Freeman Family

4 Temmuz 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Eşler Arası Elektronik Nakit Sistemi

TASARRUF ARACI + DEĞİŞİM ARACI + HESAP BİRİMİ

Dünya üzerinde 1.7 milyar yetişkin insan küresel finans sistemine erişememekte, 1.3 milyar yetişkin insan ise yetersiz hizmet almaktadır. Epic Cash, bireyleri global piyasaya bağlayarak mevcut insan potansiyelini açığa çıkarmaktadır. Hızlıdır, kullanımı neredeyse ücretsizdir ve herkese açıktır.

Version 7.1b **Turkish**

İçindekiler

I. Özet

Epic Cash, gerçek eşler arası dijital paralara doğru olan yolculukta, kişisel finans sisteminin temel taşıdır. Epic Cash, dünyanın en etkili gizlilik korumasını sağlayan dijital para birimi olmayı hedeflemektedir ve bu hedefi gerçekleştirmek için paranın üç temel işlevini yerine getirmektedir.

1. **Tasarruf Aracı:** ileri bir tarihe kadar saklanabilir, alınabilir, borsa aracılığıyla takas edilebilir ve alındığında tahmin edilebilir değerde olabilir.
2. **Değişim Aracı:** - bir değer standardını temsil eden; ve mal alımı veya hizmet kullanımı için takas edilebilir olan herhangi bir şey.
3. **Hesap Birimi:** - bir şeyin değerinin muhasebeleşebildiği ve karşılaştırma yapılabildiği birim.

	$ USD	BTC	EPIC
Tasarruf Aracı	✗	✓	✓
Değişim Aracı	✓	✗	✓
Hesap Birimi	✓	✗	✓

Bitcoin, 2009 yılında ilk blokzinciri tabanlı dijital para birimi olarak ortaya çıktı. Bitcoin ile birlikte diğer dijital para birimlerinin risklerinin değerlendirilebildiği üç tanımlayıcı özellik şunlardır:

- Güvene Gerek Duyulmaması - ağın çalışması için kimsenin merkezi bir kuruluşa veya karşı tarafa güvenmesi gerekmez.
- Değişmezlik - işlemler geri alınamaz;
  ;
  a. Geçmişe dönüp işlemleri değiştirmek imkansız olmalıdır;
  b. Özel anahtarın sahibi dışında herhangi birinin, cüzdandaki fonları taşıması imkansız olmalıdır;
  c. Tüm işlemler blokzincirine kaydedilmelidir.
- **Merkeziyetsizlik** – "Blokzincirleri politik olarak merkeziyetsizdir (kimse blokzincirlerini kontrol edemez) ve mimari olarak da merkeziyetsizdir (altyapısal olarak başarısızlık ihtimali yoktur)..."

Bitcoin, zaman içinde test edilmiş temellere bağlı kalıp, para politikasının yapısına uygun olarak teknolojik olarak yeni yollar ortaya çıkardı. Bu bağlamda Bitcoin'in başarısı güvenilir olması, değiştirilemez olması, merkeziyetsiz bir blokzincirine sahip olması ile birlikte sınırlı sayıda olmasıyla ilişkilendirilebilir. Epic Cash, Epic dijital para biriminin etkili bir tasarruf aracı işlevi görmesini sağlamak için Bitcoin'in enflasyon düşürme ve arzın sınırlı olması gibi politikalarına benzer olarak tasarlandı. Bitcoin'in başarısına rağmen, 10 yıl önceki yapısı ile ilgili olarak günümüzde bazı eksiklikler mevcuttur. Diğer projeler bu eksikliklerin üstesinden gelmek için çalışmalar yaptı. Epic Cash olarak, eksiklikleri en iyi şekilde gidermek için bunları başlangıç noktamız olarak araştırdık. Epic Cash'ten önceki projelerin keşfedilen hatalarını mükemmelleştirmemize yardımcı olması için Grin kod temelini ve birçok projenin özelliklerini kullanmaya karar verdik. Epic Cash aşağıdaki kilit özelliklere sahiptir:

- Takas Edilebilirlik – elirli bir Epic para birimin değeri her zaman diğer bir Epic para birimine eşit olmalıdır. Bunu tıpkı, Yen veya Yuan para birimlerinin her zaman başka bir Yen veya Yuan ile eşit olması ve takas edilebilmesi gibi düşünebiliriz.
- Ölçeklenebilirlik – Epic Cash, yoğunlaştırılmış kaynak ihtiyacı olmadan kolayca yeni düğümlerin kurulabildiği verimli bir blokzinciri sağlamaktadır. Epic Cash blokzinciri, Bitcoin'in mevcut üretiminin en az iki katı kapasiteye sahiptir.
- Gizlilik– Epic Cash blokzinciri, işlem detaylarını üçüncü şahıslardan koruyarak Epicsahiplerinin ve kullanıcılarının gizliliğini korur ve takip edilemez. Epic Cash blokzinciri gözetleme durumlarına karşı görünmez olacak şekilde tasarlanmıştır.
- Hız– Epic Cash işlemleri sorunsuz, kesintisiz ve kendisinden önceki nesil blokzinciri teknolojilerinden çok daha hızlı bir şekilde gerçekleştirmektedir. Bitcoin blokzincirinde işlem onayının tamamlanması için altı adet 10 dakikalık blok gerektirirken, Epic işlemleri 1 dakikalık sürede bir blok çıkarıldıktan hemen sonra tek bir blok onayında gerçekleşmektedir.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Gizlilik

Günümüzde para kullanımı, hesap birimlerinin insanlar ve kurumlar arasında toplu şekilde aktarımı olarak gerçekleşmektedir. Herhangi bir zamanda, para birimlerinin alanı aşağıdaki sorular cevaplanarak haritalandırılabilir:

1. *Parayı kimler tutuyor ve ne kadar tutuyorlar?*
2. *Kim kiminle ve ne kadar işlem yapıyor?*

Geleneksel fiat para birimleri ve Bitcoin için bu soruları rahatlıkla cevaplayabiliriz. Bunu yaparken tüketim kalıpları, mülkiyet ve işlem tarafları gibi insanların yaşamları hakkında birçok veri ortaya çıkarılabilir. Değer aktarımları yani para transferleri izlenerek bireyin çıkarları ve niyetleri hakkında oldukça doğru sonuçlar çıkarılabilir. Gizlilik barındırmayan işlem verileri, üçüncü kişilerin elinde tehlikeli bilgilere dönüşebilirler.

