TÜRK

WHITEPAPER

PRIZM

Dijital para biriminin ilk kavramı

Prizm Whitepaper Revizyonu Haziran, 2020

PZM.SPACE

GIRIŞ

Bitcoin, bilgi iletmek için P2P ağını kullanarak kripto paraları kolayca depolamanıza ve aktarmanıza, çift harcamayı önlemek için bir senkronizasyon sinyali olarak karma oluşturmanıza ve madeni paraların sahibini belirlemek için güçlü bir komut dosyası sistemi oluşturmanıza olanak tanıyan dünyanın ilk merkezi olmayan dijital para birimidir. Bu, büyüyen bir teknoloji ve iş altyapısını gösterir. Orijinal tasarıma göre, bitcoinler birbirinin yerine kullanılabilir ve tarafsız bir değişim aracı olarak görülür. Bitcoinler, İhraççı veya bir kamu anlaşması tarafından desteklenen özel özelliklere sahip olabilir ve temel alınan nominal değerden bağımsız bir değere sahip olabilir. Bitcoin, P2P elektronik ödeme sisteminin herhangi bir üçüncü tarafın katılımı olmadan gerçekten çalışıp ödeme yapabileceğini kanıtladı.

Bununla birlikte, tüm e-ekonominin tamamen merkezi olmayan bir eşler arası çözüme dayanması için sistemin aşağıdakileri yapabilmesi gerekir:

1 - İşlemleri güvenli, hızlı ve verimli bir şekilde, saatte binlerce veya daha fazla miktarda işleyin.
2 - İnsanları ağ güvenliğine katılmaya teşvik edin.
3 - Minimum kaynak tüketimi ile küresel düzeyde ölçeklendirin.
4 - Ve mobil de dahil olmak üzere çok çeşitli cihazlarda çalışabilmek.

PZM ("Prizm" olarak telaffuz edilir) tüm bu koşulları karşılar. Diğer bir avantaj, benzersiz olan, diğer mevcut kripto para birimlerinde sunulmayan PARAMİNİNG'dir.

Ama daha sonra daha fazlası.

PRIZM

GÖZDEN GEÇIRMEK

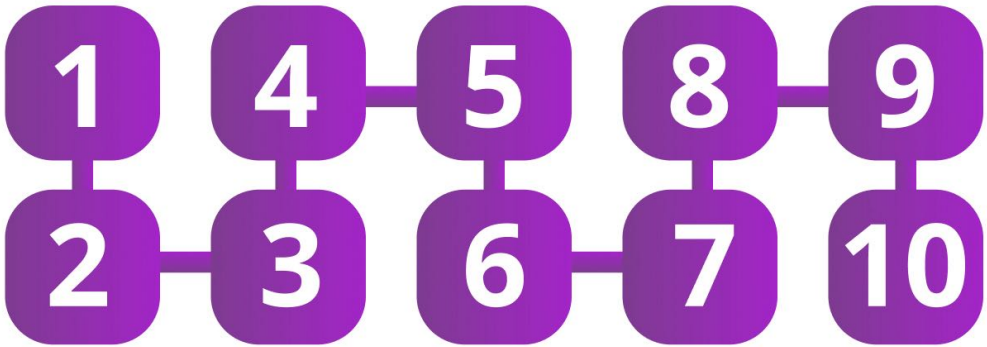
PRIZM, Java temelli açık kaynak kodlu **NEXT-Kernel** tabanlı% 100 kanıtlanmış bir kripto para birimidir. Benzersiz PRIZM proof-of-stake algoritması, diğer proof-of-stake kripto para birimleri tarafından kullanılan "madeni para yaşı" konseptinin herhangi bir uygulamasına bağlı değildir ve sözde "tehlikede olmayan" saldırılara karşı dirençlidir. Mevcut olan toplam sikke sayısı Genesis bloğunda dağıtıldı. Curve25519 kripto grafisi, daha yaygın olarak kullanılan SHA256 hash algoritmalarıyla birlikte bir güvenlik dengesi ve gerekli işlem gücü sağlamak için kullanılır.

PRIZM

GÖZDEN GEÇIRMEK

60 saniye

Ağ düğümlerinde engellenmeyen hesaplar tarafından ortalama olarak her 60 saniyede bir blok oluşturulur.

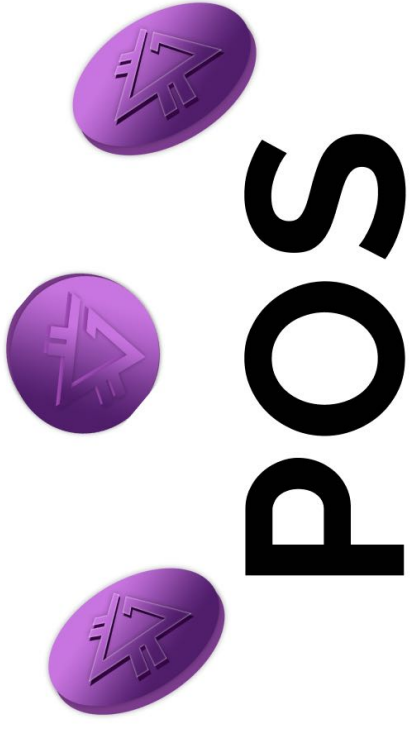


PZM, başarılı bir şekilde blok oluşturduğunda bir hesaba verilen işlem ücretlerini birleştirerek yeniden dağıtılır. Bu işlem dövme olarak bilinir ve diğer kripto para birimleri tarafından kullanılan "madencilik" kavramına benzer. İşlemler, 10 blok onayından sonra güvenli kabul edilir ve PZM'nin mevcut mimarisi ve blok boyutu, günde **367.200** işlemin işlenmesine izin verir.

PZM, ağın ek güvenlik mekanizmaları ile birlikte, üretim algoritması deterministik blok kullanarak işlem işleme performansını iki büyüklük sırasına kadar artırmanıza olanak tanıyan **Şeffaf Dövme** uygulamasını içerir.

Proof of Stake

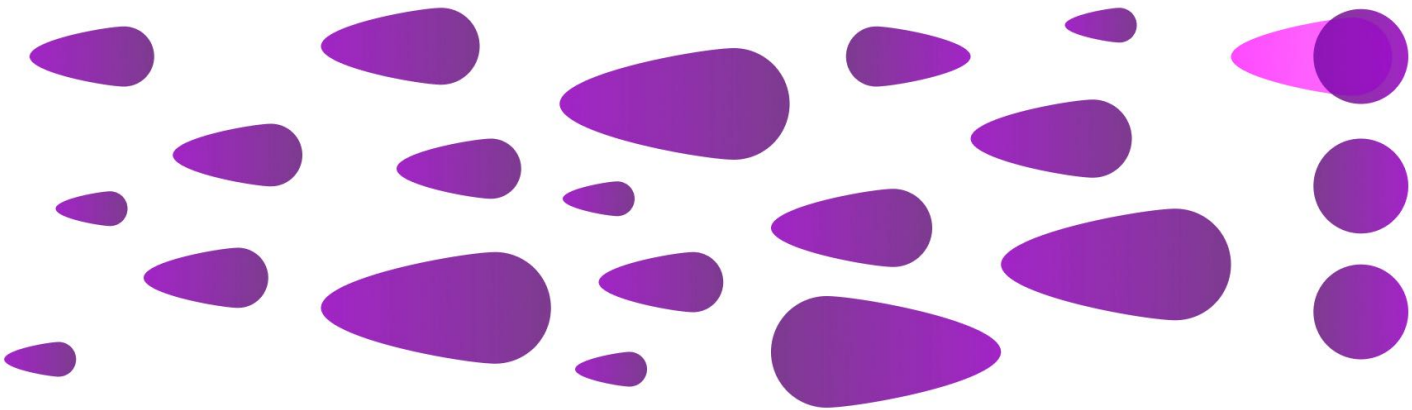
Kripto para birimlerinin çoğunluğu tarafından kullanılan geleneksel "Proof of Work" modelinde, ağ güvenliği "iş" yapan katılımcılar tarafından sağlanmaktadır. Kaynaklarını (hesaplama / işlem süresi) iki kat maliyetle işlemleri uzlaştırmak ve işlemleri daraltmaya çalışanlara olağanüstü maliyetler yüklemek için kullanırlar. Bu çalışma için katılımcılara PZM verilir ve bunların sıklığı ve miktarı kripto para biriminin çalışma parametrelerine göre değişir. Bu süreç madencilik olarak bilinir. Kripto para madenciliği için mevcut her bir ödülü belirleyen blok oluşturma sıklığı, kural olarak sabit kalmalıdır.



Sonuç olarak, ağ daha verimli hale geldikçe ödül elde etmek için gereken işin emek yoğunluğu artmalıdır. Proof of Work ağı geliştikçe, potansiyel ödülleri daha fazla meslektaş arasında dağıtıldığı için, bireysel kullanıcı ağı desteklemek için daha az teşvik eder. Kârlılık arayışında madenciler, önemli yatırım ve yüksek cari enerji maliyetleri gerektiren özel, patentli ekipman biçiminde kaynaklara yatırım yapmaya devam ediyor. Zamanla, daha küçük ortaklar (daha az iş yapabilenler) kaynaklarını bıraktıkça veya havuzlarda bir araya getirdikçe ağ daha merkezi hale gelir. Bitcoin Satoshi Nakamoto'nun yaratıcısı, bitcoin ağının tamamen merkezden uzaklaştırılmasını amaçladı. Ancak **Proof of Work** sistemleri tarafından sağlanan teşviklerin madencilik sürecinin merkezileşmesine yol açacağını kimse tahmin edemezdi. Bu, potansiyel güvenlik açıklarına yol açar.

PRIZM PROOF OF STAKE

ÇEKIRDEK TEKNOLOJILER



GHash. Bitcoin IO havuzu, geçmişte Bitcoin madencilik gücünün% 51'ine ulaştı ve ilk beş bitcoin madenciliği havuzu, ağın karma gücünün% 70'ini oluşturuyor. Ademi merkeziyet kavramı tamamen kayıp riski altındadır. Prizm tarafından kullanılan Proof of Stake modelinde ağ güvenliği, ağda payı olan ortaklar tarafından düzenlenir.

Bu algoritma tarafından sağlanan teşvikler, Proof of Work algoritmaları olarak merkezileştirmeye elverişli değildir ve veriler, Prizm ağının başlangıcından bu yana son derece merkeziyetsiz kaldığını göstermektedir: ağa bloklara katkıda bulunan çok sayıda (ve artan) benzersiz hesap ve en çok beş hesaplar toplam blok sayısının% 35'ini oluşturur.

