ücretlerinin piyasa yaratıcılarının kararlarına bağlanmasını koparmak, raporcuların(ve çatallaşma protokolünün bütünlüğünün) piyasa yaratıcıları arasında en düşük ücretli piyasaları yaratma rekabetinden zarar görmemelerini garantiye alır. Kaliteli piyasalar ve kaliteli raporlama ölçülmeli ve ayrı ayrı ödüllendirilmeli. Muhabirlere verilen ücretleri düşürmeden, piyasa yaratma ücretlerinin sıfıra çekilmesi için rekabete izin verilmeli.

2. Ticaret Ücretleri

Eski tasarımda ücretler tüccarlarda her ticarete alınırdı. Yeni tasarımda ücretler, tüccarlardan sadece piyasa sözleşmesi ile hesap kapatımında alınıyor. Bu değişiklik kısmen, Augur çevrimdışı ticareti takip edemeyeceği için yapıldı. Piyasa sonuçlarının hisseleri kullanıcılar arasında serbestçe takas edilebilecek tokenlerdir. Her takasta ücret almak imkânsız olduğu için Augur, tüccarlar doğrudan Augur'un piyasa sözleşmeleriyle hesap kapattıklarında ücret alır. Bu yaklaşımın bir faydası da tüccarlar tarafından ödenen ortalama ücreti azaltması ve bu nedenle Augur'u rekabetli yapmasıdır.

3. Evrenler

Eski tasarımda REP'in sadece bir "versiyon"u vardı ve toplam arzı sabitti. Yeni tasarımda REP her biri asıl versiyondan daha az veya çok ile sonuçlanan birçok versiyona (evrene) çatallaşabilir. Eğer bir çatallaşma çekişmeliyse çocuk evrenlerin her birinde REP arzı, ebeveyn evrendeki toplam arzın yalnızca bir kısmı olabilir. Çekişmesiz bir çatallaşmada katılımcılara verilen erken taşıma primi, çocuk evrenin ebeveyn evrenden daha fazla toplam REPe sahip olmasına neden olabilir

Çatallaşma ile oluşturulan REP'in yeni versiyonları, kendi arzlarına ve değerlerine sahip birbirlerinden farklı tokenlerdir ve hizmet sağlayıcılarımızın da buna göre davranması gerekir. Augur faaliyete geçtiğinde sadece bir evren(birincil başlangıç evreni) ve REP'in bir versiyonu olacak, tam olarak şu anda olduğu gibi. Ancak bir çatallaşma gerçekleştiğinde REP'in tek versiyonu birçok versiyona bölünecek: Örnek olarak, A ve B sonuçlu çatallaşan bir piyasa REP-A, REP-B ve REP-Geçersiz olarak yeni tokenler ortaya çıkaracak. REPi kullanan cüzdanlar ve ticaretlerin (teorik olarak) kullanabileceği dört farklı REP versiyonu - Rep-başlangıç (artık kilitlenmiş olması gereken asıl REP versiyonu), REP-A, REP-B ve REP-Geçersiz- olacak.³¹

Her çocuk evrende toplam REP arzı, o evrene ne kadar REP taşındığına ve ne zaman taşındığına bağlıdır. Bir Çatallaşma sırasında hangi evrende mutabakatın sağlandığı belli olmadan REP taşımak, kullanıcıyı küçük (ama sıfır olmayan) (detaylar için III E) bir riske maruz bırakır. Bu durum çekişmeli çatallarda katılımdan caydırabilir. Katılma teşvik için kullanıcıların bu riski telafi edilmelidir

Çatallaşma aşamasında dahil olmayan kullanıcılar REP tahvillerinin bir kısmı kaybedilerek cezalandırılabilirler. Hatta eski tasarımın katılımda bulunmayanları yanlış raporlamışlar gibi cezalandıran bir "kullan ya da kaybet" mekanizması vardı. Ancak, katılımda bulunmayan kullanıcıları cezalandırmak ciddi kullanılabilirlik sorunları yaratır. Katılımda bulunmayan kullanıcıları cezalandırmak müşterilerinin REPlerinin saklayıcıları olan cüzdanlar ve takaslar için sorunludur. Çatallaşma durumunda takasların, müşterilerinin REPlerini çatallaşma aşamasında bir çocuk evrene taşımaları veya REP hisselerinin bir kısmını kaybetmeleri gerekirdi.³²

Katılmayanları cezalandırmak yerine, çatallaşma aşamasında taşınan çatallaşma katılımcıları taşıdıkları

³¹Pratik anlamda, hizmet sağlayıcıları kullanıcılarını çatallaşmaya katılmaya teşvik etmeyi ve sonra çatallaşma çözümlendiğinde kazanan evreni desteklemeyi en kolay (ve en az aksatıcı) yol olarak bulabilirler.

³²Pratik anlamda, akıllı sözleşme kodunun sadece yeniden tahsis kullanarak çatallaşma ödülleri uygulamasının aşırı karmaşık olduğunu fark ettik. Sözleşme kodunun karmaşıklığı bir güvenlik riskidir, bu nedenle uygulamayı mümkün oldukça basitleştirdik.

çocuk evrende 5%lik bir prim basılarak ödüllendirilirler Eğer REP'in 4.762%'si (veya daha fazlası) kaybe-

den (1.25%-2.5% kadarı itiraz tahvili olarak adanmış) bir evrene taşınırsa bütün evrenlerin toplam REP arzı ebeveyn evrenin REP arzından daha az olacaktır.