Geçtiğimiz on yılı göz önüne alırsak kripto paraların kullanımı, çeşitli blokzinciri uygulamalarında "gizlilik" özelliğinin devam ettiğini göstermektedir. Bu bağlamda gizlilik kavramının yapısı değişmekle birlikte önemli bir ölçüde dikkate alınmalıdır. Gizlilik özelliği göz ardı edildikçe, kripto paraların en temel özelliklerinden biri olan güven özelliği düşüşe geçmektedir. Bitcoin blokzincirinin analiz hizmetlerinin başarısı ile de kanıtlandığı gibi, Bitcoin gizlilik skalasının sonuna doğru yerleştirilmiştir. Kullanıcılar, Bitcoin blokzincirince yanlış işlem yapmadıklarından emin olmak için adım adım ilerlemelidir. Epic Cash çözümü, işlemleri anonim hale getirerek ve bu sayede hem bireyin gizliliğinin hem de işlemlerin gizliliğinin temel düzeyde tasarlanmasını sağlayarak bu temel özelliği geri yükler.

Kimlik Gizliliği

İşlem Gizliliği

Kimlik Gizliliği

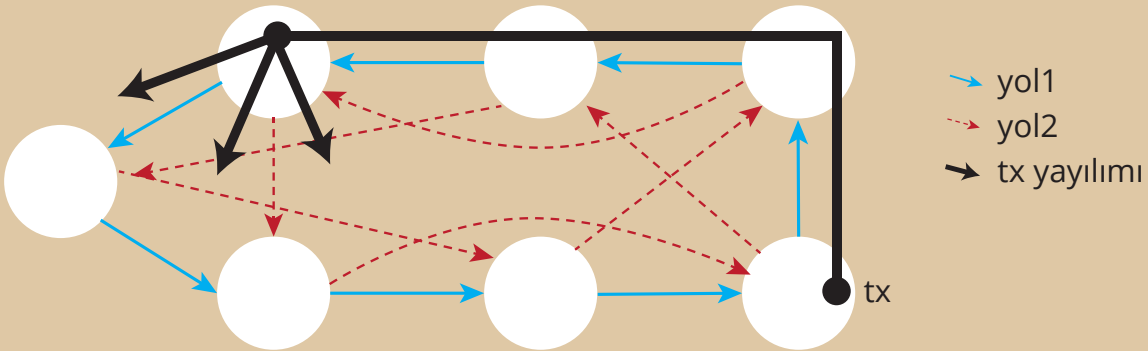
Çoğu kripto para birimi, Bitcoin gibi adresleri bir cüzdanın özel anahtarlarından türetilen ve ortak anahtarlara yönlendirilen cüzdanlarda saklanır. Bu adresler, dijital dünyadaki bireyin özel kasasının konum belirleyicileri olarak düşünülebilir. Epic Cash blokzinciri, adresleri tamamen ortadan kaldırarak bunun yerine, tüm genel ve özel anahtarların tek kullanımlık bir şekilde üretildiği çoklu imza teknolojisini kullanmaktadır.

Bitcoin cüzdan adresleri dijital dünyadaki bir kasanın konum belirleyicisi olduğundan dolayı belirli bir zamanda ve belirli bir yerde cüzdanını bilgisayara bağlayan cüzdan sahibi İnternet Protokolü (IP) adresine kadar izlenebilir. Basitçe açıklarsak; bir Bitcoin işlemi gerçekleştiğinde, işlem "düğüm" adı verilen bir iletişim merkezinden yayınlanır ve ardından "eş" adı verilen diğer düğümlere yayılır. Bu bilgiler daha sonra, ağın her yerine arka arkaya bu düğümlerin eşlerinin her birine hızlı bir şekilde yayılmaktadır. Bu işlem tanımına uygun bir şekilde "Dedikodu Protokolü" olarak adlandırılmıştır. Bu da her işlemin oldukça basit bir şekilde, görünür bir çevrimiçi konuma ve Bitcoin sahibinin bulunabileceği fiziksel bir konuma sahip olduğu anlamına gelmektedir. Gazeteci Grace Caffyn'ın da belirttiği gibi, "Bitcoin bir evdeki internet bağlantısından yapılan bir Google aramasından farksız değildir."

Cüzdan adreslerini ekarte etmenin yanı sıra, Epic Cash blokzincirindeki IP adreslerinin izlenememesini sağlayarak kimlik gizliliğini güvence altına alır. Bunu, Dandelion ++ Protokolü entegrasyonuyla yapmaktadır. Orijinal Dandelion Protokolü'nün geliştirilmesiyle ortaya çıkan Dandelion ++ Protokolü, yedi araştırmacının blokzincirindeki gizliliği yok etme saldırılarına karşı mücadelesi çerçevesinde oluşturulan bir protokoldür. Dandelion ++ aracılığıyla, işlemler rastgele iç içe geçmiş şekilde yollanır veya "kablolar" üzerinden geçirilir. Daha sonra aniden köklerinden üflendiğinde adeta bir Karahindiba çiçeğinin yaprakları gibi büyük bir düğüm ağına yayılır (Şekil 1). ve bu sayede işlemlerin kökenlerine ve dolayısıyla işlemlerin gerçekleştiği kaynak IP adreslerine kadar izlenmelerini neredeyse imkansız hale getirir.

Şekil 1: Dandelion ++ Protokolü ile Anonimleştirme İşlemleri

Dandelion++ dört normal diyagramda iç içe geçmiş iki yoldan biri üzerinden iletiler şeklinde gerçekleşir ve ardından yayınım özelliği kullanarak yayılır. Şekilde işlem mavi yoldan üç farklı şekilde yayılır. Bu sayede, işlemlerin kendi kaynaklarına göre izlenmesi ve gizliliğin açığa çıkması oldukça zorlaştırılır.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

İşlem Gizliliği

Epic Cash blokzinciri, işlemin tutarları ve o işlemin gönderici-alıcı ilişkisini gizleyerek işlem gizliliğini garanti eder. Bu durum, Confidential Transactions (CT) ve CoinJoin gibi çeşitli teknolojiler ile bilinen fikirlerin, Bitcoin Core geliştiricisi, kurucu ortağı ve Blockstream'in CTO'su Gregory Maxwell'in büyük ölçüde geliştirdiği yöntemlerin uygulanmasıyla başarılmıştır.

İlk olarak Adam Back tarafından hayata geçirilen ve daha sonra Maxwell tarafından geliştirilen CT, işlem gizliliğini korumak için önce şifre çözmeden şifreli bilgilerle ilgili hesaplamaları gerçekleştiren bir yöntem olan homomorfik şifreleme yoluyla işlemleri daha küçük parçalara bölerek çalışır. İşlemler bölündüklerinde gözlemciler, bu işlem parçalarının değerlerini gizlemek için rastgele sayıları işlem parçaları ile karıştıran bir sistem devreye girer. Bu sayede işlemlerin gerçek miktarları görünmez hale gelir. Sonuç olarak sadece işlem yapan taraflar borsadaki değeri bilirler. İşlem ağ tarafından çıkış değerlerinin toplamının giriş değerlerinin toplamına eşit olduğunu teyit ederek doğrulanır. Çıkış körleştirme faktörlerinin toplamı, giriş körleştirme faktörlerinin toplamına eşittir.

Meraklı gözlerin işlemleri takibini daha da karmaşık hale getirmek için, tüm Epic Cash işlemleri CT ile gizlenir ve ardından işlem yapan taraflar arasındaki bağlantıları gizlemek için diğer işlemlerle karıştırılır. Bu uygulama, Maxwell'in ikinci konsepti CoinJoin ile yapılır.

CoinJoin'i basitçe anlatmaya çalışırsak, A, B ve C'nin sırasıyla X, Y ve Z'ye Epic gönderdiğini hayal edin. CoinJoin aracılığıyla gönderilen işleme dair bilinen tek şey A, B ve C'nin gönderdiği ve X, Y ve Z'nin aldıkları bilgisi ve işlem tutarlarının görünmez kaldığıdır. CoinJoin sistemi, bir blok içindeki tüm işlemleri tek bir işlemde birleştiren, Tek Yönlü Toplu İmzalar (OWAS) teknolojisi ile Epic Cash'in temelini oluşturur.

Gizlilik: Özet

Epic Cash blokzinciri, bireylerin ve bireylerin yaptığı işlemlerin gizliliğini aşağıdakilerle korumaktadır:

- **Cüzdan adreslerinin kaldırılması - Epic Cash blokzincirindeki dijital kasalarda konum tanımlayıcı yani cüzdan adresi bulunmamaktadır. İşlemler doğrudan kişiden kişiye aktarım temelinde yapılır;**
- **Gizli İşlemler - işlemler çoklu parçalara ayrılır ve elde edilen parçalar diğer işlem parametrelerinin değerlerinin bilinmemesi için, diğer parçalarla karıştırılarak gizlilik sağlanır;**
- **Dandelion ++ Protokolü - işlemin dijital olarak takibini önlemek için işlemi yapanın IP adresini gizler;**
- **CoinJoin - İşlem yapan taraflar arasındaki bağları gizlemek için işlemler paketler halinde birleştirilir.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Takas Edilebilirlik

Litecoin'in yaratıcısı olan Charlie Lee, takas edilebilirlik özelliğinin Bitcoin ve Litecoin'de eksik olan tek kripto para özelliği olduğunu belirtmiştir. Gizlilik ve takas edilebilirliğin bu paralar için bir sonraki savaş alanı olduğunu kabul etmiştir. Dünyanın en önde gelen blockchain uzmanlarından Andreas Antonopoulos bozulmuş kripto paraların piyasa için yıkıcı olduğunu iddia etti. "Takas edilebilirlik ve gizlilikten kaçarsanız, o kripto para bir işe yaramaz."[7]

Takas edilebilirlik, bir malın ya da varlık kümesine ait bir setin ve bu setin ayrı birimlerinin eşit değerde olmasını ve birbirlerinin yerine geçebilmesini sağlar. En eski para birimlerini önceki takas sistemlerinden ayıran şey tam olarak budur. Takas edilebilirliği olmayan para, değerini hızlı bir şekilde kaybedecektir. Aşağıda gösterileceği gibi, çoğu kripto para takas edilebilirlik konusunda belirsizdir; oysa Epic Cash'in gizlilik mimarisi aynı tehditlere karşı geçirimsiz olmasını sağlar.

Blokzinciri teknolojisinin şeffaf olmasının doğası gereği, Bitcoin'e benzer çoğu kripto para, tutuldukları her cüzdandan doğru ve kolay bir şekilde takip edilebilir. Üçüncü şahıslar ve hükümetler, Bitcoin blokzincirindeki faaliyetlerde gerçekleştirilen işlemleri hızlı bir şekilde tanımlamak için giderek daha karmaşık sistemler kullanmaktadır. Bu durum doğal olarak, kripto paralarla yapılan işlemlerin günün birinde yasaklanabileceği ve bununla birlikte iyi niyetli insanların zararına neden olabileceği endişelerine yol açmaktadır.

19 Mart 2018'de, ABD Dış Varlık Kontrol Ofisi (OFAC) Amerika'da kişilerin veya işletmelerin işlem yapmasının yasak olduğu kuruluşlar olan kripto para adreslerinin SDN listesine eklendiğini düşündüğünü açıkladı.

Daha da rahatsız edici olan durum OFAC, halihazırda kripto para sahiplerinin adreslerini SDN listesine dahil etmeyi reddetti; ve bu da söz konusu kripto para biriminin sahiplerini bir kara listeye eklenme tehlikesi ile karşı karşıya bıraktı. New York Üniversitesi'nde görevli hukuk profesörü Andrew Hinkes'in "takas edilebilirliğe güle güle" açıklaması, halkın yeni teknolojilerle işlevli kripto paralar beklemesini sağladı. [8].

Tüm bu gelişmeler göz önüne alındığında, kripto piyasasında bir karışıklık beklentisi ve birçok köklü kripto para biriminin yok olmasını beklemek olası bir düşünce haline geldi. Bununla birlikte Epic, bu teknik dökümanda daha önce açıklanan güçlü gizlilik özellikleri nedeniyle bu sorunu tamamen önleyen az sayıdaki kripto para biriminden biridir. Epic, kimlik ve mülkiyet arasındaki bağlantıyı ve işlem yapan taraflar arasındaki ilişkiyi tamamen ortadan kaldırarak, hiçbir zaman bir kişiye veya bir faaliyete bağlı olmayan bir yapıdadır. Bu nedenle Epic'in değeri kullanıcılarından bağımsız olmaya devam etmekte ve kötü niyetli insanlar tarafından kriminal, finansal veya siyasi arenalarda kolaylıkla manipüle edilemeyecek, yüksek derecede gizlilik ve güvenlik sağlamaktadır.

> **"... BOZULMUŞ KRİPTO PARALAR YIKICIDIR. EĞER TAKAS EDİLEBİLİRLİK VE GİZLİLİĞİ YOK EDERSENİZ, O KRİPTO PARA HİÇBİR İŞE YARAMAZ"** **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Ölçeklenebilirlik

Epic Cash, gereksiz işlem verilerini barındırmayan ve bu sayede yer tasarrufu sağlayan teknolojik bir tasarımın bir sonucu olarak ölçeklenebilirlik konusunda gelişmeler sağlayan bir MimbleWimble uygulamasıdır. Bunu sağlayan Cut-Through özelliği, blokzincirinin Bitcoin de dahil olmak üzere çoğu şifreleme işleminden farklı olarak zaman içinde daha az yer kaplamasını ve yeni düğümlerin bellek ve bilgi işlem gücüne minimum yük oluşturmasını garanti edecek şekilde tasarlanmıştır. Alan verimliliğini koruyarak geniş çapta düğümlerle dağılmış bir ağı güçlendirir ve merkeziyetsizliği teşvik eder. Ayrıca, her Bitcoin düğümü tüm blokzinciri verilerini depolamak zorunda olsa da, Epic Cash düğümleri küçük bir blok alt kümesi oluşturarak ağ güvenliğine katkı sağlamaktadır.

Çoğu kripto para birimi, tüm işlem verilerinin blokzincirinde sınırsız şekilde depolanmasını gerektirir. Bitcoin blokzincirinin hafızası günde 0.1353 GB artarken, Ethereum blokzinciri günde 0.2719 GB ile daha da hızlı bir şekilde artmaktadır. Bitcoin blokzinciri şu anki hızıyla büyümeye devam ederse, en son ödül bloğu 2140 yılında kazıldığı zaman yaklaşık 6 TB boyutunda olacaktır. Ethereum ise bu tarihe kadar 10 TB'yi geçecektir. MimbleWimble altyapısında olmayan çoğu blokzincirinde, işlemler dünyanın her yerindeki düğümler tarafından doğrulanması gerekmektedir. Veri arttıkça, bununla beraber her düğümdeki yük de artar. Şu an mevcut Bitcoin zincirinin yaklaşık boyutu olan 200 GB'da bile, verilerin senkronize edilmesi kararlı bir ağ ve yüksek hızlı disk okuma ve yazma özelliği gerektirmektedir.

Sonuç olarak, madencilik masraflı hesaplama kaynaklarından yararlanan büyük madencilik havuzları giderek daha da merkezileşti. Tüm Bitcoin blokzinciri verileri Epic Cash blokzincirinde saklanacak olsaydı, neredeyse %90 daha az alana sığacaktı. Küçük olan hızlıdır; çünkü her işlemi iletmek ve işlemin güvende olması için daha az zaman gerektirir.

MimbleWimble, bu depolama ikilemini "Cut-Through" olarak adlandırılan yenilikçi bir yöntem ile çözmektedir. Cut-Through teknlojisinin nasıl çalıştığını anlamak için, öncelikle işlemlerin ve blokların bir MimbleWimble blokzincirinde nasıl oluşturulduğuna bakmak en iyi yöntemdir.

Girdiler:

Eski çıktılara referanslar;

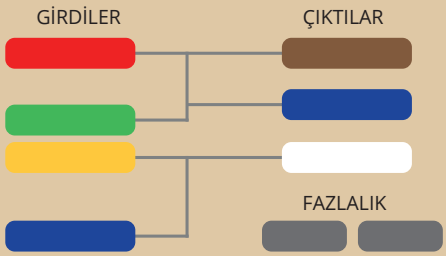
Çıktılar:

Gizli işlem çıktıları ve koruma önlemleri;

Fazlalık:

Çıktılar ve girdiler arasındaki fark ve kimlik doğrulama ve enflasyonla mücadele kanıtı için kullanılan imzalar.

Şekil 2:
MimbleWimble işlem parçaları.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Tüm Epic Cash blokları şunları içerir:

İşlem girişlerinin Merkle ağaçları;

İşlem çıktılarının Merkle ağaçları ve koruma alanları;

Fazlalık değerlerin ve imzaların bir listesi.

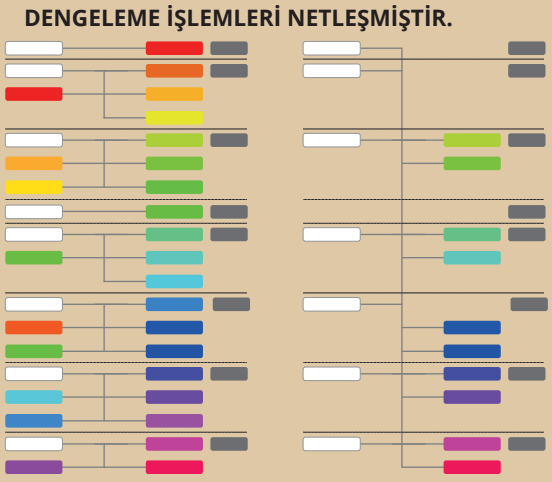
Andrew Poelstra'nın sunumlarından uyarlanmış olan Şekil 2 ve 3'te, beyaz girdi hücreleri olarak gösterilen yeni kazılmış Epic'i görebiliriz. Aynı renkli hücreler, harcanan girdilere sahip işlem çıktılarını temsil eder. Cut-Through yöntemiyle, girdiler ve eşleşen harcanan çıktılar blok içerisinde yer açmak için kaldırılır ve bu da blokzincirinde depolanması gereken veri miktarını azaltır. İşlemler blokzincirinden çıkarılırken, sadece 100 bayt boyutundaki kalan çekirdekler, işlemlerin gerçekleştiğini kalıcı olarak belgelemektedir.

Bloklar oluşturulmaya devam ettikçe, MimbleWimble blokzincirinde Cut-Through yöntemi uygulanır. Böylece uzun vadede bloklar arasında geriye kalanlar ise blok başlıkları (yaklaşık 250 bayt), harcanmamış işlemler ve işlem çekirdekleridir. (yaklaşık 100 bayt) Piyasaya sürülecek ikinci MimbleWimble uygulaması olan Grin, Bitcoin zincirine benzer sayıda işlem yapan bir MimbleWimble zincirinin Bitcoin'in zincirinin büyüklüğünün yaklaşık% 10 olacağını göstermiştir. Ayrıca, bir bloktaki düğümün boyutu Bitcoin blokzinciri için birkaç GB'lık yer kaplayacakken, MimbleWimble ile potansiyel olarak birkaç yüz megabayta kadar optimize edilebilmektedir."[12]

Bu durum, tüm blokzincirinin her bir düğüm tarafından depolanması gerektiren Bitcoin ile belirgin bir fark oluşturmaktadır. Zamanla, Epic Cash blokzincirinin alan verimliliği, Bitcoin blokzincirine göre büyüdükçe, düğümlerin Epic Cash ağına katılımıyla ilgili maliyet verimliliği de artacaktır. Bununla birlikte blokzincirine katılımdaki daha düşük engeller, ağ tasarımının düğüm katmanında çok önemli bir özellik olan esnekliği sağlamaya yardımcı olmaktadır.

MimbleWimble uygulanması ve Cut-Through yöntemiyle blokzinciri tasarrufu yöntemi sayesinde Epic Cash blokzinciri, kripto para komünitesi tarafından sıklıkla göz ardı edilen bir özellik olan tam ölçeklenebilirlik sunar. Bitcoin ve benzeri şekilde düşünen projelerin temel özelliği merkeziyetsizliktir. Bir coin'in saniyede kaç işlemi gerçekleştirebildiğine bakılmaksızın, geniş ve çeşitli bir ağ tarafından sürdürülememesi ne kadar iyi olabilir? Blokzincirindeki alan ve hafıza gereklilikleri bu şekilde onaylanacaksa, madencilik şirketlerinin aşırı güçlenmesi durumunda, kripto para komünitesinin merkeziyetsiz bir ekosistem yaratma çabaları engellenmiş olacaktır. Tüm bunlarla birlikte ek verim sağlamak için, Epic Cash'in geliştirme yol haritasındaki kısa vadeli bir amaç olarak bir Lightning uygulaması planlanmaktadır.

Şekil 3: MimbleWimble'da Cut-Through yönteminden önce ve sonra işlemlerin şeması.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Para Politikası

Epic Cash ve Bitcoin'in para politikası oldukça benzerdir. Epic Cash, sirkülasyon arzı ilk önce hızlı bir şekilde genişleyecek ve ardından 2028'de Bitcoin sirkülasyon arzı ile senkronize olacak şekilde tasarlanmıştır. Bundan sonra, 2140 yılında maksimum 21 milyon Epic arzına ulaşana kadar azalan bir oranda artacaktır. Epic Cash, uzun vadede değer olarak güvenli bir saklama aracı olma niteliğine sahiptir. Çünkü dolaşımdaki arz, emisyon ömrü boyunca herhangi bir noktada bilinir ve sabit bir maksimum arzla sonuçlanır. Epic Cash para politikası aşağıdaki dört özellik ile tanımlanmaktadır:

- Epic Cash, ilk dokuz yılında hızlı emisyon özelliği ile toplamda 20,343,750 Epic (toplam arzın% 96,875'i) madencilikle kazılmış olacaktır. Kesin emisyon oranları, bu teknik dökümanın Emisyon Takvimi bölümünde belirtilmiştir;
- Epic'in dolaşımdaki arz ve emisyon oranı, 24 Mayıs 2028 civarındaki tekilleşme sonrasında Bitcoin ile senkronize olur. Tekilleşmenin ardından emisyon oranı artan oranda azalırken, dolaşımdaki arz azalan oranda artacaktır;
- Bitcoin'in maksimum 21 milyon adete ulaştığı zaman ile aynı anda, yani 2140 yılında maksimum 21 milyon Epic arzına ulaşılacaktır;
- Epic, 8 ondalıklı bölünebilirlik yapısına sahiptir. Öyle ki, tıpkı 1 Bitcoin'in 100.000.000 satoshi'ye eşit olması gibi 1 Epic, 100.000.000 freeman'a eşittir.

Epic Cash para politikası, aşağıdaki nedenlerden dolayı Bitcoin ile aynı şekilde modellenmiştir:

- Bitcoin'in ekonomik temelleri ile olan benzerlik, yani dolaşımdaki arzın az olması ve güçlü bir değer saklama aracı olarak görülmesi;
- Kripto para topluluğu, hali hazırda Bitcoin'in modeline ve kuruluşundan bu yana geçen on yıldaki kanıtlanmış sicilini yeterli derecede tanıyor. Bu nedenle Epic, arzını yaklaşık olarak Bitcoin'in dolaşımdaki tedarikiyle senkronize ederek ve Bitcoin'in maksimum arz ve bölünebilirlik yapısını yansıtarak, kitlesel olarak kabul görmeye çalışıyor.

VI. Emisyon Takvimi

Epic Cash, her biri önceki dönemlerine göre blok ödüllerinde düşüşlerle tanımlanan toplam 33 madencilik döneminden oluşmaktadır. 1 numaralı Epic bloğu olan Epic Genesis'in kazımı, Ağustos 2019'da gerçekleşmiştir. Bloklar dakikada bir blok olmak üzere kazılır. İlk beş dönem yani yaklaşık dokuz yılda 20 yıllık Bitcoin emisyonuna denk olarak Epic maksimum arzının% 97'si üretlecektir. Bu durum, Bitcoin'in olağanüstü yükselişini kaçırmış olanlar için "zamanı geri alma" şansı gibi düşünülebilir.

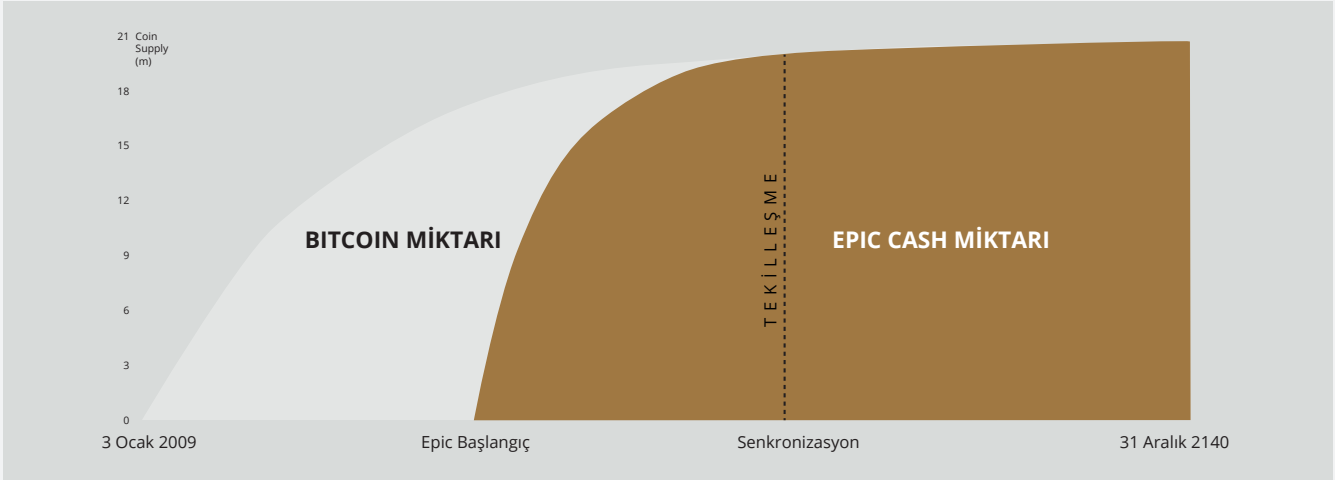
Tablo 1 emisyon programı başlangıç ve bitiş tarihlerini gösterir. İlk yedi maden dönemi, bunlara karşılık gelen blok ödülleri ve her dönem için ortaya çıkan dolaşım malzemeleri gibi bilgiler içermektedir. 8 ila 33 arası madencilik dönemleri, tabloya dahil edilmemiştir. Bu dönemlerde takip eden her bir dönemin, tam olarak Bitcoin'deki gibi bir önceki dönemin ödülünün yarısı kadar olan bir blok ödülü olacaktır. Bu dönemlerin her birinde kazılan Epic miktarı, yaklaşık 1460 günü kapsayan 4 yıllık dönemdeki blok ödüllerinin toplamı kadar olacaktır.

2028 yılında gerçekleşecek olan Epic Singularity'de yani tekilleşmede, Epic'in dolaşımdaki arzı Bitcoin'in dolaşımdaki arzına denk olacaktır; bu noktadan sonra Epic Cash, her dört yılda bir yarıya inen blok ödülleri ile Bitcoin blok ödülleri ve yarılanma modelini benimseyecektir. Bunun tek istisnası, Epic bloklarının Bitcoin'in her on dakikada bir blok hızına karşı, her dakika üretilmesi ve bir dakikada kazılmaya devam etmesidir. Bunun amacı Epic'in dolaşımdaki adetinin, Bitcoin'in dolaşımdaki adeti arasındaki parite dengesi sağlamaktır.

Tablo 1: İlk yedi madencilik dönemi için emisyon takvimi. Tarihler yakın yaklaşımlardır.

Dönem	1	2	3	4	5	SINGULARITY	6	7
Blok Ödülü	16	8	4	2	1		0.15625	0.078125
Başlangıç Tarihi	Ağustos 1, 2019	Haziran 29, 2020	Ekim 11, 2021	Haziran 3, 2023	Ağustos 10, 2025		Mayıs 24, 2028	Mayıs 22, 2032
Bitiş Tarihi	Haziran 29, 2020	Ekim 11, 2021	Haziran 3, 2023	Ağustos10, 2025	Mayıs 24, 2028		Mayıs 22, 2032	Mayıs 20, 2036
Uzunluk (gün)	334	470	601	800	1019		1460	1460
Başlangıç Miktarı	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Bitiş Miktarı	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
Toplam Miktarın Yüzde Oranı	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Şekil 4: Epic ve Bitcoin Emisyon Takvimleri



VII. Madencilik

Epic Cash blokzinciri, çok çeşitli hesaplama donanımlarına elverişli şekilde tasarlanarak merkeziyetsizliği benimsetme amacındadır. Epic madenciliği yapmak için başlangıçta üç karma algoritma aracılığıyla CPU'lar, GPU'lar ve ASIC'ler kullanılabilir: RandomX, ProgPow ve CuckAToo31+. Bu algoritmalar, blokzincirinin bütünlüğünü bozmadan çok iyi şekilde çalışırken değiştirilebilirler.

1 RandomX ve CPUs

RandomX, genel amaçlı CPU'lar için optimize edilmiş bir Çalışma İspatı (PoW) algoritmasıdır. Aşağıdaki hedeflere ulaşmak için rastgele program yürütmeleri çeşitli teknolojilerle birlikte kullanılır:

- Tek çipli ASIC'lerin gelişiminin önlenmesi;
- Özel amaçlı donanımın genel amaçlı CPU'lara göre verimlilik avantajının en aza indirilmesi.

Epic madenciliğini CPU ile yapabilmek için, iş parçacığı başına 2 GB fiziksel RAM, 16 KB L1 önbellek, 256 KB L2 önbellek ve 2 MB L3 önbellek içeren bir aralık gerekmektedir. Windows 10 aygıtları ise 8 GB veya daha fazla RAM gerektirir. Cep telefonlarının bir gün uygulanabilir madencilik düğümleri haline gelebileceği günlerin uzak olduğu düşünülemez. Epic Cash madencilik ağında erken CPU entegrasyonu ile, Epic Cash ağını güvence altına alarak blok ödüller kazanmak için mütevazı araçların kullanılabilmesi birçok kişi için mükemmel bir fırsattır.

2 ProgPow ve GPUs

Programlı Çalışma İspatı (ProgPow), bir GPU'nun bilgi işlem özelliklerinin çoğundan yararlanan ve böylece donanımın toplam enerji maliyetini verimli bir şekilde değerlendiren, bellek bant genişliğine ve rastgele matematik dizilerinin çekirdek hesaplamasına dayanan bir madencilik algoritmasıdır. ProgPow, emtia GPU'larından tam olarak yararlanmak adına özel olarak tasarlandığından, özel donanım ile önemli ölçüde daha yüksek verimlilik elde etmek hem daha zor hem de daha pahalıdır. Dolayısıyla, ProgPow algoritması, Bitcoin'in SHA-256'sı gibi diğer birçok PoW algoritmasında sıkça görüldüğü gibi, büyük ASIC havuzlarının GPU'lardan daha fazla rekabet etme imkanlarını azaltır. GPU'lar, CPU'lar kadar yaygın olmasalar da, hala yaygın olarak bulunmaktadırlar. Günümüzde Nvidia ve AMD tarafından yürütülen teknolojik gelişmeler sayesinde, GPU'lar CPU bazında birçok madencilik çözümünün birimini birim bazında paralel olarak işleyebilmektedir. Bu her yerde bulunma ve yüksek işlem gücünün birleşiminden dolayı, GPU'ların Tablo 2'de belirtildiği gibi, ilk dönemlerde madencilik faaliyetlerinin çoğunluğunu oluşturacağı açıktır.

3 CuckAToo+31 and ASICs

CuckAToo31+, Hollandalı bilgisayar bilimci John Tromp tarafından geliştirilen Cuckoo Cycle algoritmasının ASIC dostu bir devşirmesidir. ASIC dostu olmayan CuckARoo29'un başka bir versiyonu olan CuckAToo31+ rastgele çift taraflı diyagramlar üretmekte ve madencilere bu diyagramın köşelerinden geçen 'N' uzunluğunda bir döngü bulma görevi sunmaktadır.

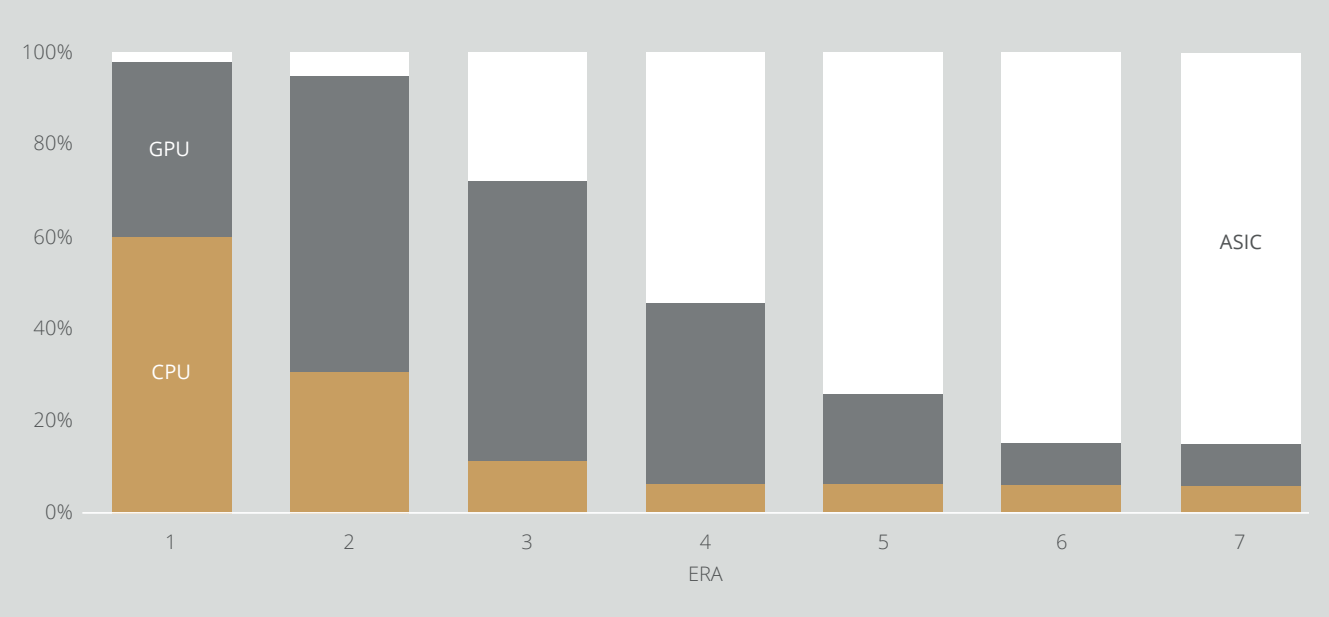
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Bu, bellek limitli bir görevdir. Bu durum, çözüm süresinin ham işlemci veya GPU hızından ziyade bellek bant genişliği ile sınırlandırılması anlamına gelir. Sonuç olarak, Cuckoo Cycle algoritmaları daha az ısı üretir ve geleneksel PoW algoritmalarından çok daha az enerji harcar. ASIC dostu CuckATOo31+, yüzlerce MB SRAM kullanmasına rağmen darboğaz oluşturan GPU'lara göre önemli bir verimlilik artışı sağlar. Sonuçta, ASIC'ler üç madencilik seçeneğinin en büyük potansiyel ölçekli ekonomisini sunmaktadır. Ancak piyasadaki kapsayıcılığın durumuna göre, erken dönemlerde CPU'lara ve GPU'lara göre madencilik ödüllerinin küçük bir kısmını kapsamalarına rağmen, CuckATOo31+ ile madencilik ekonomisinde rekabet adına oldukça önemli bir yerde olacaktır.

Tablo 2: Madencilik ödül payları. İleride değişebilir. Ödül dağıtımları, maksimum derecede merkeziyetsizliğin sağlanması ve ağın uzun vadeli çıkarlarına uygun olarak yönlendirilecektir.

Dönem	1	2	3	4	5	6	7
Gün	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Şekil 5: Tablo 2'ye göre her dönem için madencilik ödül payları. İleride değişebilir.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Madencilik Katkıları

Epic blokzincirinde madencilik Epic Genesis (2019) 'da başlayıp, Epic Singularity'de (2028) son bulacaktır. Ayrıca madencilik katkısı olarak EPIC Blockchain Vakfı'na yönlendirilen bir Epic dağılımı bulunmaktadır.

EPIC Blockchain Vakfı, Epic Cash projesinin kuruluşunun ilk yıllarında, pazarlama faaliyetleri yaratarak ve finansal teknoloji endüstrisinde ortaklıklar geliştirerek farkındalık ve toplumsal fayda sağlamayı amaçlamaktadır.

Tekilleşmenin ardından, EPIC Vakfı'nın rolü, devir teslimden önce vakıf tarafından geliştirilecek olan EPIC Dağıtık Özerk Şirketi (EDAC) tarafından üstlenilecektir. EPIC Blockchain Foundation, blok ödüllerinden düşülen madencilik ödüllerinin yüzdesi ile aşağıdaki yıllık oranları takip ederek finanse edilecektir:

Tablo 3: Madencilik ödüllerinin yüzdessel olarak vakfa olan katkı payının yıllık oranları.

Yıl	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Madencilik Ödülü Yüzde Oranı	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Sonuç

Epic, Bitcoin'in merkeziyetsiz dünyanın dijital altını olarak kabul edildiği pozisyonda "merkeziyetsiz dijital gümüş" olarak tanınmayı hedeflemektedir. Epic Cash, az enerji tüketimi ile enerji kaybını azaltan ve enerji tasarrufu sağlayan ekolojik olarak uyumlu donanım desteği ile tekrar kullanılabilirliği sağlayarak yeni merkezileşme eğilimlerinin aksine, güç dengesini bireysel kullanıcıların lehine olacak şekilde değiştirmektedir.

Bitcoin ekonomisinin kombinasyonu, kanıtlanmış bir çalışma ispatı (Proof of Work) formülünü, çağdaş blokzinciri teknolojisinin en iyisi ile birleştirmesi, ölçeklenebilir olması, kullanıcılarının gizliliğini koruyan, güvenilir, değişmez ve merkezi olmayan bir para birimi olmasıdır.

Epic Cash blokzinciri açık kaynak, halka açık, sınırlandırılamayan ve sansüre dayanıklı bir yapıdadır. Kullanıcılarının gizliliğini ve varlıklarını korur; diğer yandan donanımlarını ağ desteği için madencilik yoluyla kullananları ödüllendirir. Her Epic bloğu madencilikle kazılarak oluşur. Epic arzı sıfırdan başlayacak ve şu anda çalışmakta olan fonksiyonel bir test ağıyla ağın piyasaya sürüldüğü kabul edilmektedir.

Epic Cash Önemli Bilgiler:

- **Madencilik Ağustos 2019'da başlıyor.**
- **Epic Cash blokzinciri MimbleWimble temellerine dayanmaktadır.**

  Protokolün özelliklerini tanımlamayacak olursak:

  1. **Cut-Through** – alan verimliliğini artırmak, ağ onaylama işlemine geniş çaplı katılımın teşvik edilmesi ve yönetimin merkeziyetsizliğinin sağlanması için gereksiz bilgilerin blokzincirinden kaldırılması;
  2. ***CoinJoin*** – Epic'in güvenilirliğini sağlamak için bir blok içindeki işlemlerin bir araya getirilmesi;
  3. ***Dandelion++ Protocol*** – iç içe geçmiş kanallar arasında iletişim kurarak ve geniş bir düğüm ağı arasında yayılarak işlemler arasında bağlantı kurarak işlemlerin yayılması;
  4. **Cüzdan Adreslerinin Kaldırılması** – tişlem yapan taraflar için tek kullanımlık özel anahtarlar üretmek için çoklu imza teknolojisinin kullanılması ve cüzdan adreslerine duyulan ihtiyacı tamamen ortadan kaldırması.

- Epic Cash para politikası, Epic'in dolaşımdaki arzını Bitcoin'in dolaşımdaki arzı ile yaklaşık 9 yıl içinde senkronize etmek ve 2140 yılında Bitcoin ile aynı anda 21 milyon adetle aynı maksimum arza ulaşmak için tasarlanmıştır. Bu azalan arzın getirdiği enflasyonist politika, şeffaflığı, arzın öngörülebilirliğini ve adetin sabitliğini garanti eder ve uzun vadeli değer depolanmasının güvenliğini arttırır.

- Madencilik, kitle benimsemeyi ve ağ etkinliğini kolaylaştırmak için karşılık gelen RandomX, ProgPow ve CuckATOO31 algoritmaları aracılığıyla CPU'ları, GPU'ları ve ASIC'leri içerir.

IX. Teknik Özellikler

Proje Adı: Epic Cash
Para Birimi Adı: Epic
Blok Süresi: 60 seconds
Blokların Boyutu: 1 MB
Başlangıç Miktarı: 0
Nihai Miktar: 21,000,000
Başlangıç Bloğu: August 2019
Konsensüs RandomX (CPUs), ProgPow (GPUs) and CuckATOO31+ (ASICs)

Linkler:

www.epic.tech

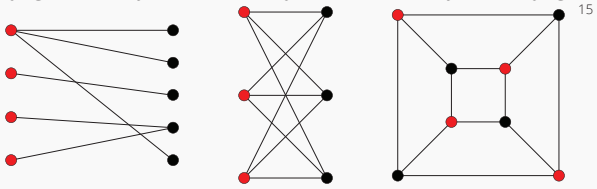
t.me/EpicCash – Telegram

t.me/EpicCashTurkish

X. Sözlük

ASIC - uygulamaya özel tümleşik devrelerden oluşan tekil bir amaç için tasarlanmış çiplerin genel adı.

İki Bölmeli Diyagram - iki küme halinde ayrıştırılmış bir diyagramın köşeler kümesi, aynı kümedeki hiçbir iki diyagram köşesi ile bitişik değildir.



Körleştirme Faktörü - işlemdeki şifrelemeyi kolaylaştırmak için dijital bir iletiye eklenen rastgele bir işlem; diğer ifadeyle söz konusu işlemdeki girdi ve çıktıları şifreleyen, işlem yapan tarafların ortak ve özel anahtarlarının olduğu yapı.

Blok Ödülü - epic blokzincirinde yeni işlemler içindeki işlemlerin doğrulanması amacıyla yapılan hesaplamalar için verilen ödül.

Önbellek - verilerin depolandığı donanım veya yazılım bileşenlerinin genel adı. Bu sayede veriler hakkındaki talepler daha hızlı bir şekilde yerine getirilebilmektedir.

Dolaşım Miktarı - belirli bir zamanda var olan Epic coin miktarıdır.

CPU - verilen komutların çoğunu bilgisayarın diğer donanım ve yazılımı ile yürütmekten sorumlu bilgisayar bileşeni.

Cut-Through - blokzincirindeki girişlerin ve çıkışların eşleştirilmesinin blok içindeki alanın artırılması için kaldırıldığı ve blokzincirinde depolanması gereken veri miktarını azaltan bir MimbleWimble uygulaması.

Merkeziyetsizlik - bir ağın operasyonlarının ve yönetiminin merkezi olmaması, dağıtık şekilde yürütülmesi.

Emisyon - madenciler tarafından blok ödülü olarak kazanılan yeni Epic'in yaratılmasına verilen ad. Epic'te blok süresi 60 saniyedir ve işlemler blokzincirinde onaylanır.

Epic Tekilleşmesi - epic'in dolaşımdaki miktarının Bitcoin'in dolaşımdaki miktarıyla senkronize edildiği nokta. (Mayıs 2028)

Fazlalık (MimbleWimble) - girdiler ve çıktılar arasındaki farklar ve artı olarak kimlik doğrulama, enflasyonu önlemek adına kullanılan imzalar.

Takas Edilebilirlik - kişisel varlıkların temelde birbirinin yerine geçebildiği ve parçalarının her birinin başka bir parçadan ayırt edilemez olduğu bir malın veya mülkiyetin özelliği.

Başlangıç (Etkinlik) - ilk Epic bloğunun madenciliği ve blokzincirinin resmi olarak başlangıcı

GPU - görüntüleme işlevleri konusunda uzmanlaşmış, programlanabilir bir mantıksal işlemci içeren birim. Tüketici GPU'ları, kripto para madenciliği için oldukça uygun yapıdadır.

Yarılanma (Bitcoin için) - 4 yılda bir gerçekleşmektedir. Her yarılanmanın ardından arz oranı % 50 azalmaktadır.

Hash - karma işlevi kullanan bir temel giriş numarasından hesaplanan değer.

Hashing Algoritması (işlev) - isteğe bağlı boyuttaki verileri dijital imzalar, ileti doğrulama kodları (MAC'ler) ve diğer doğrulama biçimlerini oluşturmak ve doğrulamak için kullanılan sabit boyutlu bir karma değere eşleyen matematiksel algoritma.

Homomorfik Şifreleme Belirsizliği - programlamada kullanılan şifrelenmiş bilgiler üzerinde şifresini çözmeden hesaplamalar yapmak için bir nesnenin yaratılmasından sonra değiştirilemeyen durum.

Girdi (MimbleWimble) - işlemin gönderen tarafını temsil eden bir MimbleWimble işleminin bileşeni; önceki işlemlerin çıktılarından elde edilmektedir.

I/O - girdi-çıktı. Bilgisayar gibi bir bilgi işlem sistemi ile dış dünya arasındaki iletişim. Bir insan ya da başka bir bilgisayar sistemi olabilir.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Toplam Miktar - dolaşımdaki miktarın artmayacağı Epic miktarı (21.000.000 Epic).

Memory-Hard - paralel olarak eşzamanlı gerçekleştirilen bağlantıları engellemek için çok fazla RAM kullanılması durumu. Memory-hard fonksiyonları, hesaplama zamanları olan ve öncelikle veriyi tutmak için mevcut hafıza tarafından karar verilen algoritmalardır. Limitli bellek işlevleri olarak da bilinir.

Merkle Ağacı - bilgisayar bilimlerinde kullanılan bir veri yapısı. Merkle ağaçları, blokzincirinde büyük veri yapılarında bulunan içeriğin etkin ve güvenli bir şekilde doğrulanmasını sağlamaktadır.

MimbleWimble - Bitcoin geliştiricilerin chat odasında isimsiz bir katılımcının ortaya çıkardığı bir protokol.

Çoklu imza - bir grup kullanıcının işlemler için tek bir belgeyi imzalamasını sağlayan dijital imza şeması. Genellikle, çok oturumlu bir algoritma, tüm kullanıcılardan gelen farklı imza koleksiyonundan daha küçük olan ortak bir imza oluşturulur.

Düğüm - bir blokzinciri ağına bağlanan, işlemler ve bloklarla ilgili bilgileri eşler arası bir şekilde dağıtmak için ağ içindeki diğer düğümlere yayılan bilgisayarların genel adı.

Tek yönlü toplu imza (OWAS) - bir şekilde şifrelenmiş birçok imzadan oluşan bir işlem imzasına verilen ad. Böylece toplamın bir parçası olan bireysel imzaları hesaplamak ve takip etmek zorlaşır.

Çıktı (MimbleWimble) - işlemin alındığını gösteren bir MimbleWimble bileşeni; sonraki işlemler için girdi olarak kullanılır.

Pedersen Onay Şeması - bir kanıtlayıcının, herhangi bir bilgiyi açığa çıkarmadan seçilen bir değere onay vermesini sağlayan bir şifreleme yöntemi.

Özel Anahtar - özel anahtarlar, metin şifreleme ve şifre çözme algoritmalarını başlatmak için bir genel anahtarla eşleştirilmiş küçük bir kod parçasıdır. