BLOKZİNCİR TEKNOLOJİSİNDE UZLAŞMA MODELLERİ

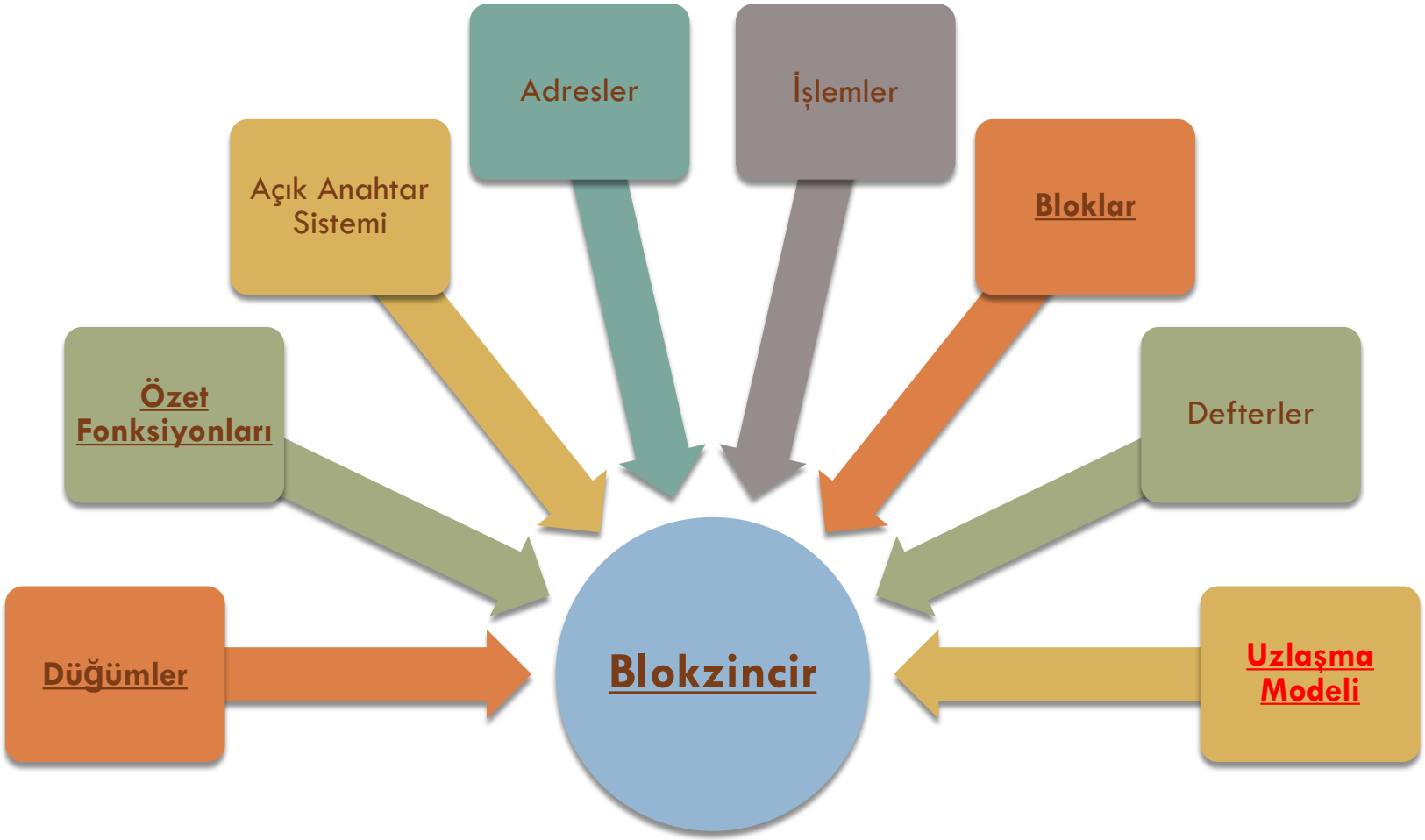
1. Ulusal Blokzincir Çalıştayı
2-3 Nisan, 2018 Ankara, Türkiye

Dr. Süleyman KARDAŞ
Bilgisayar Mühendisliği, Batman Üniversitesi

Ajanda

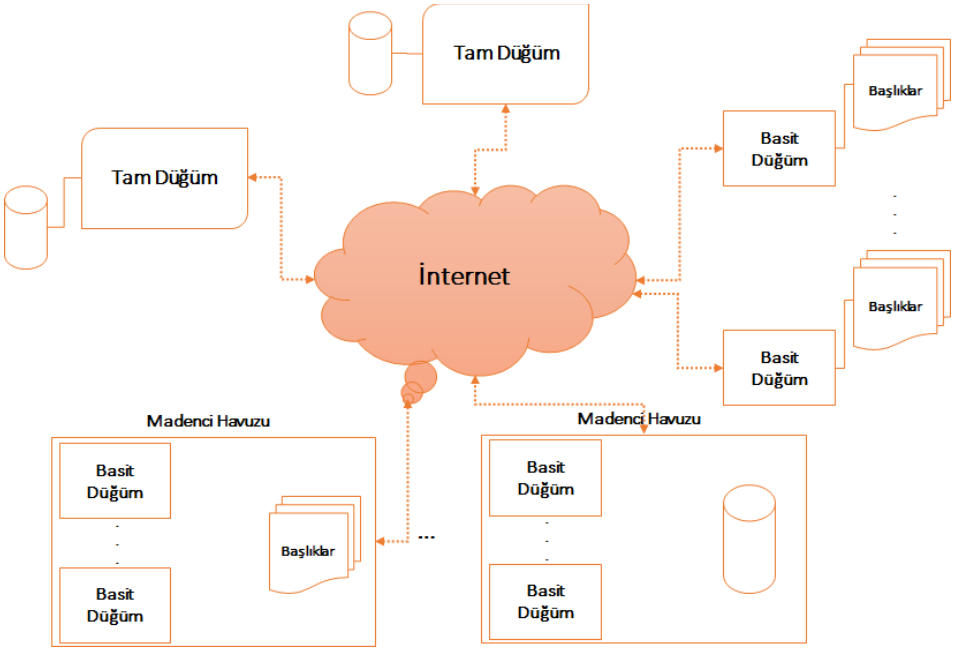
- Motivasyon
- Emek Kanıtı Uzlaşma Modeli
- Hisse Kanıtı Uzlaşma Modeli
  - Temsili Hisse Kanıtı
  - Kiralık Hisse Kanıtı
  - Önem Kanıtı
  - Casper Hisse Kanıtı
  - Ouroboros: Hisse Kanıtı
- Bizans Hata Toleransı Uzlaşma Modeli
  - Temsili Bizans Hata Toleransı
  - Pratik Bizans Hata Toleransı
  - Federe Bizans Anlaşması
- Sonuç