PRIZM

PRIZM'DE POS

Prizm, hesaptaki her "madeni paranın" minyatür bir madencilik çiftliği olarak kabul edilebileceği bir sistem kullanır. Hesapta ne kadar çok jeton bulunursa, hesabın bir blok oluşturma hakkı elde etme olasılığı o kadar artar. Blok oluşturma sonucunda alınan toplam "ödül", blok içinde yer alan işlemlerin komisyon miktarıdır. PRIZM, blok oluşturmanın bir sonucu olarak herhangi bir yeni coin yaratmaz. PRIZM, yapı taşlarının bir sonucu olarak herhangi bir yeni para yaratmaz. PZM yeniden dağıtımı, işlem ücretlerini alan blok üreticilerinin bir sonucu olarak meydana gelir, bu nedenle bu bağlamda "madencilik" yerine "dövme" terimi kullanılır ve "ilişkiler veya yeni koşullar yaratmak" anlamına gelir. Doğrulanabilir, benzersiz, ve önceki bloktan neredeyse tahmin edilemeyen bilgiler. Bloklar, bu bağlantılar sayesinde birbirine bağlanır ve Genesis bloğuna kadar izlenebilen bir blok zinciri (ve işlem) oluşturur. Blok oluşturma süresi yaklaşık 59 saniyedir, ancak olasılıklardaki değişiklikler, bloğun ortalama oluşturma süresinin 80 saniye olabilmesine, blok aralıklarının daha uzun olmasına yol açmıştır. Blockchain'in güvenliği her zaman Proof-of-Stake sisteminde belirlenir.

Prizm «Proof of Stake» algoritmasına uygulanan temel ilkeler:

- Kümülatif karmaşıklık değeri, her blokta bir parametre olarak saklanır ve sonraki her blok, yeni "karmaşıklığını" önceki bloğun değerinden alır. Belirsizlik durumunda, ağ en yüksek kümülatif karmaşıklığa sahip bir blok veya zincir parçası seçerek fikir birliğine varır.

- Hesap sahiplerinin blok oluşturabilmek için bir manipülasyon aracı olarak fonlarını bir hesaptan diğerine taşımamaları için, paraların blok oluşturma sürecine katkıda bulunabilmeleri için 1.440 blokluk hesapta sabit olması gerekir. Bu kriteri karşılayan madeni paralar, verimli bir hesap bakiyesine katkıda bulunur ve bu bakiye, sahte olma olasılığını belirlemek için kullanılır.

- Bir saldırganın Genesis bloğundan sonuna kadar yeni bir zincir oluşturmasını önlemek için, ağ yalnızca mevcut bloğun arkasında bulunan 720 blokluk zincirin yeniden yapılandırılmasına izin verir. Bu eşiğin altındaki tüm bloklar reddedilecektir. Bu hareket eşiği tek sabit PZM kontrol noktası olarak kabul edilebilir.

- Herhangi bir hesabın kendi blok zincirini oluşturarak Blockchain yönetimini devralma olasılığı son derece düşük olduğu için, işlemler mevcut bloğun 10 blok arkasında bulunan bir bloğa kodlanmışsa güvenli kabul edilir.

PRIZM

PEERCOIN «PROOF OF STAKE» ILE KARŞILAŞTIRMA

Peercoin, madeni paranın yaş ayarını algoritmanın bir parçası olarak madencilik olasılığını kullanır. Bu sistemde, Peercoin'leriniz hesabınızda ne kadar uzun süre kaldıysa (90 güne kadar), blok oluşturmak için daha fazla güç (jeton yaşı) gerekir. Bloğu "Karşılama" eylemi, madeni para çağının saygınlığının tüketilmesini gerektirir ve ağ, toplam tüketilen en büyük madeni para yaşına sahip zinciri seçerek fikir birliğini belirler. Peercoin blokları ayrıldığında, tüketilen jeton yaşı orijinal blok hesabına geri döndürülür.

Sonuç olarak, Peercoin ağına saldırmanın maliyeti düşüktür, çünkü saldırganlar başarılı oluncaya kadar bloklar oluşturmaya (bifteği öğütme olarak adlandırılır) devam edebilir. Peercoin, blok zincirini "dondurmak" ve işlemleri bloke etmek için günde birkaç kez blok zinciri kontrol noktalarını merkezi olarak yayınlayarak bu ve diğer riskleri en aza indirir. Prizm, madeni para yaşını dövme algoritmasının bir parçası olarak kullanmaz. Herhangi bir hesap tarafından blok oluşturma "şansı", yalnızca cari bakiyesine (bu her hesabın avantajıdır), son bloktan bu yana geçen süreye (tüm sahte hesaplar tarafından paylaşılan) ve temel hedef değere (ayrıca tüm hesaplar için ortaktır).

PRIZM JETONLAR

ILK EMISYON

SON EMISYON

İlk emisyon **10 milyon** PZM ve nihai miktar **6 milyar** PZM'dir. Madeni paralar, Genesis bloğunun (blok zincirindeki ilk blok) oluşturulmasıyla basıldı. Premining, ademi merkeziyetçilik Prizm'i başlatmak için dünyanın tüm ülkelerinde nominal maliyetle, sınırlı miktarlarda uygulandı. Toplam PZM miktarı 6 milyar token olacak. Account Genesis, eksi 6 milyar PZM sınırına kadar Premining'in anti-coin sinyallerini (belirli bir cüzdan için coin gönderme sinyali) üretir.

Genesis'te anti-coin'lerin varlığının birkaç ilginç yan etkisi vardır:

Negatif hesap bakiyesi onları iptal ettiği için Genesis hesabına gönderilen tüm jetonlar etkili bir şekilde imha edilir Prizm'in ana işlevi geleneksel ödeme sistemidir, ancak çok daha fazlasını yapmak için yaratılmıştır. CWT topluluğunun hedeflerine, ana Fiat para birimleri ile PZM paritesi koşulu altında ulaşılabilir.

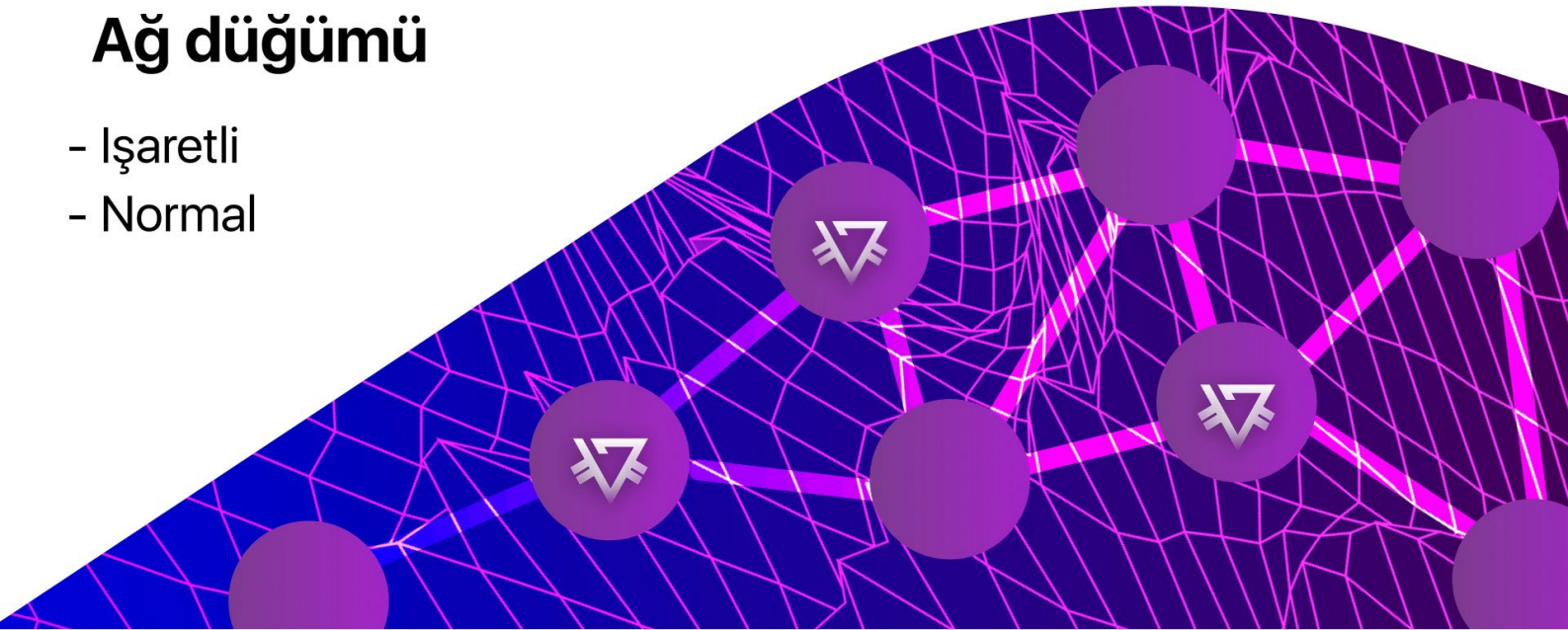
PRIZM

AĞ DÜĞÜMÜ

Ağ düğümü Prizm, ağa bir işlem yapan veya verileri engelleyen herhangi bir cihazdır. PZM yazılımına sahip herhangi bir cihaz bir düğüm olarak kabul edilir.

Ağ düğümü

- Işaretli
- Normal



İşaretli bir düğüm, hesabın özel anahtarından alınan şifreli bir belirteç ile işaretlenmiş bir düğümdür; bu simge, belirli PZM hesap adresini ve düğümle ilişkili bakiyeyi göstermek için çözülebilir. Bir düğüm üzerindeki etiket yerleştirme eylemi, bir hesap verebilirlik ve güven katmanı ekler, böylece işaretli düğümler, ağ üzerinde işaretlere sahip olmayanlardan daha güvenilirdir. Hesap bakiyesi işaretli bir düğüme ne kadar çok bağlanırsa, bu düğüme o kadar fazla güven verilir. Bir saldırgan, ağda güven kazanmak için bir düğümü işaretlemek ve ardından bu güveni kötü amaçlarla kullanmak isteyebilirken, giriş engeli (yeterli güven oluşturmak için gereken PZM maliyeti) bu tür kötüye kullanımı önler.

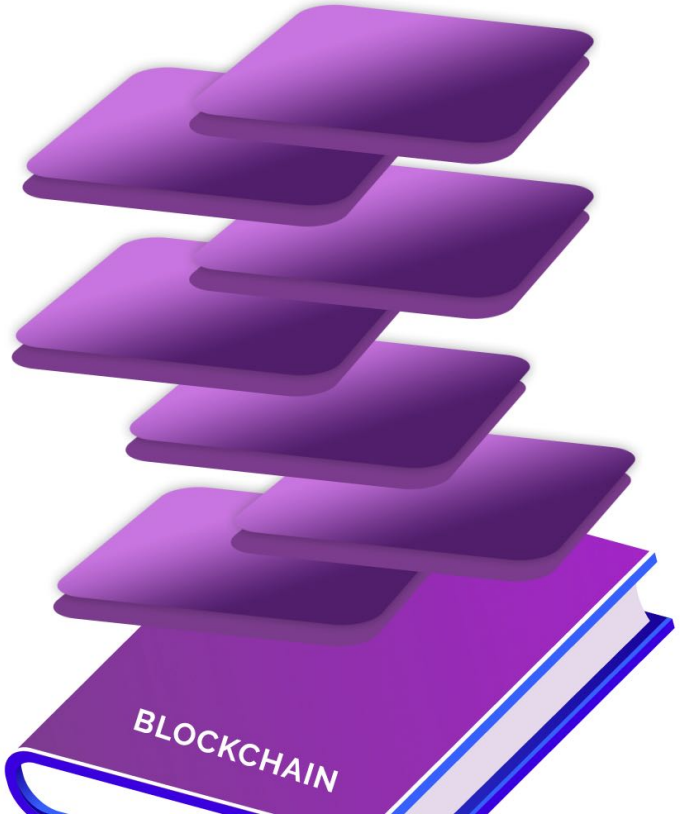
PZM ağındaki her düğüm, hem işlemleri hem de blok bilgilerini işleme ve iletme yeteneğine sahiptir. Bloklar, diğer düğümlerden alınırken taranır ve bir blok kontrolünün yapılmadığı durumlarda, düğümler geçici olarak "kara listeye" alınabilir. geçersiz blok verisi.

Her düğüm, herhangi bir kullanıcıdan gelen ağ isteklerinin sayısını saniyede 30 ile sınırlayan yerleşik DDOS koruma mekanizmalarına (Dağıtılmış Hizmet Reddi) sahiptir.

PRIZM

BLOKLAR

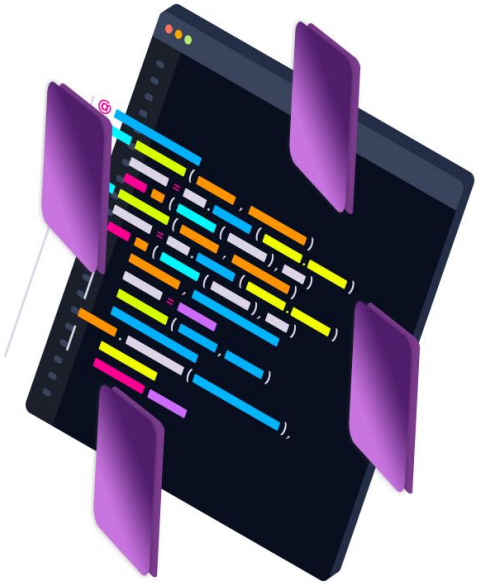
Diğer kripto para birimlerinde olduğu gibi, PZM Ledger (işlemlerin defteri), blok zinciri olarak bilinen bağlantılı bir blok dizisinde oluşturulur ve saklanır. Bu çalışma kitabı, gerçekleşen işlemlerin kalıcı bir kaydını sağlar ve ayrıca işlemlerin yapıldığı sırayı belirler. Blockchain'in bir kopyası, Prizm ağındaki her düğümde saklanır ve düğümde engellenmeyen her hesap (bu hesabın özel anahtarını sağlayarak), en az bir gelen işlemin hesap **1.440** kez onaylandı. Bu kriterleri karşılayan herhangi bir hesaba aktif hesap denir. PZM'de, her blok **255** adede kadar işlem içerir, bunların hepsinden önce tanımlayıcı parametreleri içeren **192** baytlık bir Başlık gelir. Bir bloktaki her işlem maksimum **160** bayt ile temsil edilir ve maksimum blok boyutu **32** KB'dir.



PRIZM

BLOKLAR

Tüm bloklar aşağıdaki parametreleri içerir:



- Bloğun sürümü, bloğun yüksekliği ve blok kimliği
- Genesis bloğundan saniye cinsinden ifade edilen blok zaman damgası
- Bloğu oluşturan hesabın kimliği ve hesabın genel anahtarı.
- Önceki bloğun kimliği ve karması
- Blokta depolanan işlem sayısı
- Bloktaki işlem ve komisyonların temsil ettiği toplam PZM miktarı
- Bloğa dahil olan tüm işlemler için işlem verileri, işlem kimlikleri dahil
- Yük bloğunun uzunluğu ve yararlı yük bloğunun bir karma işlevinin bir değeri
- Blok için temel hedef değer ve kümülatif zorluk

Üç değer, hangi hesabın blok oluşturma hakkına sahip olduğunu, hangi hesabın birim oluşturma hakkına sahip olduğunu ve çatışma zamanlarında hangi birimin yetkili olarak kabul edildiğini belirlemek için anahtardır: temel hedef değer, hedef değer ve kümülatif zorluk.

Referans hedef değeri

Blok oluşturma (oluşturma) hakkını kazanmak için, tüm aktif Prizm hesapları, belirtilen temel hedef değerden daha düşük bir hash değeri oluşturmaya çalışarak "rekabet eder". Bu temel hedef değeri bloktan bloğa değişir ve önceki bloğun temel hedef değerinin bu bloğu oluşturmak için geçen süre ile çarpımından türetilir.

Hedef değer

Her hesap, mevcut efektif orana göre kendi hedef değerini hesaplar.

Bu değer eşittir:

$$T = Tb \times S \times Be$$

Nerede:

T - yeni hedef değer
Tb - referans hedef değer
S - saniye cinsinden son bloktan bu yana geçen süre
Be - etkin hesap bakiyesi

Formülden de görebileceğiniz gibi, hedef değer, önceki bloktan bu yana geçen her saniye ile artar.

Maksimum hedef değer **1,53722867 x 1017'dir** ve minimum hedef değer, önceki bloğun temel hedef değerinin yarısıdır. Bu hedef değer ve temel hedef değer, belirli bir bloğun üstüne taklit etmeye çalışan tüm hesaplar için aynıdır. Tanımlanmış tek hesap parametresi, etkin bir bakiye parametresidir.

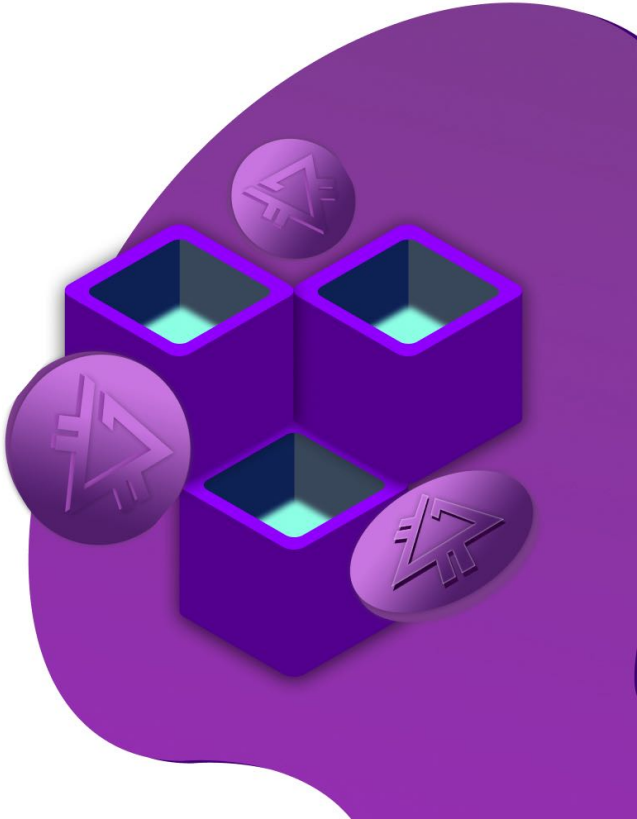
Toplam karmaşıklık

Aşağıdaki formüle göre referans hedef değerinden elde edilen toplam karmaşıklık değeri:

$$Dcb = Dpb + 264 / Tb$$

Nerede:

Dcb - mevcut bloğun karmaşıklığı
Dpb - önceki bloğun karmaşıklığı
Tb - mevcut bloğun temel hedef değeri



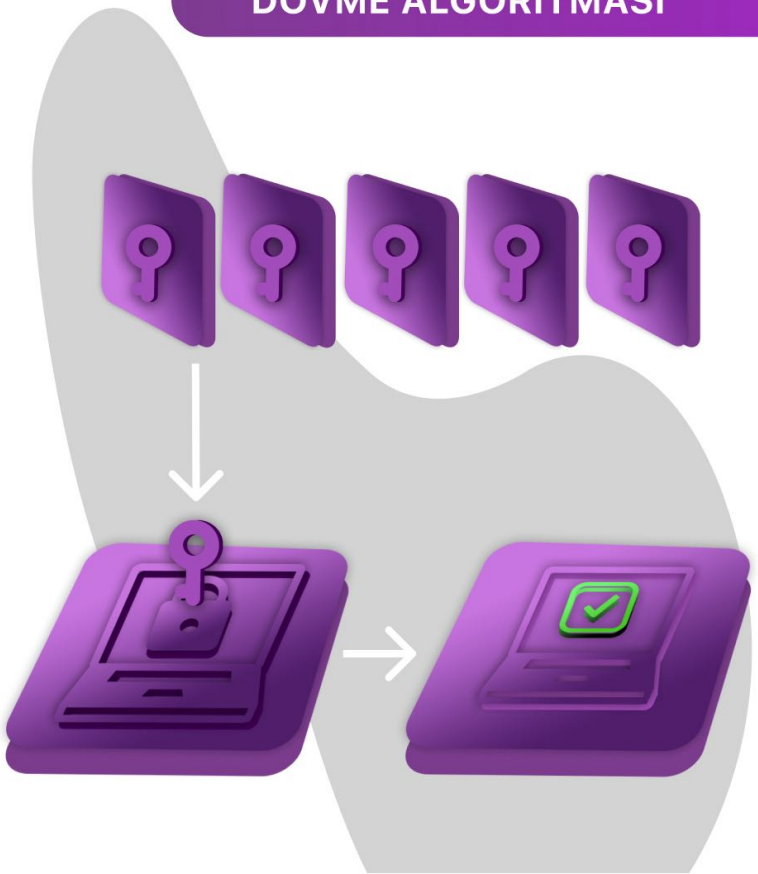
DÖVME ALGORITMASI

Zincirdeki her bloğun bir imza oluşturma parametresi vardır. Bir bloğun dövme sürecine katılmak için, aktif hesap önceki oluşturulan bloğu kendi genel anahtarıyla kriptolojik olarak imzalar. Bu, daha sonra SHA256 kullanılarak karma hale getirilen 64 baytlık bir imza oluşturur. Ortaya çıkan hash'in ilk 8 baytı, hesabın isabeti adı verilen bir sayı verir. İsabet, mevcut hedef değerle karşılaştırılır. Hesaplanan isabet hedeften daha düşükse, sonraki blok oluşturulabilir. Hedef değer formülünde belirtildiği gibi, hedef değer her saniye artar. Ağda yalnızca birkaç aktif hesap olsa bile, bunlardan biri sonunda bir blok oluşturacaktır çünkü hedef değer çok büyük olacaktır. Bunun sonucu, o hesabın isabet değerini hedef değerle karşılaştırarak, herhangi bir hesabın bloğu zorlaması için gereken süreyi tahmin edebilmenizdir. Son nokta çok önemlidir. Herhangi bir düğüm herhangi bir aktif hesap için etkin bir bakiye talep edebileceğinden, Bireysel isabet değerlerini belirlemek için tüm aktif hesaplardan geçmek mümkündür. Bu, makul bir doğrulukla, aşağıdaki hesabın sahteciliği engellemek için neyi kazandığını tahmin edebileceğiniz anlamına gelir. Bir karıştırma saldırısı, bir bahis tutarını bir sonraki bloğu oluşturacak bir hesaba taşıyarak tetiklenebilir, bu da **PZM** bahsinin, sahteciliğe katkıda bulunmadan önce **1.440** blok boyunca sabit olması gerektiğinin bir başka nedenidir (etkin bir denge değeri aracılığıyla). İlginç bir şekilde, bir sonraki blok için yeni temel hedef makul bir şekilde tahmin edilemez, bu nedenle bir sonraki bloğu kimin zorlayacağını belirleyen neredeyse deterministik bir süreç, gelecekteki blokları tahmin etme girişimleri arttıkça giderek daha fazla stokastik hale gelir.

PRIZM

DÖVME ALGORITMASI

PRIZM dövme algoritmasının bu özelliği, Şeffaf Dövme algoritmasının geliştirilmesi ve uygulanması için temel oluşturmaya yardımcı olur. Aktif bir hesaba blok oluşturma hakkı verildiğinde, **255** adede kadar onaylanmamış işlemi yeni bir blokta birleştirir ve bloğu gerekli tüm parametreleriyle doldurur. Bu blok daha sonra ağa bir Blockchain adayı olarak iletilir. Hesabı oluşturan yük ve her bloktaki tüm imzalar, onu alan tüm ağ düğümleri tarafından kontrol edilebilir. Birden fazla bloğun üretildiği bir durumda, düğümler yetkili blok olarak en yüksek birikmiş karmaşıklığa sahip bloğu seçer. Blok verileri üyeler (eşler) arasında dağıtıldığı için, her çatalda depolanan zincirlerin kümülatif karmaşıklığı incelenerek çatallar (yetkisiz zincir parçaları) tespit edilir ve sökülür.



PRIZM

PARAMINING

PARAMINING — PRIZM'in diğer kripto para birimlerine göre en önemli avantajıdır. PRIZM geliştiricileri, ekonomik çekiciliği ve dünyadaki tüm mevcut finansal araçların PZM kütlesiyle kademeli olarak değiştirilmesini amaçlayan fonların depolanmasının ödülünü belirlemek için benzersiz, doğrusal-retrograd bir mekanizma ekledi.

Bu, sistemdeki fon miktarını artırmayan temel dövme mekanizmasına bir ilavedir. PZM'de bu ek mekanizma, dünya ekonomisinin diliminde normalleştirilmiş finansal sistemin standart matematik gelişiminin ölçütlerine göre yeni madeni paralar yaratan ParaMining'dir. Hesaplamalarımıza göre, yalnızca böyle bir madeni para ağırlık artışı biçimi, mevcut tüm ekonomik araçların kademeli ve güvenli bir şekilde değiştirilmesini sağlayabilir.

PRIZM

PARAMINING

Paramining kullanarak yeni madeni para madenciliği oranı, **(1)** kişisel cüzdandaki jeton sayısı, **(2)** takipçi cüzdanlarındaki 88 seviyeye kadar jeton sayısı ve **(3)** üç ana parametreden hesaplanır. madencilik zorluk faktörü. Zorluk faktörü yüzde olarak hesaplanır ve verilen toplam jeton sayısı ile orantılıdır. Standart hesaplar için maksimum zorluk seviyesi% **98'dir** ve bu da 3 milyar üretilen PZM'ye karşılık gelir. **HOLD - MODE'daki** hesaplar için maksimum zorluk seviyesi% **97'dir**. Özelliklerine göre Paramining, basit bir kişiyi ağ işinden uzaklaştıran her şeyi dışlayan bir MLM 2.0 sistemidir, ancak aynı zamanda kişisel cüzdanında madeni para madenciliğinin hızını artırmak için onu ağın geliştirilmesine dahil eder.

M-cüzdanda herhangi bir işlem yapılırken ParaMining sistemi, cüzdan sahibinin coin sayısının değerini ve takipçilerinin cüzdanlarındaki jeton sayısını içeren bir blok zinciri yazar, bu anda cüzdan bakiyesine yeni paralar üretilir.

HOLD - Coinleri kişisel cüzdanınızda saklayın ve herhangi bir işlem yapmayın, bu nedenle coin madenciliğinde zorluk katsayısını azaltabilir ve cüzdanınızın karlılığını artırabilirsiniz.

PARAMINING SİSTEMİ herhangi bir modern kripto para biriminde benzeri olmadığı için tanıtım ve popülerleştirme için en gelişmiş araçtır. Paramining'in temel avantajı, hiçbir ağ kullanıcısının bu mekanizmaya müdahale edememesi ve yeni coin'leri tahrif edememesidir, tüm kullanıcılar sistem tarafından çıkarılan coin sayısını gerçek zamanlı olarak izleyebilir.

Paramining, bakiyesi **1 PZM'nin** üzerinde olan herhangi bir cüzdanda çalışır ve **1 milyon PZM** bakiyesine ulaşıldığında otomatik olarak durur. Ayrıca, ilk kez, herhangi bir bağlantı kullanılmadan yönlendirme bağlantıları kurma sistemi uygulandı. Yeni bir cüzdan oluşturduktan sonra, sistem ilk işlemin geldiği blok zincirinde yakalar ve kalıcı olarak değiştirilemeyen bir yönlendirme zinciri kurar, bu da küresel MLM ağları kurmayı ve yeni madeni para madenciliğinin hızını artırmayı kolaylaştırır.

Teknik uygulama şu anda ayrıntılı olarak açıklanmamaktadır, çünkü hepimiz için asıl mesele 100 "ölü" araç değil, iyi destek sağlayan araç yaratmaktır. ve iyi iş. Know-how'ımız ortaya çıkarsa, o zaman birisi kesinlikle tekrar etmeye çalışacak ve bu, yanlışlıkla dikkat dağılmasına ve bu fikrin gezegenimiz için asil ve önemli hedefler için değil, bizim yapmadığımız hedefler için kullanılmasına yol açacaktır. her zaman olumlu renklendirme niyetini bilir ve değildir.

PRIZM

PARAMINING SEÇENEKLERI

Yeni bir PZM madenciliğine başlamak için, **Paramining**'i otomatik olarak başlatan bir elektronik cüzdanda yalnızca tek bir madeni para gerekir. Bu, herhangi bir elektrik maliyeti olmadan cüzdandaki jeton sayısını artırmanıza izin veren bir işlemdir.

Paramining işlemi **1 jetonla** başlar ve cüzdanınızda 1 milyon jetona ulaştığınızda otomatik olarak durur.

Paramining — üç parametre ile düzenlenen, aynı anda tüm kullanıcılar tarafından yeni madeni paralar yaratmanın benzersiz bir yöntemidir:

1 - Kişisel cüzdanınızdaki jeton sayısı
2 - Takipçi yapısının madeni para sayısı
3 - Paratax denilen madencilik zorluğu

1 - Kişisel cüzdanınızdaki jeton sayısı

Kişisel cüzdanınızdaki jeton sayısı (PZM)	Günlük kar	Aylık kar
500.000'den 1.000.000'a	0,33%	9,9%
100.000'den 499.999'a	0,28%	8,4%
50.000'den 99.999'a	0,25%	7,5%
10.000'den 49.999'a	0,21%	6,3%
1.000 ile 9.999 arası	0,18%	5,4%
100 ile 999 arası	0,14%	4,2%
1'den 99'a kadar	0,12%	3,6%

2 - Takipçi yapısının madeni para sayısı

Toplam ses	Çarpan
1000 ile 9999 arası	2.18
10.000'den 99.999'a	2.36
100.000'den 999.999'a	2.77
1.000.000 ile 9.999.999 arası	3.05
10.000.000'den 99.999.999'a	3.36
100.000.000'den 999.999.999'a	3.88
1.000.000.000	4.37

Paramining ilkesi, **"Görünür Radyasyon"** bölümünden gelen temel fizik yasalarına dayanmaktadır. Evrenimizin modeli gibi, **55 saniyelik** karmaşık bir ilgi yeniden sayımı sayesinde sistem sürekli genişliyor, hız kazanıyor.

PRIZM

PARAMINING SEÇENEKLERI

Bakiyesi **1000 ila 110.000 PZM** arasında olan herhangi bir kullanıcı, bakiyesinin sahteciliğe dahil olması koşuluyla bileşik faizi hesaplama süresini artırabilir. TUTMA dönemini başlatmak için, hedef işlemlerle en az bir blok oluşturmanız gerekir. TUTMA süresi, gelen bir işlemle veya bir sahte ücret alınmasıyla kesintiye uğratılamaz. HOLD döneminin süresi, sahtecinin 100.000'den en az bir blok oluşturması koşuluyla sınırlı değildir.

HOLD süresi, giden bir işlemle kesintiye uğrar.

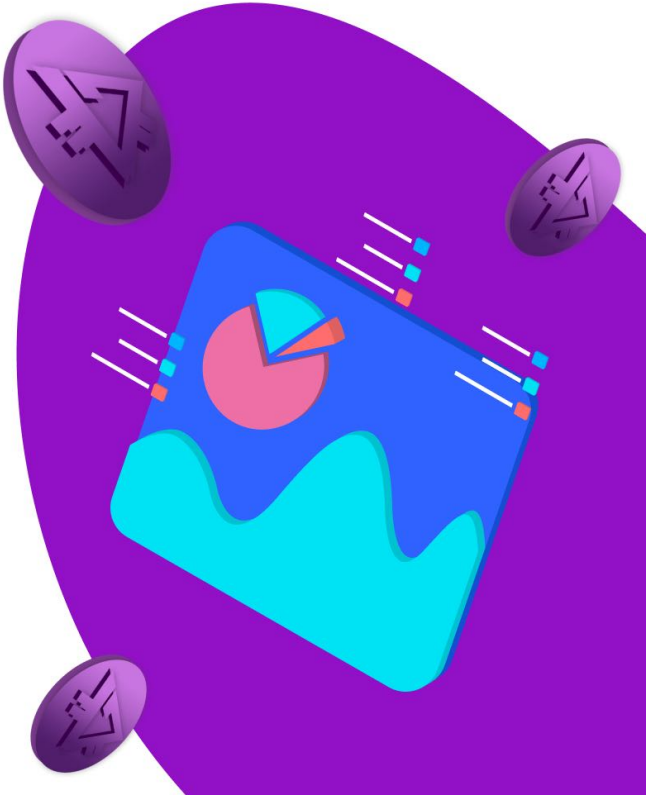
3 - Madencilik zorluğu

PARATAX

madeni para üretmenin zorluğundaki doğrusal bir artıştır ve tüm kullanıcılar tarafından halihazırda çıkarılan madeni para sayısının yüzdesi olarak ifade edilir.

Maksimum PARATAX limiti, 3 milyar PZM üretimi sırasında% 98 olacaktır.

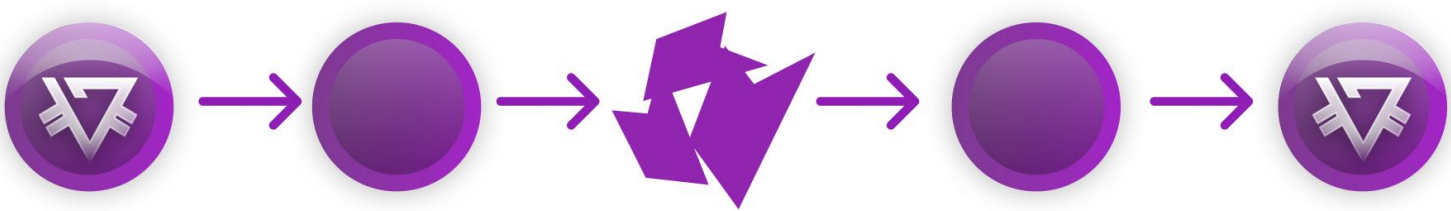
Bloğun oluşturulması sırasındaki bakiyesi 110.000 PZM'yi geçmeyen FORGERS için, PARATAX'ın maksimum değeri% 97'dir.



PRIZM

PRIZM HESAPLARI

Prizm, tasarımının bir parçası olarak akıllı bir cüzdan uygular: tüm hesaplar, **SHA256 ve Curve25519** işlemlerinin bir kombinasyonunu kullanarak her bir hesabın kod ifadesinden doğrudan türetilen, olası her hesap adresi için kişisel anahtarlarla ağda saklanır. Her hesap 64 bitlik bir sayı ile temsil edilir ve bu numara, hesabın adresindeki dörde kadar hatayı tespit etmenize veya en fazla iki hatayı düzeltmenize olanak tanıyan Solomon Kodunun Hata Düzeltmesi kullanılarak hesap adresi olarak ifade edilir. . Bu format, yanlış bir hesap adresinin bozuk paralar, takma adlar veya varlıkların geri döndürülemez bir şekilde hatalı hedef hesaplara aktarılmasına neden olabileceği endişelerine yanıt olarak uygulandı. Hesap adreslerinin başında her zaman **"PRIZM -..."** bulunur, bu da Prizm hesap adreslerinin kolayca tanınmasını ve diğer kripto para birimleri tarafından kullanılan adres biçimlerinden farklı olmasını sağlar.



Gizli bir parola ile ilişkilendirilmiş Solomon Kodu kodlu adres hesabı aşağıdaki şekilde oluşturulur:

- **Gizli parolaya, hesabın özel anahtarını almak için SHA256 kullanılarak hashing uygulanır.**
- **Özel anahtar, hesabın genel anahtarını almak için Curve25519 kullanılarak şifrelenir.**
- **Hesap kimliğini almak için ortak anahtara SHA256 ile hashing uygulanır.**
- **Hesap kimliğinin ilk 64 biti görünen hesap numarasıdır.**
- **Solomon-Code kodlaması, "PRIZM -" ön ekli görünür hesap numarası, hesabın adresini oluşturur.**

Bir hesaba ilk kez gizli bir parola ile erişildiğinde, genel bir anahtarla korunmaz. Hesaptan ilk giden işlem yapıldığında, paroladan alınan 256 bitlik genel anahtar blok zincirinde saklanır ve bu da hesabı korur. Genel anahtarlar (2256) için adres alanı, hesap numaraları (264) için adres alanından daha büyüktür, bu nedenle kod sözcüklerinin hesap numaraları ve olası çakışmalarla bire bir eşleşmesi yoktur. Bu çarpışmalar şu şekilde tespit edilir ve önlenir: Hesaba erişmek için belirli bir parola kullanıldıktan ve hesap 256 bitlik bir genel anahtarla korunduktan sonra, başka hiçbir genel-özel anahtar çifti bu hesap numarasına erişemez.

Hesap bakiyesinin özellikleri:

1. Hesabınızı faturalandırmak için temel olarak etkili bir hesap bakiyesi kullanılır. Etkin bir hesap bakiyesi, 1.440 blok için bu hesapta sabit olan tüm coin'lerden oluşur. Ayrıca, "Hesap Kiralama" işlevi, başka bir hesapta geçici bir süre için etkin bir bakiye belirlemenize olanak tanır.

2. Garantili hesap bakiyesi, 1.440 birimlik hesapta sabit olan tüm jetonlardan oluşur. Etkin bir bilançodan farklı olarak, bu bakiye başka bir hesaba devredilemez.

3. Temel hesap bakiyesi, en az bir onayı olan tüm işlemleri hesaba katar. Takviye hesap bakiyesi, başarılı zorlama bloklarının bir sonucu olarak alınan toplam PZM miktarını gösterir.

4. Onaylanmamış hesap bakiyesi, Prizm istemcilerinde görüntülenen bakiyedir. Onaylanmamış, gönderilen işlemlerde yer alan madeni paralar hariç cari hesap bakiyesini temsil eder.

5. Garantili varlık bakiyeleri listesi (bir liste yapın), belirli bir hesapla ilişkili tüm varlıkların garantili bakiyeleri.

6. Belirli bir hesapla ilişkilendirilmiş tüm varlıkların onaylanmamış bakiyeleri ve onaylanmamış varlık bakiyesi listesi.

PRIZM

CÜZDAN.DAT

Bitcoin ve ilgili para birimleri, madeni paraları almak için oluşturulan adresleri saklamak için genellikle isim ve cüzdan altında şifrelenmiş bir dosya kullanır. Prizm'de kullanılan **Next** çekirdeği bu işlevselliği ne simüle eder ne de dışlar. İstemci geliştiricileri, Prizm hesapları için özel bir anahtar grubunun şifrelenmiş bağımsız bir dosyada depolandığı bir sistemi uygulayabilir.

İşlemlerin teyidi

Tüm PZM işlemleri, geçerli bir ağ bloğuna dahil edilene kadar onaylanmamış olarak kabul edilir. Yeni oluşturulan bloklar, onları oluşturan düğüm (ve ilişkili hesap) tarafından ağa dağıtılır ve bloğa dahil olan işlemin bir onay tarafından alındığı kabul edilir. Sonraki bloklar mevcut bir blok zincirine eklendiğinde, her bir ek blok, işlem onaylarının sayısına başka bir onay ekler. Bir işlem, süresi dolmadan önce bloğa dahil edilmezse, yanar ve işlem havuzundan silinir.

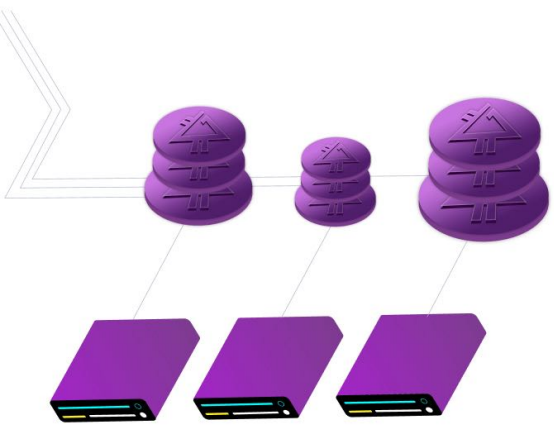
İşlemin zamanlaması

Her işlem, işlemin ağa gönderilmesinden bu yana geçen dakika sayısına ayarlanmış bir son tarih parametresi içerir. Varsayılan olarak, son tarih 1440 dakikadır (24 saat). Ağa gönderilen ancak bloğa dahil edilmeyen bir işleme, onaylanmamış işlem adı verilir.

İşlem, son işlem tarihinden önce bloğa dahil edilmemişse, işlem ağdan kaldırılır. İşlemler, geçersiz veya çarpıtılmış oldukları için ya da bloklar daha yüksek bir Komisyon ödemeyi teklif eden işlemlerle doldurulduğu için onaylanmadan bırakılabilir. Gelecekte, çoklu imzalı işlemler gibi özellikler, sona erme işlemini zorunlu kılmak için son tarihleri kullanabilir

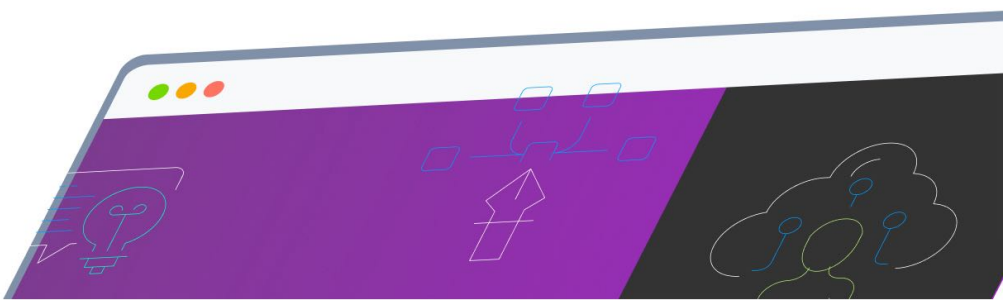
İşlemlerin oluşturulması ve işlenmesi

Bir PZM işleminin oluşturulması ve işlenmesiyle ilgili ayrıntılı bilgiler aşağıdaki gibidir: - Gönderen, işlem parametrelerini belirtir.



İşlem türleri değişir ve işlemi oluşturduğunuzda istediğiniz türü belirtirsiniz, ancak tüm işlemler için birden çok parametre belirtmelisiniz:

- **Gönderen hesabın özel anahtarı**
- **İşlem son tarihi**
- **İsteğe bağlı işlem referansı**



Prizm'deki anahtar değişimi, Diffie-Hellman'ın yüksek koruma derecesine sahip hızlı verimli eliptik eğrisini kullanarak paylaşılan bir sır oluşturan **Curve25519** algoritmasına dayanmaktadır. Algoritma ilk olarak 2006 yılında Daniel J. Bernstein tarafından gösterildi. Java ile ilgili sonraki uygulamalar Mart 2014'te Doctor Evil tarafından gözden geçirildi. Prizm'de mesajların imzalanması, **Elliptic-Curve** dijital imza algoritması **(EC-KCDSA)** kullanılarak gerçekleştirildi. **IEEE P1363a** grubu tarafından 1998 yılında **KCDSA** Görev gücü ekibi tarafından tanımlanmıştır. Her iki algoritma da yalnızca **32** baytlık bir anahtar boyutu için hız ve güvenliği dengelemek üzere seçildi..

Ana Özellikler

Gelişmiş JavaScript istemcisi

Temel yazılım Prizm'in dağıtımına gömülü olan ve yerel bir web tarayıcısı aracılığıyla erişilebilen İkinci nesil uygun istemci uygulaması. İstemci, kullanıcıların özel anahtarlarına hiçbir zaman çevrimiçi olarak erişilemeyecek şekilde uygulanan tüm önemli Prizm özellikleri için tam destek sağlar. Ayrıca, Prizm düşük öncelikli uygulama programlama arabirimi için gelişmiş bir yönetim arabirimi ve yerleşik Javadoc belgeleri içerir.

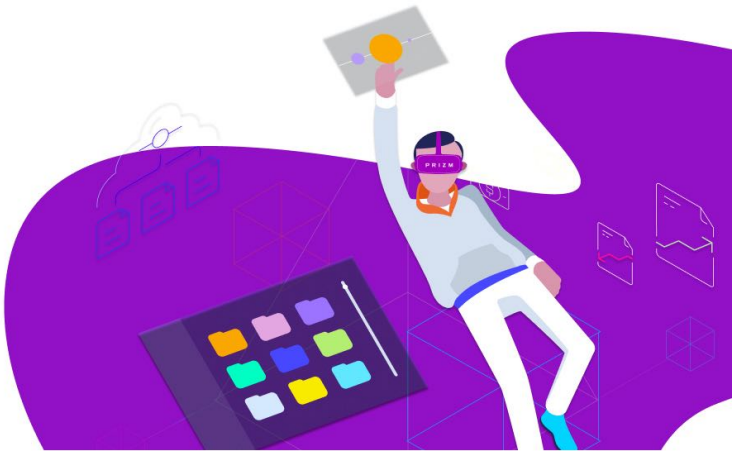
PRIZM ŞIFRELEMESININ TEMELLERI

Taşınabilir cihaz

Java köklerine dayalı çapraz platformu, Proof of Stake'in karması ve gelecekteki blok zinciri boyutunu küçültme yeteneği sayesinde Prizm, küçük, düşük güçlü düşük kaynak cihazlarında kullanım için son derece uygundur. Android ve iPhone uygulamaları ve yazılımları, RaspberryPi ve CubieTruck platformları gibi düşük güçlü ARM cihazlarına taşındı. Prizm'i düşük güçlü, akıllı telefonlar gibi her zaman bağlı cihazlarda uygulama yeteneği, çoğu Prizm ağının mobil cihazlarda desteklendiği bir senaryo sunmamızı sağlar. Bu cihazların düşük maliyeti ve kaynak tüketimi, geleneksel kripto para birimi Proof of Work ile karşılaştırıldığında ağ maliyetlerini önemli ölçüde azaltır.

Temel ödemeler

Herhangi bir kripto para biriminin en temel özelliği, bir hesaptan diğerine coin transfer etme yeteneğidir. Bu, Prizm işlemlerinin en temel türüdür ve temel ödeme işlevlerini kullanmanıza izin verir.



PRIZM

PRIZM ANA ÖZELLIKLER

POS — dövme yazma

İki teknolojiyi aynı anda karıştırmak: paramining dövme. Klonlara karşı koruma olarak, sistemin sıvı olacağının garantisi olarak kaynak kodları belli bir süreye kadar kapatılır (sıralanmaz).

- **Yapıda 88 seviyeli ortaklık programı**
- **Kripto sisteminin NEXT Core | POS**
- **Mobil cihazlar için kullanıcı dostu arayüz**
- **Kullanıcı parolası sunucuya gönderilmiyor**

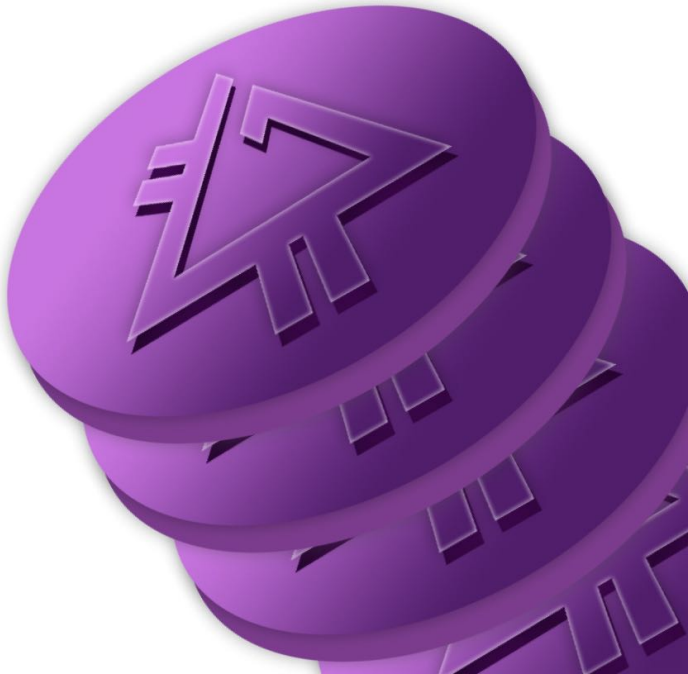
Hiçbir şey tehlikede değil

"Hiçbir şey tehlikede değil" saldırısında, sahtekarlar gördükleri tüm çatalların üzerine bloklar oluşturmaya çalışırlar çünkü bu onlara neredeyse hiçbir maliyeti yoktur ve herhangi bir çatalı görmezden gelmek, o çatal durumunda kazanılacak ödülleri blokta kaybetmek anlamına gelebilir en kümülatif zorluğa sahip zincir olacak şekilde tasarlandı. Bu saldırı teorik olarak mümkün olsa da şu anda pratik değildir. Prizm ağı, uzun blok zinciri çatalları deneyimlemez ve düşük blokların ödülü, kâr için güçlü bir teşvik sağlamaz; Ek olarak, bu kadar küçük bir kazanç için ağ güvenliğinden ve güvenden taviz vermek her zaferi boşa çıkarabilir.

Tarihe saldırılar

"Tarihe saldırı" da, birisi çok sayıda madeni para alır, satar ve daha sonra madeni paraları satılmadan veya takas edilmeden hemen önce başarılı bir çatal oluşturmaya çalışır. Saldırı başarısız olursa, girişim değersizdir çünkü madeni paralar zaten satılmış veya transfer edilmiştir; Saldırı başarılı olursa, saldırgan jetonlarını geri alır. Bu saldırının ekstrem biçimleri, eski hesaplardan özel anahtarlar almayı ve bunları doğrudan Genesis bloğundan başarılı bir zincir oluşturmak için kullanmayı içerir. Ödüllerde, ana geçmiş saldırısı genellikle başarısız olur çünkü tüm bahisler sahte için kullanılmadan önce 1,440 blok olarak sabitlenmelidir; Ek olarak, her bloğun oluşturduğu etkin hesap bakiyesi, blok kontrolünün bir parçası olarak doğrulanır. Bu saldırının ekstrem biçimi genellikle başarısız olur çünkü PRIZM blok zinciri mevcut blok yüksekliğinin arkasında 720 bloktan fazla olacak şekilde yeniden düzenlenemez. Bu, kötü bir oyuncunun bu tür bir saldırıyı gerçekleştirebileceği zaman çerçevesini sınırlar.

UYGULAMA



Prizm'de ele alınan Bitcoin sorunları.

Prizm, Bitcoin'e yanıt olarak bir kripto para birimi 2.0 olarak oluşturuldu. Prizm, Bitcoin'de iyi bilinen işlevleri kullanır ve endişe verici yönleri dikkate alır. Bu uygulama, Prizm teknolojisi ile düzelen Bitcoin Protokolü ve ağı ile ilgili sorunları giderir.

Günlük işlem sayısı hakkında

2013'ün sonunda, Bitcoin ağında işlenen işlem sayısı günde maksimum 70.000'e ulaştı, bu da saniyede yaklaşık 0,8 işlem (tps) anlamına geliyor. Müşterilerin "tam" sitesinde her on dakikada bir (ortalama olarak) oluşturulan bir megabaytlık mevcut standart Bitcoin blok boyutu, mevcut Bitcoin ağının maksimum bant genişliğini yaklaşık 7 TPS ile sınırlar. Bunu, 10.000 TPS işlemek için VISA ağının bant genişliğiyle karşılaştırın ve Bitcoin'in bugün olduğu gibi rekabet edemeyeceğini göreceksiniz.

Blockchain Boyutu

Bitcoin Blok Zinciri, Ocak 2009'da piyasaya sürülmesinden bu yana gerçekleşen tüm Bitcoin işlemlerini e-kitap kayıtlarını içeren oluşturulmuş veri bloklarının eksiksiz bir sıralı koleksiyonudur. Dört yıl sonra, Ocak 2013'te Bitcoin'in blok zinciri boyutu 4 gigabayt (GB) idi - iki saatlik bir filmi DVD'de saklamak için gereken yaklaşık veri miktarı. On sekiz ay sonra, Temmuz 2014'te, Bitcoin blok zinciri boyutu neredeyse beş ila 19 gigabayt (GB) 37 arttı. Bitcoin blok zinciri üstel bir büyüme gösteriyor ve orijinal Bitcoin Protokolünde yapılacak değişiklikler bunun için bir çözüm gerektirecek.

PRIZM'in yanıtı

Mevcut durumunda, Prizm günde 367.200 işlemi gerçekleştirebilir - mevcut Bitcoin zirvesinin dokuz katından fazla. Şeffaf Dövme uygulaması, işlemlerin neredeyse anında işlenmesini sağlayarak bu limiti önemli ölçüde artırır.

İşlemi onaylama zamanı

Bitcoin için işlem onay süresi çoğunlukla 2013 boyunca 5 ila 10 dakika arasında değişiyordu. 2013'ün sonunda Çin bankalarının Bitcoin'leri işlemesine izin verilmeyeceğinin duyurulmasının ardından, ortalama Bitcoin işlem süresi önemli ölçüde artarak 8-13 dakikaya yükseldi. , 19 dakikalık periyodik zirvelerle. O zamandan beri, onay süresi 8'den 10 dakikaya kaydı. Bununla birlikte, bir Bitcoin işlemini tamamlamak için birkaç kontrol (genellikle tercih edilen altı onay) gerektiğinden, Bitcoin tarafından ödenen varlıkların satışı tamamlanmadan önce bir saat kolayca geçebilir.

PRIZM'in yanıtı

PZM için ortalama blok oluşturma süresi tarihsel olarak 80 saniyeydi ve ortalama işlem işleme süresi aynıydı. İşlemler on onaydan sonra güvenli kabul edilir, bu da işlemlerin 14 dakikadan daha kısa sürede kalıcı hale geleceği anlamına gelir. Şeffaf Dövme uygulaması, neredeyse anında işlem yapmanızı sağlar ve bu da bu süreyi daha da azaltır.

Merkezileşme sorunları

Bitcoin için hash oranının yanı sıra karmaşıklık artışı, yeni gelenlerin girişi için yüksek bir engel oluşturdu ve mevcut madencilik kurulumları için daha düşük karlar yarattı. Bitcoin tarafından kullanılan blokları teşvik etme teşviki, özel madencilik ekipmanlarının 44 büyük tek katmanlı kurulumlarının oluşturulmasına ve ayrıca küçük bir büyük madencilik havuzlarına 45 güvenilmesine yol açmıştır. Bu, "merkezileştirme" etkisine yol açmıştır. Büyük hacimli madencilik, azalan insan sayısının kontrolünde yoğunlaşmıştır.Bu, yalnızca Bitcoin'in baypas etmek için tasarladığı türden bir güç yapısı oluşturmakla kalmaz, aynı zamanda tek bir madencilik operasyonu veya havuzunun% 51 kazanabileceği gerçek olasılığı sunar. Toplam madencilik kapasitesinin 46 ağındaki toplam madencilik kapasitesinin% 51'ini gerçekleştirdiğini ve toplam ağ hash gücünün yalnızca% 25'ini gerektiren saldırılar da var. 2014 Ocak ayı başlarında GHash.io kendi madenciliğinin gücünü gönüllü olarak azaltmaya başladı, % 51 düzeyine yaklaştı. Birkaç gün sonra güç havuz, şebekenin toplam kapasitesinin% 34'üne düştü, ancak hız hemen artmaya başladı ve Haziran 2014'te tekrar tehlikeli seviyelere ulaştı.

PRIZM'in yanıtı

Prizm'de kullanılan Proof of Stake algoritmasının sağladığı teşvikler, yaklaşık% 0,1 gibi düşük bir yatırım getirisi sağlıyor. Her blokta yeni madeni paralar üretilmediğinden, bloklar oluşturmak için ortak çabaları teşvik eden ek bir "madencilik için ödül" yoktur. Veriler, Prizm ağının başlangıcından bu yana oldukça merkezsiz kaldığını göstermektedir: büyük (ve büyüyen) benzersiz hesapların sayısı ağa bloklar ekler.

Proof of Work - bakım maliyetleri

Mevcut bitcoin üzerindeki işlemlerin onaylanması ve dolaşıma girmek için yeni bitcoinlerin oluşturulması, sürekli çalışması gereken muazzam bir hesaplama gücü gerektirir. Bu bilgi işlem gücü, madenciler tarafından yönetilen sözde madencilik teçhizatı tarafından sağlanır. Bitcoin madencileri, bir sonraki işlem bloğunu genel bitcoin zincirine eklemek için birbirleriyle rekabet eder. Bu, son on dakika içinde meydana gelen tüm Bitcoin işlemlerini birleştirerek ve bunları, içinde tesadüfen belirli sayıda ardışık sıfır bulunan bir veri bloğu olarak şifrelemeye çalışarak "hashing" ile yapılır. Hashing madencileri tarafından oluşturulan deneme bloklarının çoğu bu hedef sıfır sayısına sahip değildir, bu nedenle küçük değişiklikler yapar ve tekrar dener. Bu "kazanan" bloğu bulmaya yönelik bir milyar girişim GH olarak adlandırılır ve Madencilik teçhizatı, saniyede kaç GH gerçekleştirebileceği ile tahmin edilir ve GH / sn ile gösterilir. Kriptolojik olarak doğru bir Bitcoin bloğu oluşturan ilk kişi olan kazanan madenci, hemen bir ödül alır. 25 yeni bitcoin - yazı yazılırken ödül yaklaşık 15.750 ABD dolarıydı. Madenciler arasında ödüllü bu yarışma yaklaşık her on dakikada bir tekrarlanır. 2014'ün başında, günde yaklaşık 2,2 milyon dolara eşit olan 3.500'den fazla bitcoin üretildi. Bahiste çok fazla para varken, madenciler kazanma şanslarını artırmak için madencilik teçhizatı teknolojisindeki hızlı silahlanma yarışını destekliediler. Başlangıçta, bitcoin'ler tipik bir masaüstü bilgisayar olan Merkezi işlemci (CPU) kullanılarak çıkarıldı. Daha sonra hızı artırmak için ileri teknoloji grafik kartlarında özel bir grafik işleme biriminin (GPU) yongası kullanıldı. Daha sonra programlanabilir geçit dizisine (FPGA) sahip mikroişlemci ve daha sonra özel uygulamalı entegre devrelerin (ASIC) çipi kullanıldı. ASIC teknolojisi, bitcoin madencileri için hattın zirvesidir, ancak silahlanma yarışı, farklı nesil ASIC yongalarının ortaya çıkmasıyla devam ediyor. Mevcut ASIC yongaları nesli, 28 nm cihaz tabanlı nanometre cinsinden mikroskobik transistörlerinin boyutuna göre. 2014'ün sonunda 20nm ASIC modülleri ile değiştirildi.

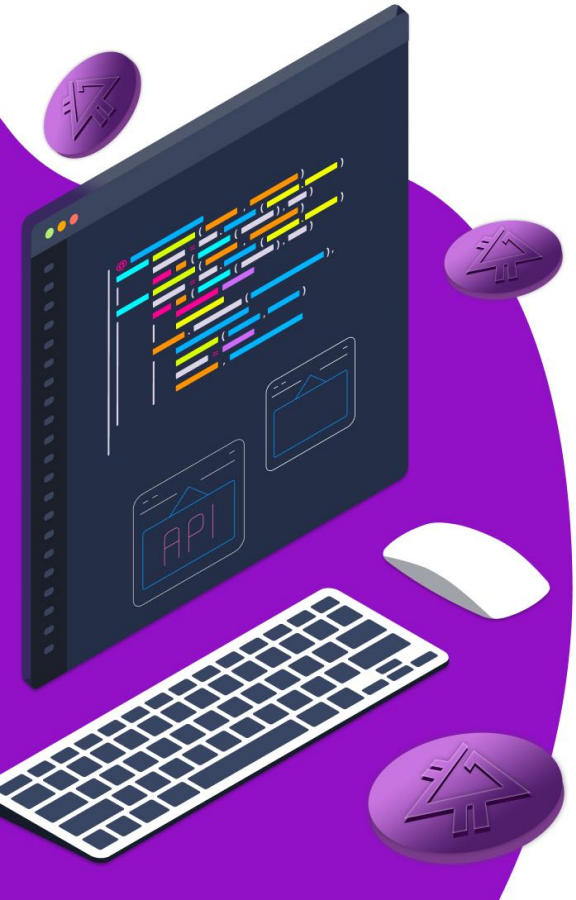
Proof of Work - bakım maliyetleri

Yeni bir son teknoloji madencilik teçhizatı örneği, bir elektrik tüketimi için 600GH / sn sağlayacak olan Butterfly Labs'ın 28nm ASIC kartı "the Monarch" olacaktır. 350 watt ve 2.200 USD fiyat. Şu anda Bitcoin'in mevcut operasyonlarını desteklemek için kullanılan madencilik teçhizatı altyapısı dikkat çekicidir. Bitcoin ASIC, otistik bilim adamlarına benzer - yalnızca bir bitcoin bloğunun hesaplamasını yapabilirler ve daha fazlasını yapamazlar, ancak bunu bir süper bilgisayarın hızlarında tek bir hesaplama ile yapabilirler. Kasım 2013'te Forbes dergisi, "küresel bitcoin hesaplama gücü, 500 kombine süper bilgisayardan 256 kat daha hızlıdır!" Başlıklı bir makale yayınladı. Ocak 2014'ün ortalarında, blockchain.info sitesinde depolanan istatistikler, Bitcoin işlemlerinin sürekli desteğinin yaklaşık 18 milyon GH / s'lik sürekli bir hash oranı gerektirdiğini gösterdi. Birinde gün, bu hashing gücü, 2,2 milyon doları kapsayacak bir büyülü 144 blok arayışı için Bitcoin'in mayonezi tarafından üretilen ve reddedilen 1,5 trilyon deneme bloğu üretti. Neredeyse tüm Bitcoin hesaplamaları, DNA'yı modelleyerek veya E.T.'den radyo sinyalleri arayarak felaketi düzeltmeyi amaçlamaz; Bunun yerine, tamamen boşa harcanırlar. Bu savurgan Bitcoin arka plan desteğiyle ilişkili güç ve maliyetler çok büyük. Tüm Bitcoin madencilik teçhizatları yukarıda açıklandığı gibi "Monarch" seviyelerine sahipse - ve yükseltilene kadar olmayacaklar - 63 milyon $ 'dan fazla değere sahip 30.000 makineden oluşan bir havuzu temsil edecekler. Çalışma sırasında 10 megavattan fazla sürekli güç tüketir ve elektrik faturası günlük 3,5 milyon dolardan fazladır. Gerçek rakamlar, bugün Bitcoin'i gerçekten destekleyen mevcut, daha az verimli madencilik teçhizat havuzu için çok daha yüksek. Ve bu rakamlar, bitcoin mevcut değerinden ilerledikçe üstel büyüme eğrisinde yukarı çıkıyor. Saniyede en fazla yedi işleme kadar saniyede bir işlem.

Prizm Çözümleri

Prizm ağının maliyet ve enerji verimliliğinin analizi, tüm PRIZM ekosisteminin yılda yaklaşık **60.000 $ 'a** muhafaza edilebileceğini gösteriyor ki bu, şu anda Bitcoin ağını işletme maliyetinden neredeyse **2.200** kat daha ucuz.

PRIZM.SPACE



Madeni para sahipleriyle ilgili olarak POW bakımının maliyeti

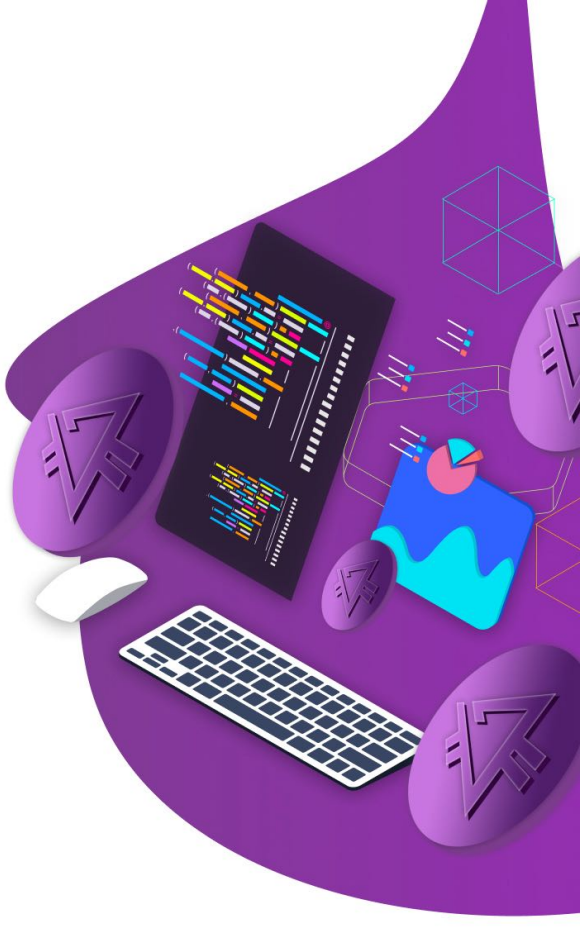
Büyük elektrik maliyetlerine ek olarak, bitcoinlerin basitçe depolanması için gizli bir ücret vardır. Bulunan her blok için, bloğu oluşturan kişi bir ödül alır. Yazım sırasında, toplam Bitcoin arzında% 10 enflasyon olan yaklaşık 12,5 BTC'lik bir ödül (şimdilik). Ait olduğu her 1000 dolarlık bitcoin için, bir kişi ağ güvenliği için madencilere "ödeme yapmak" amacıyla bitcoin için 100 dolar öder.

Prizm gücü sizinle olsun!

PRIZM Entegrasyonu

PRIZM ödeme sistemi, kripto ödemeleri almanın ve göndermenin en kolay yoludur.

PRIZM'i projenize, çevrimiçi mağazanıza, eşanjörünüze vb. Kolayca entegre edebilirsiniz.



Adım adım öğretici:

https://pzm.space/en/pzm-integration/

Prizm ödeme sistemi entegrasyonu

PRIZM ile çalışmaya başlamak için ağ düğümünü (Düğüm) ve API_Servlet'i başlatmanız gerekir.

Ağ Düğümü

Yazılım, tek bir sunucuda ve farklı sunucularda çalışabilir. Ancak, rahatınız için onu bir tanesinde başlatmak daha iyidir.

Öncelikle, düğümü başlatmalı ve eşitlenirken beklemelisiniz. Sonraki adım, PrizmAPIServlet modülünün yapılandırılmasıdır.

PrizmCore wallet

https://github.com/prizmspace/PrizmCore#prizmcore-wallet-download-v1103-windows-osx-linux

Easy API Gateway

https://github.com/prizmspace/PrizmCore#easy-api-gateway-prizmapiservlet

Yapılandırma
PrizmAPIServlet

Arşivin içinde adında bir dosya var

PrizmAPIServlet.properties

çizgide

passphrase: NONE

«NONE» yerine projeniz tarafından kullanılacak cüzdanın özel anahtarını yazmalısınız.

Alanları doldurduktan sonra, sunucu uygulamasını şuradan başlatmalısınız:

run-servlet.sh

çizgide

sendkey: NONE

«NONE» yerine şifreyi yazmalısınız (yetkisiz işlemlere karşı ek bir koruma olarak bozuk para gönderme işlevi tarafından kullanılacaktır).

PHP'de uygulama örneği

Madeni para alma ve gönderme ile çalışmanın tanımı, hazır fonksiyon örnekleri ve çalışma ilkelerinin tanımı. Mysql veritabanı işlem listesini depolamak için kullanılır, aşağıdaki depolama tablosunun bir dökümü ve tabloyla çalışmak için kod örnekleri vardır (QueryBuilder'ı uygularsanız, bu bir sorun olmayacaktır).

Ana çalışma prensibi

Cron-görevinde, her 2-5 dakikada bir servlet'e talepte bulunan bir komut dosyası vardır, böylece mağazanın cüzdanında yeni işlemler alabilir. İşlemlerin listesini aldıktan sonra, bunları yerel veri tabanına kaydetmelisiniz. Veritabanında herhangi bir işlem yoksa, komutu herhangi bir parametre olmadan çalıştırmalısınız. Ancak yeni işlemler almak istiyorsanız son işlemin numarasını parametre olarak göndermelisiniz..

Örnek fonksiyonun:

```
<?php
function historyPZM($last_id = 0)
{
 if ($last_id) {
  $url = 'http://localhost:8888/history?fromid=' . $last_id;
 } else {
  $url = 'http://localhost:8888/history';
 }
 $page = '';
 $result = get_web_page($url);
 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }
 $array_new = array();
 $xcmorewrite = explode("\n", str_replace("\r", '', $page));
 foreach ($xcmorewrite as $value) {
  if ($value) {
   $array_new[] = explode(';', $value);
  }
 }
 return $array_new;
}
?>
```

Sayfa içeriğini alma işlevi:

```
<?php

function get_web_page($url)
{
 $uagent = "Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.14";
 $ch = curl_init($url);
          curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // recovers the web page
         curl_setopt($ch, CURLOPT_HEADER, 0); // doesn't recover headers
         curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1); // follows redirects
         curl_setopt($ch, CURLOPT_ENCODING, ""); // handles all encodings
        curl_setopt($ch, CURLOPT_USERAGENT, $uagent); // useragent
        curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 20); // time-out of the connection
        curl_setopt($ch, CURLOPT_TIMEOUT, 20); // time-out of the answer
        curl_setopt($ch, CURLOPT_MAXREDIRS, 2); // stops after the 10th redirect

 $content = curl_exec($ch);
 $err = curl_errno($ch);
 $errmsg = curl_error($ch);
 $header = curl_getinfo($ch);
 curl_close($ch);

 $header['errno'] = $err;
 $header['errmsg'] = $errmsg;
 $header['content'] = $content;
 return $header;
}

?>
```

Sayfa içeriğini alma işlevi:

You can test it through the console, for example: curl http://localhost:8888/history

The example of the Cron-task handler script for receiving new transactions and the table structure

```
CREATE TABLE `pzm_history` (
  `id` bigint(20) NOT NULL,
  `tarif_id` int(1) NOT NULL,
  `tr_id` varchar(255) NOT NULL,
  `tr_date` varchar(255) NOT NULL,
  `tr_timestamp` int(11) NOT NULL,
  `pzm` varchar(50) NOT NULL,
  `summa` decimal(16,2) NOT NULL,
  `mess` varchar(255) NOT NULL,
  `status` int(1) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

** All necessary keys and autoincrement for ID should be added to the table

İşleyici:

Bu örnekte, yerel veritabanına kaydedilmesi gereken yeni işlemlerin listesini alırsınız.

Bu nedenle, cüzdandaki tüm işlemlerin bir geçmişini tutarsınız ve ileride bunları yerel veri tabanımızda anahtar verileri kullanarak arayacaksınız.

```
<?php
$nomer = getLastPrmHistory();
$historys = historyPZM($nomer);

foreach ($historys as $item) {
   if ($item['0'] != "No transactions!") {

// this line adds data to the ‘pzm_history’ table using
INSERT IGNORE

PzmHistory::find()->insertIgnore([
        'tr_id' => $item['0'],
        'tr_date' => $item['1'],
        'tr_timestamp' => $item['2'],
        'pzm' => $item['3'],
        'summa' => $item['4'],
        'mess' => $item['5'],
        'status' => 0
      ]);
   }
}
```

```
function getLastPrmHistory()
{
//  this line searches for the last row in the table to get the last ID of the transactions which are in the table

if (!empty($pzmHistory = PzmHistory::find()->orderBy('id', "DESC")->first())) {
  return $pzmHistory->tr_id;
 };
 return 0;
}

?>
```

Projeniz aynı Prizm Cüzdan ile çalışmalıdır, bu nedenle tüm müşterilere dahili hesabı yenilemek için aynı gereksinimler ve işlemin aynı hash kimliği verilecektir. Müşteriye, ödeme yorumunda hash tanımlayıcısını belirten şartlara kesinlikle bir işlem yapması gerektiğini bildirdiğinizden emin olun.

Bu nedenle, ödeme yorumunda müşterinin karma tanımlayıcısı varsa, yeni gelen işlemleri analiz edecek ve dahili hesaba para yatıracak başka bir işlem olmalıdır. Ayrıca, müşteri için, üzerine tıkladıktan sonra bu kullanıcı için yeni işlemleri arayabilen ve kaydedebilen ayrı bir **"ÖDEDİM"** düğmesi yapmanız gerekir.

Madeni para göndermenin ikincil işlevleri ve işlevleri

Cüzdan için genel anahtar alma (yalnızca bakiyesi olan etkinleştirilmiş cüzdanlar için çalışır).

```
<?php

 function destinationPZM($pzm)
   {
      $url = 'http://localhost:8888/publickey?destination=' . $pzm;
      $page = '';
      $result = get_web_page($url);
      if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
         $error = $result['errmsg'];
         return '';
      } else {
         $page = $result['content'];
         $haystack = "Public key absent";
         $haystack2 = "Send error!";
         $pos = strripos($page, $haystack);
         $pos2 = strripos($page, $haystack2);
         if ($pos === false AND $pos2 === false) {
            $xcmorewrite = explode(' ', $page);
            $page = trim($xcmorewrite[0]);
            return $page;
         } else {
            return '';
         }
      }
      return $page;
   }

?>
```

Cüzdanın mevcut bakiyesini almak:

```
<?php

 function getBalancePZM($pzm)
   {
      $ip = '*******';  // пример 192.168.1.1:9976  with port
  $url = 'http://'.$ip.'/prizm?requestType=getAccount&account=' . $pzm;
      $page = '';
      $result = get_web_page($url);
  //print_r($result); die;
      if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
         $error = $result['errmsg'];
         return '';
      } else {
         $page = $result['content'];
         $page = json_decode($page, true);
         if ( isset($page['balanceNQT']) ) {
           return $page['balanceNQT'] / 100;
         } else {
           return 0;
         }
      }
   }

?>
```

Madeni para gönderme yöntemi:

```
<?php

public function payPZM($summa, $pzm, $public_key, $text)
{
 $p2 = SENDKEY;   // this is the password that you specified during setup
 $return = false;
 $url = 'http://localhost:8888/send?sendkey=' . $p2 . '&amount=' . $summa .
'&comment=' . urlencode($text) . '&destination=' . $pzm . '&publickey=' . $public_key;
 $page = '';
 $result = get_web_page($url);

 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }

 if (preg_match('/^\+?\d+$/', $page)) {
  $return = true;
 } else {
  $return = false;
 }
 return $return;
}

?>
```

WHITEPAPER

PRIZM

Dijital para biriminin ilk kavramı

Prizm Whitepaper Revizyonu

Haziran, 2020

PZM.SPACE