Blokzincir Teknolojisi Mimarisi



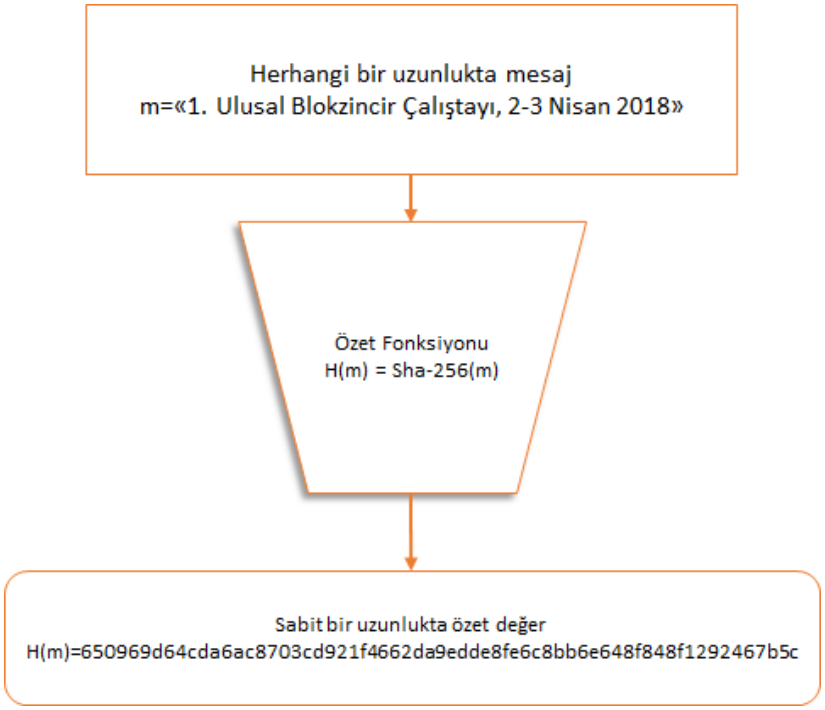
BLOKZİNCİR: Düğümler

- Bir blokzincir, veri akışını yöneten herhangi bir merkezi yetkiye sahip olmayan **düğümler** arası bir sistemdir.
  - Düğümler **aynı haklara** sahiptirler.
  - Bir düğüm **istemci** ve/veya **sunucu** olabilmektedir.
- Düğümler **yapılarına** göre farklılık gösterirler.
  - Tam düğüm
  - Basit düğüm
  - Madenci düğüm
  - Madenci havuzu

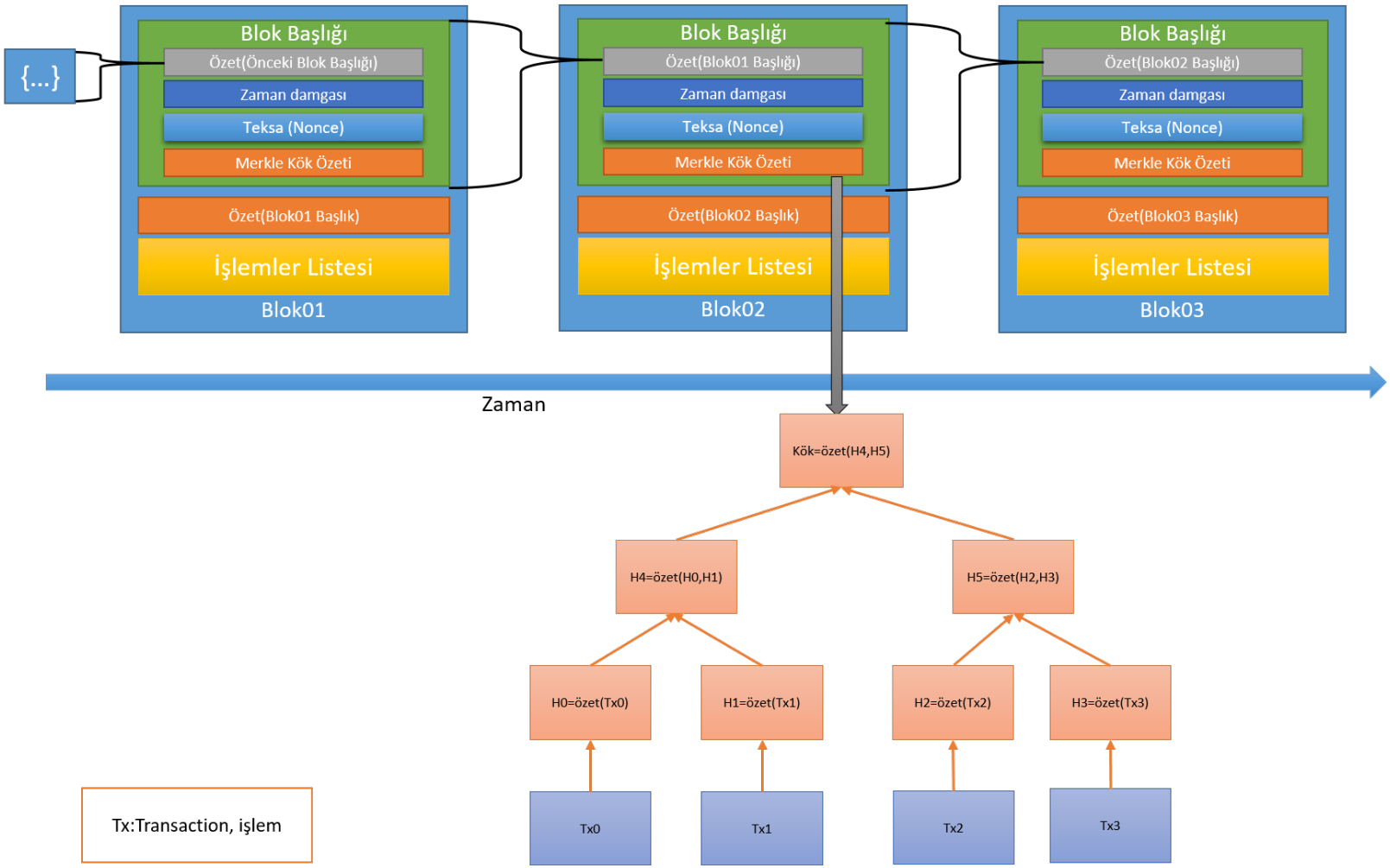


Kriptografik Özet Fonksiyonu

- Değişken uzunlukta bir mesajı sabit uzunlukta bir özet değerine dönüştüren fonksiyonlardır.
  - $h: \{0,1\}^* \rightarrow \{0,1\}^n$
- Bir açık metnin özet fonksiyon değeri o metnin parmak izi veya DNA'sı olarak tanımlanır.
- Temel özellikleri:
  - Hesaplama kolaylığı
  - Çakışma saldırısına karşı güvenli olmalı
    - Özet(m1)=Özet(m2) durumunu sağlayan iki mesajın bulunmasıdır
  - Ters görüntü Elde edilmesine karşı güvenli olmalı
    - Verilen bir özet değerine karşılık gelen açık metinin bulunmasıdır
- En çok kullanılan özet fonksiyonlar: SHA-256, Keccak-256, RIPEMD160, Scrypt, X11



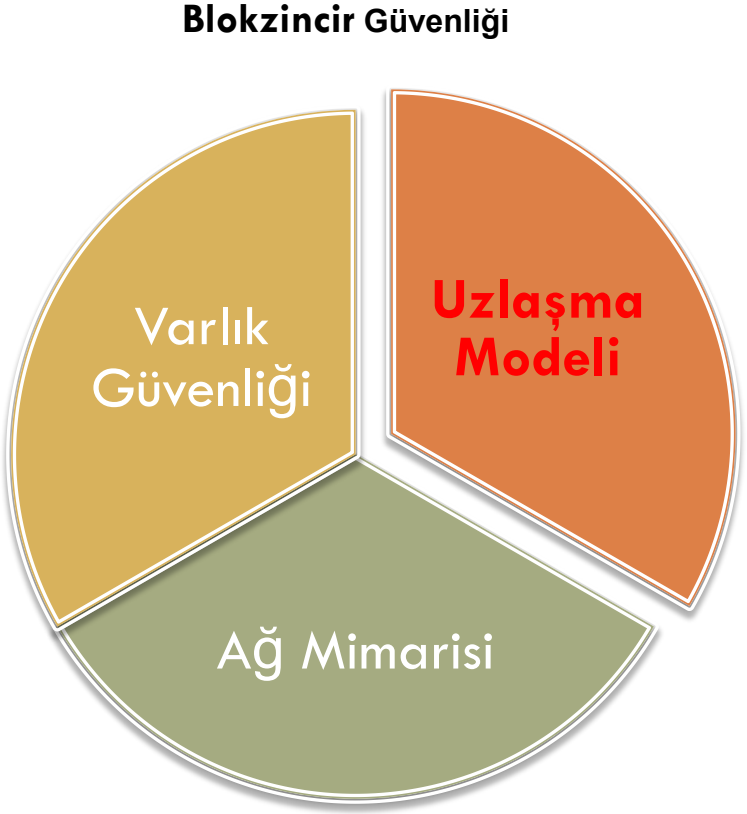
BLOKZİNCİR



Blokzincir Teknolojisinde Uzlaşma Modelleri

Neden Uzlaşma Modeli Gerekli

- İnsanlar, bir blokzincir ağına **neden** katılmak **isterler?**
- Bir düğüm, neden **başka** bir düğüm tarafından **çözülmüş** bir bloğu **yayınlamak** ister?
- Birden fazla madenci düğümü bir bloğu yaklaşık olarak **aynı anda** çözdüğünde **çatışmaları** kim yönetecektir?
- **Kötü** niyetli **düğümlere** karşı nasıl bir **yol** izlenecek?
- İyi niyetli düğümlerin işlemler esnasında **ağdan düşmesi** durumunda ağın durumu?



İyi Bir Mutabakat

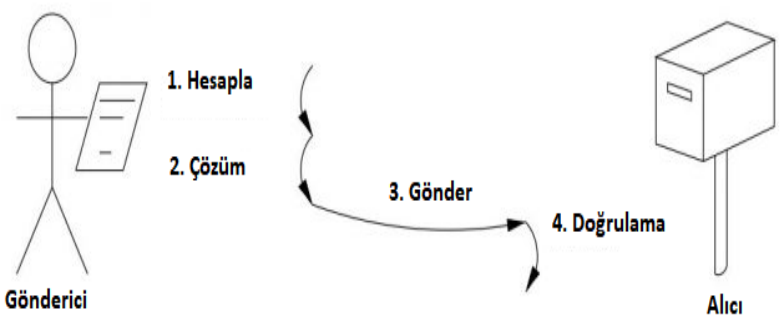
EMEK KANITI (Proof of Work)
UZLAŞMA MODELİ

Emek Kanıtı Uzlaşma Modeli

- Emek kanıtı (Proof of Work) hizmet saldırılarını ve diğer hizmet ihlallerini engellemek için ekonomik bir önlem olarak tanımlanmaktadır.
  - Bu model, Cynthia Dwork ve Moni Naor tarafından istenmeyen e-postalar ile mücadelede kullanıldı (Yıl: 1993)
  - Markus Jakobsson and Ari Juels tarafından 1999'daki makalelerinde bu yöntem formalize edildi.
- İki farklı emek kanıtı yöntemi bulunmaktadır.
  - Çözüm-Doğrulama, Sorgu-Cevap

Emek Kanıtı: Çözüm-Doğrulama Protokolü

- Bu protokolde gönderici ve alıcı arasında herhangi bir senkron iletişime gerek yoktur.
- Belirli bir kurallara göre hazırlanmış **bulmacalar** çözümüne kavuşturulur.
- **Bulmacalar** asimetrik özelliğe sahiptirler.
  - İstekte bulunan taraf için orta derecede zor ve hesaplanması mümkün.
  - Servis sağlayıcı tarafından doğrulanması kolay.
- Bulmacaların çözümü yüksek miktarda CPU/GPU işlemi gerektirmektedir.
- Bazı bulmacalar:
  - Kriptografik özet fonksiyon tabanlı
  - Büyük asal sayı modunda tamsayıların karekökü
  - Kismi özet fonksiyon tersinin bulunması



Çözüm-Doğrulama Protokolü

ZenCash ETHEREUM bitcoin ZCASH MONERO

Özet Fonksiyon Tabanlı Bulmaca

- SHA-256 özet fonksiyonu kullanılarak hazırlanır.
- **Örnek Bulmaca:**
  - SHA256 ("blokzincir" + Teksa) = "0000000" ile başlayan özet değeri
  - Yedi tane sıfır ile başlayan özet değeri.
  - Teksa: Tek Kullanımlık Sayı
- Bu çözüm için i7 işlemcili 12GB RAM'e sahip bir makinede Windows 10 İşletim Sisteminde Java BouncyCastle kütüphanesi kullanıldığında:
  - 33758449 deneme,
  - 25 sn.

Özet Algoritma ve Mesajın Başı	Teksa	Özet Değeri
SHA256("blokzincir"+0)	0	0x11dda4b2f8409049aedb06247f0423f45194bdad1c23308b69565e49a671ebab
SHA256("blokzincir"+1)	1	0xb2efee8229b6fabd4dad44351ec327c6a3295b19e47e1a239ec381919fcf90ea
. . .	. . .	. . .
SHA256("blokzincir"+teksa)	33758449	0x0000000 67d668d96d3415bcd2909fed7242cf75438596b38f675e8a926a5e30c

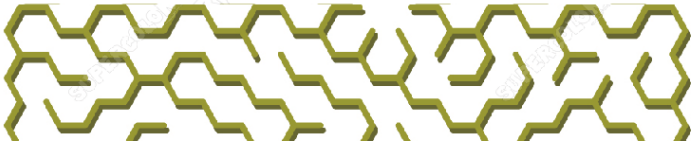
Özet Fonksiyon Tabanlı Bulmaca

- Bulmacaların zorluk derecesi sıfırların sayısının arttırılması ile gerçekleştirilir.
  - Daha fazla teksa kullanılması ile çözülür.
  - Daha fazla zaman gerektirir.
- Hedefi 8 sıfırla başlayan özeti bulma olarak değiştirildiğinde:
  - Çözümü aynı donanım ile 9.264.471.446 farklı teksa ile
  - 1 saat 53 dakika 13 saniyede çözüldü
  - Çözüm: SHA256("blokzincir9264471446") =0x**00000000**8252af91fb84d5c0cbb5103e169892c8b56334bfa4666bb6ff49b17e
- Şuan Bitcoin'deki zorluk derecesi: ikilik tabanda 73 tane sıfırla başlayan özet değeridir.

https://bitcoinwisdom.com/bitcoin/difficulty

Özet Fonksiyon Tabanlı Bulmaca

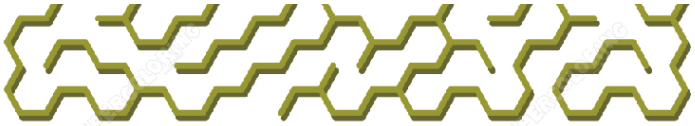
- Bu bulmacaların çözümünde kısa yol yoktur.
- Madenci düğümler, hedef değer için doğru olan değeri bulmak için yoğun bir hesaplama yapmak ve bunun için de zaman ve enerji kaynakları harcamak zorundadır.
- Zorluk derecesinin artması ile herhangi bir bilgisayar için bir bulmacayı çözmek imkansız hale gelmektedir.
  - Bu nedenle, madenci düğümleri kendilerini "**havuz**" ya da "**kolektif**" olarak örgütleyerek bulmacaları topluca çözmektedirler.
- Örnek: 40.000.000.000 tane farklı teksa denenerek 8 tane sıfır ile başlayan bir özet değeri hesaplansın.
  - 4 tane düğüm arasında eşit aralıklar ile paylaşılır.



Düğüm	Teksa: başlangıç	Teksa: son değer
1. Düğüm	0000000000	10000000000
2. Düğüm	10000000001	20000000000
3. Düğüm	20000000001	30000000000
4. Düğüm	30000000001	40000000000

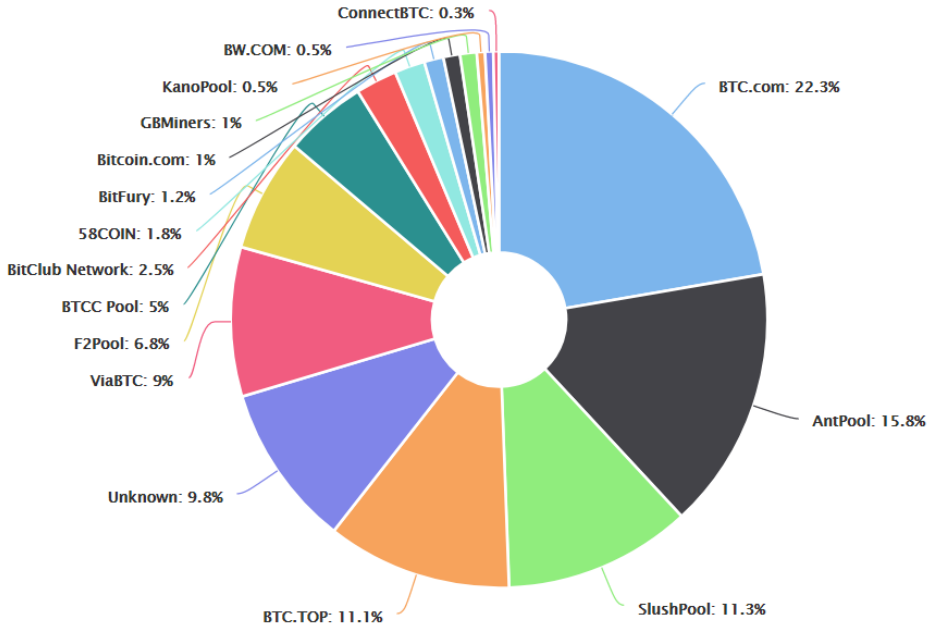
Çözüm: Toplamda 1.835.009.602 farklı teksa değeri denenmiştir ve 30458017781 teksa değerini kullanan 4. düğüm 8. dk 5 saniyede çözmüştür:

Cevap: SHA256("blokzincir30458017781")
=0x**00000000**d4fa2df066b145aeda4e7a975e0049cba2a18f683c51d83f60f74db9



Emek Kanıtı: Dezavantajları-I

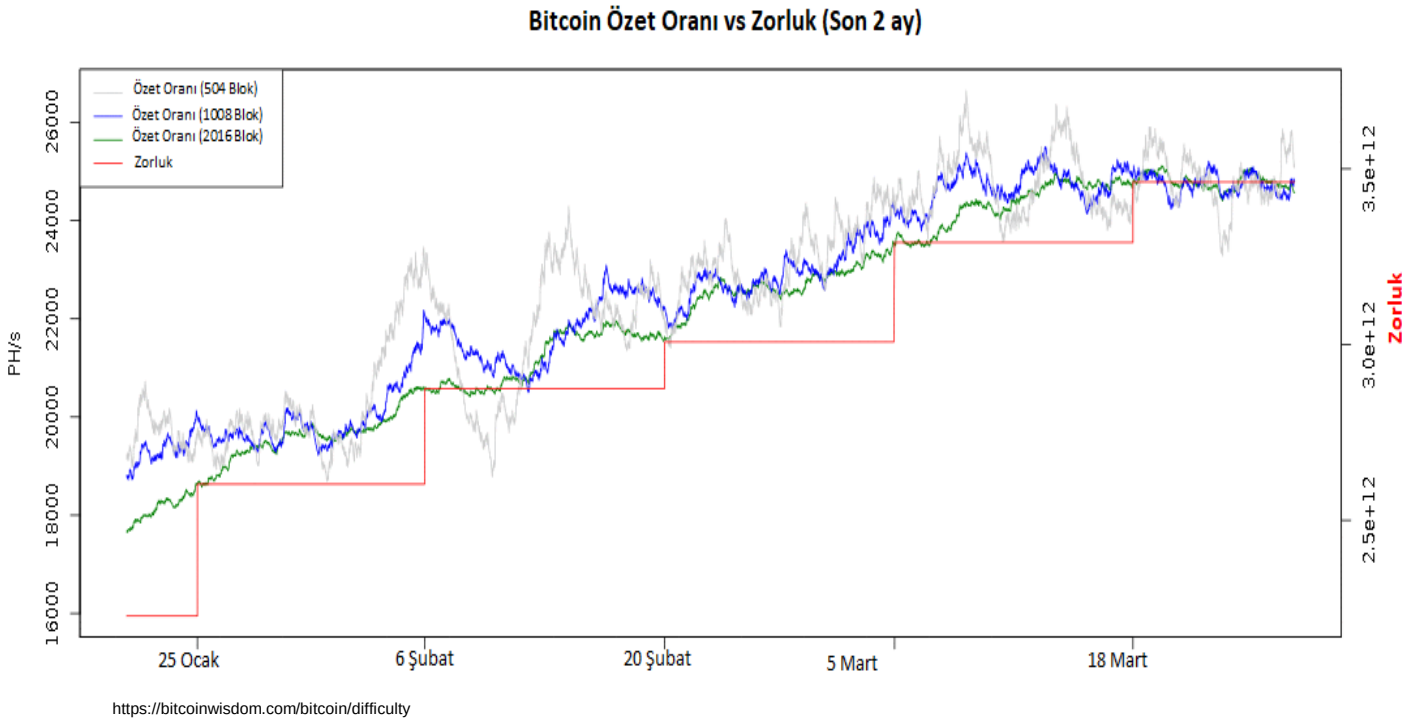
- Madenciliğin merkezileşmesi
  - İşlem gücünün **%50'den fazlasını 4 tane** madencilik havuzu yönetmektedir.
- ASIC ile madencilik yapılması, çok az şirket tarafından kontrol edilmesine sebebiyet vermektedir.



https://blockchain.info/tr/pools

Emek Kanıtı: Dezavantajları-II

- Zorluk derecesi arttıkça, blok üretimi için **çok fazla enerji** gerekmektedir.



https://bitcoinwisdom.com/bitcoin/difficulty

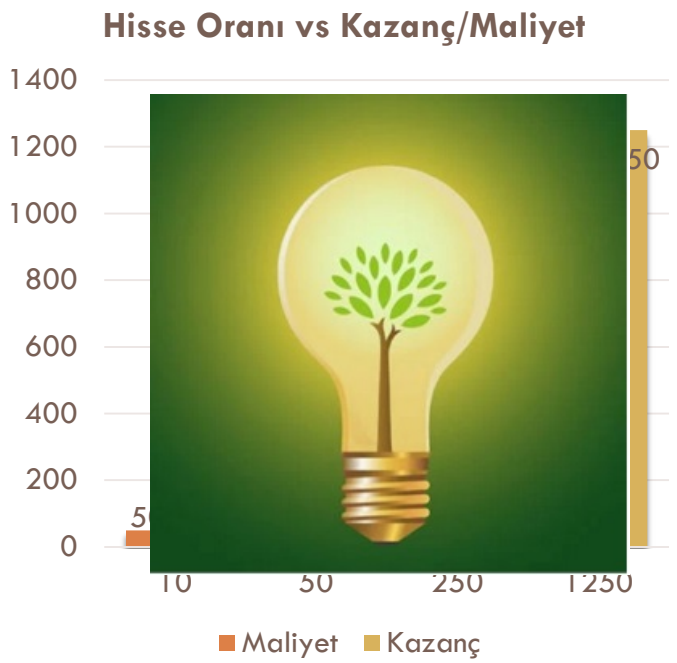
HİSSE KANITI (Proof of Stake)
UZLAŞMA MODELİ

Hisse İspatı Uzlaşma Modeli

- Hisse İspatı kavramı ilk defa Bitcoin için **paranın kıymetlenmesi/yaşı** olarak 2011 yılının başlarında ortaya atıldı.
  - **Hisse Sayısı x Zaman**
  - Gerçekleşecek işlemlerin önceliklerini belirlemek için kullanıldı.
- Sunny King ve Scott Nadal hisse ispatının blokzincirlerde güvenlik modeli olarak kullanılabileceğini gösterdiler (2012).
  - Bir blok oluşturma ve ödül alma olasılığı, kullanıcının sistemdeki payıyla orantılıdır.
  - Dolaşımdaki madeni paraların %x payına sahip bir hissedar, %x olasılığı ile yeni bir blok oluşturur.
  - Bloku oluşturacak düğüm, sahip olduğu hisse pay oranına göre rasgele olmayan bir yöntemle seçilir.

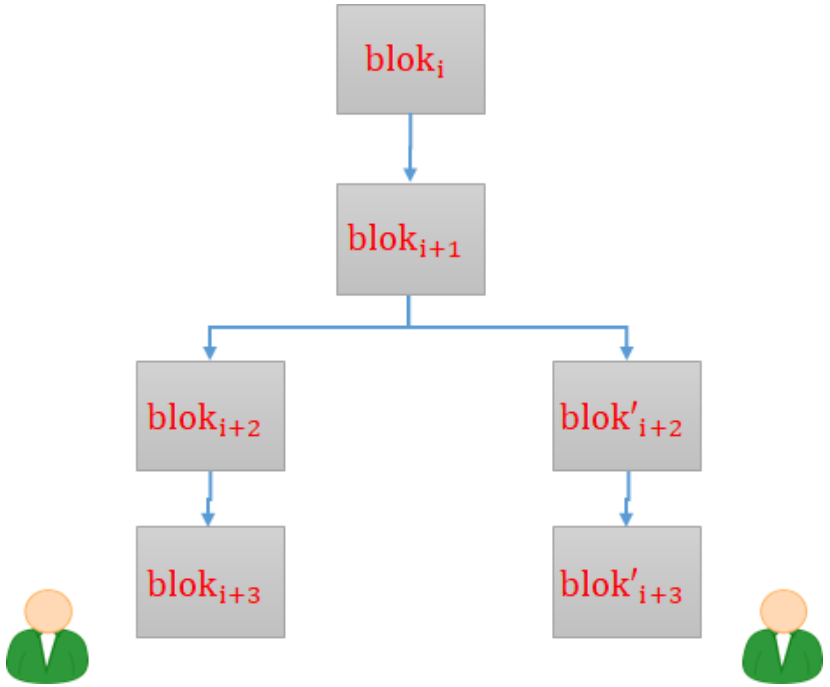
Hisse İspatı: Avantajları/Dezavantajları

- Avantajları
  - Az enerji kullanılmaktadır.
  - Saldırı için azaltılmış teşvikler bulunmaktadır.
  - Bloklar daha hızlı üretilmektedir.
- Dezavantajları
  - Zenginler daha fazla zenginleşmektedir.
  - Merkezileşme riski azaltıldı!?
  - Sıfır hisse problemi (Nothing at Stake)



Sıfır Hisse Problemi

- Düğümlerin yaptıkları işlemler çok az işlem/enerji gerektirmektedir.
- Bazı düğümlerin aynı anda iki farklı bloku oluşturması ve imzalaması problemidir.
  - **Çatallaşma** oluşabilir.
  - Çatallaşmalarda **çift harcama** problemi gerçekleşme olasılığı çok büyüktür.
- Çözüm:
  - Böyle davrananları cezalandırmak.

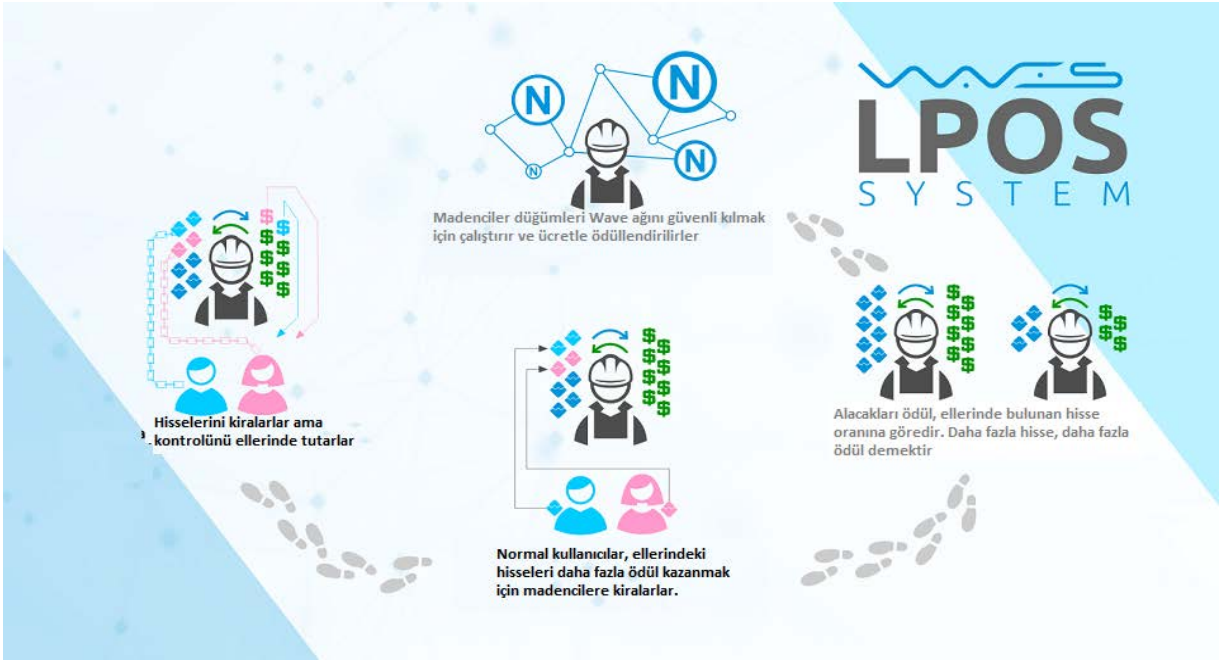


Temsili Hisse Kanıtı Uzlaşma Modeli

- Daniel Larimer 2014 yılında geliştirilen bu modelde **oylama** ile **temsilciler meclisi** seçilmektedir.
  - Herkes sahip olduğu **hisse oranı** kadar **oy** kullanırlar.
- Temsilciler, blokları oluşturmak ve işlemleri onaylamaktan sorumludurlar.
  - Bu işlemlerden ötürü **ödüllendirilmektedir.**
- Temsilciler, **blokların** içerisinde yer alan işlemleri **değiştiremezler**.
- Temsilciler, bloklara uygun olmayan **kötücül işlemlerin** eklenmesini **engellerler.**
- İtibarını kaybeden tanıkları **oylama** ile **değiştirilirler**.
- BitShares, Steem, EOS, List ve Ark.

Kiralık Hisse Kanıtı Uzlaşma Modeli

- WAVES tarafından geliştirilen bu modelde hisseler kiralanmaktadır (2016).
  - Cüzdanında **en az 10.000 WAVE** bulunduran herkes madenci düğüm olabilmektedir.
  - Az hisseye sahip kişiler **kontrolü kendilerinde** olmak üzere hisselerini herhangi bir **madenci düğüme kiralarlar**.
  - Kiralayan düğümler hisse ağırlıklarını **arttırırlar** ve böylece blok **oluşturma olasılıklarını** arttırırlar.
  - Blok oluşturmada elde edilen **ödül** kiralanan **hisse oranında** paylaşılır.



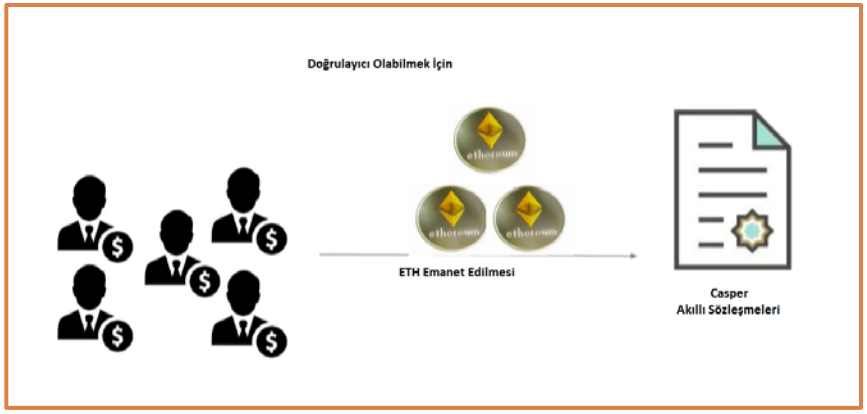
Önemin Kanıtı Uzlaşma Modeli

- NEM tarafından geliştirilen bu modelde her bir hesap için bir **güven derecelendirme notu** verilmektedir.
- **Önemli** olarak kabul edilen kullanıcılar **blok oluşturabilir** ve karşılığında **ödül** almaktadırlar.
  - Sadece bloktaki işlem ücretleri dağıtılır.
- Bir NEM kullanıcısının **önemi**, sahip oldukları **paraların sayısı** ve cüzdanlarından **yapılan işlem sayısı** ile ölçülmektedir.
  - Önem hesabı için en az 10.000 XEM gerekir.
  - **Gönderdiği** hesaptan tekrar para **alanların** önem skoru azaltılır.
  - Her 24 saatte bir eldeki **hissenin %10'u** önem skoruna eklenir.
  - Önem hesabından bir düğüm son 30 günde **en az 1000 XEM** göndermiş olmalı.

(Proof of Importance)

Casper Hisse Kanıtı

- 2017'de **Ethereum** için geliştirilen ve yakın zamanda uygulamaya geçecektir.
  - Bu model, **hisse** kanıtı ile **Bizans hata toleransı** modelinin birleştirilmesinden oluşur.
  - **Emek** ispatı ile **beraber** yürütülecektir.
  - Zamanla emek ispatının etkisi kaldırılacak ve sadece bu model geçerli olacaktır.
- Blokların oluşturulması ve onaylanmasını **doğrulayıcılar** tarafından gerçeklenir.
  - Bir miktar ETH **depozit** olarak Casper akıllı sözleşmelerine yatırmak gerekiyor.
  - Depozitle, **kötü** doğrulayıcılar **cezalandırılır**. Bununla Sıfır Hisse Problemi çözülmüş olur.
  - İki fazda oylama ile bloklar hazırlanır ve yayınlanır. Her iki fazda da **en az 2/3** oranında onay gerekir.



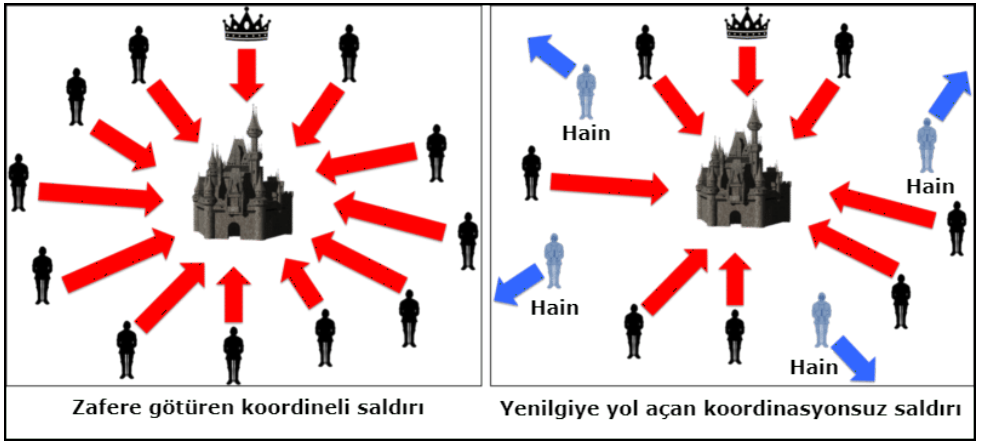
Ouroboros: Hisse Kanıtı

- Cardano Foundation tarafından geliştirilen bu modelde, zaman, çağlara ve çağlarda 20snlik zaman aralıklarına bölünür.
  - Bir çağda **N** tane zaman aralığı bulunur.
- Her zaman aralığı için **belirli bir orandan fazla** hisseye sahip düğümlerden bir lider seçilir.
  - Diğer düğümlerden gelen işlemleri alır. İşlemleri blok haline getirip imzalar ve ağa dağıtır.
  - Lider, kendi zaman aralığında çevrimdışı olursa hedeflenen blok boş kalacaktır.
  - Bir çağda bulunan blokların en az %50 + 1'i oluşması gerekir.
- Lider seçiminin **tarafsız ve bağımsız** olması için seçmenler arasında **Güvenli Çoklu Hesaplama protokolleri** (SMC) koşturulur.
  - Her seçmenden rasgele «madeni para atma»'ları istenmektedir ve sonuçlarını SMC ile kendi aralarında paylaşırlar ve en sonunda ortak bir değere ulaşılır.
    - Kamu Tarafından Doğrulanabilir Giz Paylaşımı (Publicly Verifiable Secret Sharing)
  - Bu final değeri ile FTS (Follow Satoshi Algorithm) algoritmasına yedirilerek zaman aralıklarındaki liderler seçilir.

BİZANS HATA TOLERANSI
(Byzantine Fault Tolerance)
UZLAŞMA MODELİ

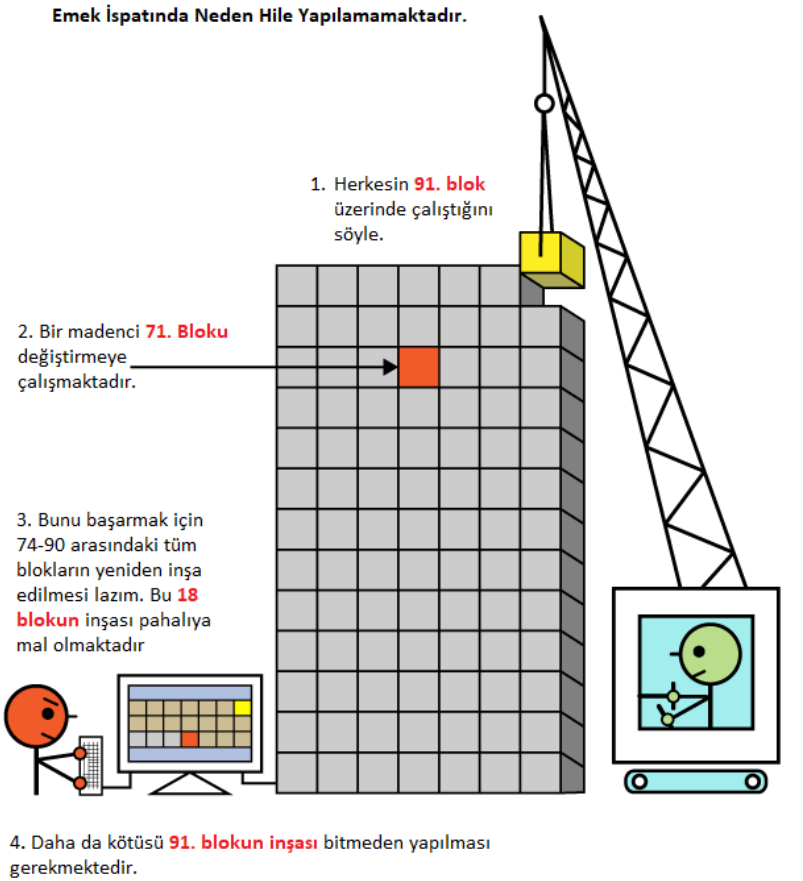
Bizans Hata Toleransı (BHT) Uzlaşma Modeli

- Bu model, Bizans savaş stratejisini anlatan Bizans federalleri hikâyesinin çözüm temeline dayanmaktadır.
  - Birkaç **bölük düşman kentin dışında** ve kendi generalin komutasındadır. Generaller, yalnızca **ulakları** vasıtasıyla haberleşirler.
  - Generallerin bazıları **sadık**, bazıları **haindir**. **Sadıklar** kurallara **uyarken**, **hainler** kurallara uymadıkları gibi, uyanları da **yanıltabilirler**.
  - Şehre ne zaman girileceği **orduların güçlü bir birlikteliği** olması gerekmektedir.
- Bu modelde **hainler** ne yaparsa yapsınlar **sadıkların kötü bir plan** hazırlamasına izin vermemesi gerekir.



BHT Uzlaşma Modeli: Çözüm I

- Emek kanıtı uzlaşma etkili bir şekilde BHT'yi sağlar.
  - Yeterince **büyük katılımcıya** sahip olan bir Blokzincirde kullanıcılar **hile** yapamamaktadırlar.
  - Yüksek **enerji** gerektirdiğinden, her zaman tercih **edilememektedir**.



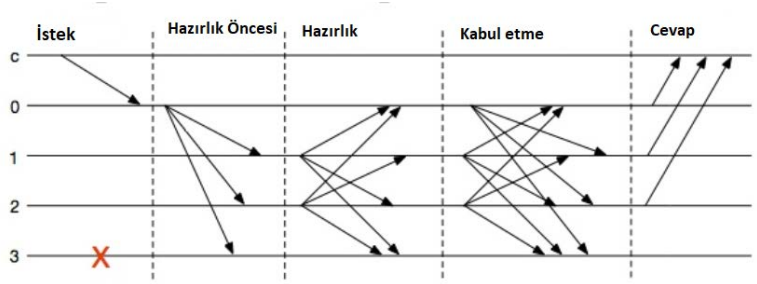
https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb

BHT Uzlaşma Modeli: Çözüm II

- Sınırlı bir grup **düğüm** arasında **uzlaşmaya** varılarak çözülür.
  - Her düğüm bir durum tablosu tutar.
  - Her düğüm blokların hazırlanmasında ve/veya yayınlanmasında oy kullanırlar.
  - **Düğüm oylarına** ve **çoğunluğun uzlaşması** beklenir.
  - Tam/temsili **demokratik** bir çözümdür.

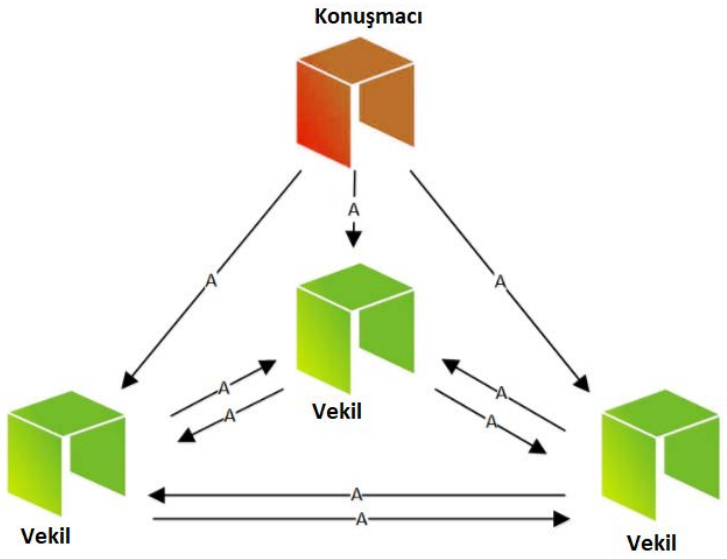
Pratik BHT Uzlaşma Modeli

- Hyperledger, BHT'yi pratikte uygulayan platformlardan biridir.
- Bu modelde:
  - **Önceden belirlenmiş n=3f+1** tane düğüm ile uzlaşma yapılmaktadır.
  - Bu uzlaşmadan **f** tane **düğüme tolerans** gösterilmektedir.
  - Her makine kendisine gelen bir işlem bilgisini kontrol eder, onayladığı bir işlemi imzalayarak ağ ile paylaşır.
  - Doğrulama yapanların sayısının en az **2/3'ünde** de aynı özet değeri görüldüğünde mutabakat sağlanmış kabul edilir ve oluşturulan blok muhasebe defterine kopyalanır.
- Düğüm sayısı düğümler arası mesajlaşma sayısını üstel olarak etkilemektedir



Temsili BHT Uzlaşma Modeli

- Castro ve Liskov tarafından önerilen PBHT uzlaşma modelinin **temsili** bir **demokrasi** ile geliştirilmiş halidir.
- NEO tarafından kullanılan bu modelde iki türlü düğüm bulunmaktadır:
  - Defter tutucular, tüm ağ için muhasebe hizmeti sağlar ve muhasebeyi sürdürür.
  - **Sıradan düğümler** ise transferleri sağlar, para değişimi yapabilirler ve gelen verileri kabul ederler.
- NEO hissesine sahip olanlar kimlerin defter tutucu olacağı oylama ile belirlenir.
  - $f = \left\lfloor \frac{n-1}{3} \right\rfloor$ tane delegenin ele geçirilmesine tolerans gösterilir.

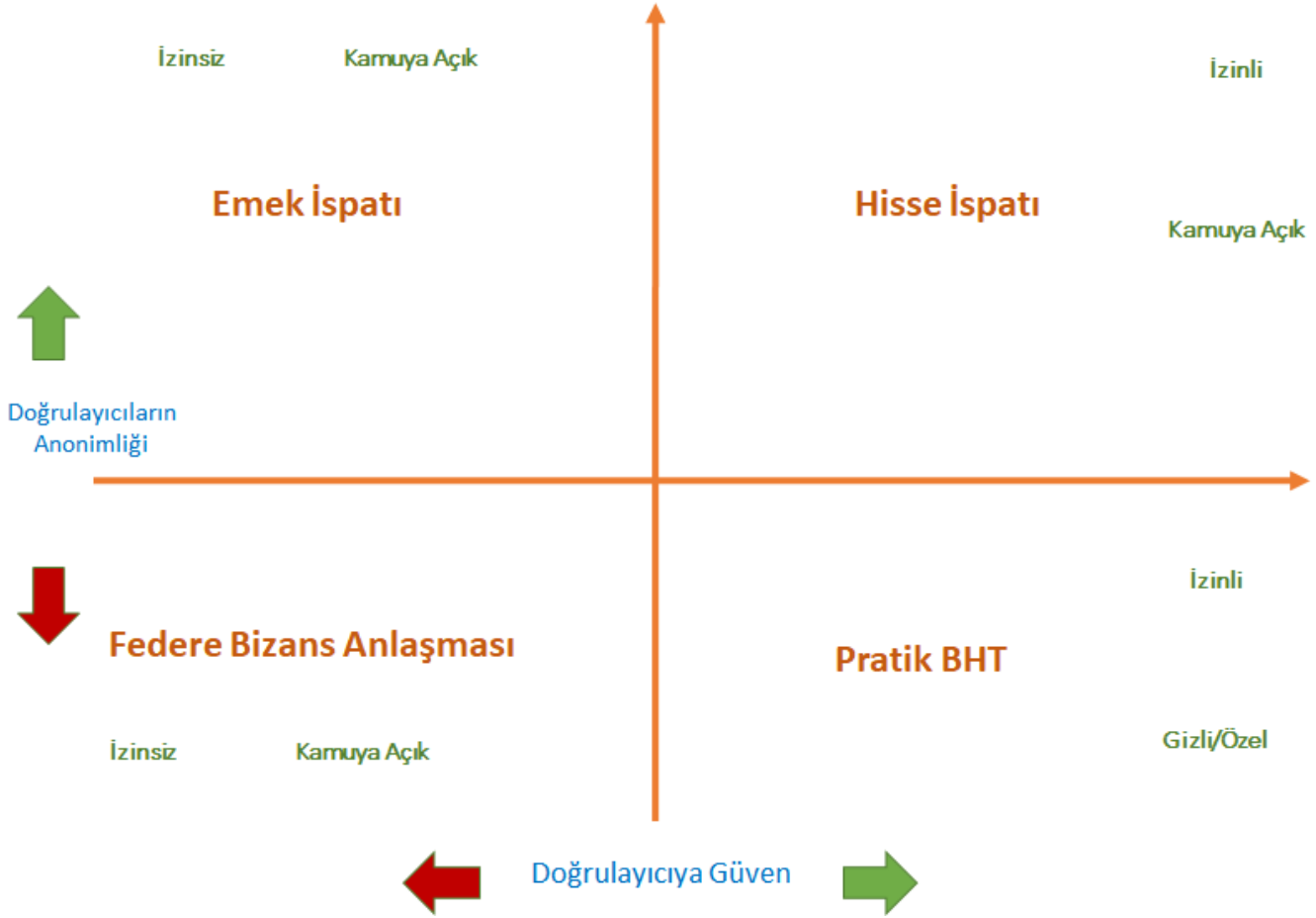


Federe BHT Uzlaşma Modeli

- İlk defa **Ripple** tarafından ortaya konan bu modelin çalıştığını Stellar'da formalize edilerek resmileştirildi.
  - Her düğüm belirli bir sayıdaki düğümlere **güven** duyar.
  - Uzlaşma **lokal** gruplar arasında gerçekleşir.
  - Birden fazla yapılan uzlaşma ve gruplar arasında kesişmenin olması durumunda genel uzlaşma sağlanmış olur.
- Ripple'de katılımcılar **önceden** belirlenmişken Stellar'da ağa **herkes** katılabilir.
- Ripple **merkezi** bir Blokzincirdir.
- Stellar **dağıtık** bir sistemdir. Kimlerin doğrulayıcı olacağını hangi doğrulayıcılara güvenileceğini düğümler seçer.

https://distributedlab.com/blog/how-to-classify-kinds-of-consensus

Sonuç


İzinsiz
Kamuya Açık
İzinli
Emek İspatı
Hisse İspatı
Kamuya Açık
Doğrulayıcıların
Anonimliği
İzinli
Federe Bizans Anlaşması
Pratik BHT
İzinsiz
Kamuya Açık
Gizli/Özel
Doğrulayıcıya Güven

Uzlaşma Protokollerinin Karşılaştırılması

	Emek İspatı	Hisse İspatı	PBHT	TBHT	Federe BHT
Blokzincir Türü	İzinsiz	İzinli/İzinsiz	İzinli	İzinli/İzinsiz	İzinsiz
İşlem Kesinliği	İhtimale Bağlı	İhtimale Bağlı	Kesin	Kesin	Kesin
İşlem Hızı	Yavaş	Hızlı	Hızlı	Hızlı	Hızlı
Katılma Maliyeti	Var	Var	Yok	Yok	Yok
Düğüm ağının büyümesi	Yüksek	Yüksek	Düşük	Yüksek	Yüksek
Güven Modeli	Güvensiz	Güvensiz	Yarı-Güven	Yarı-Güven	Yarı Güven
Saldırgan Toleransı	<= %25	Kullanılan Algoritmaya Bağlı	<= %33	<= %33	<= %33

SORULAR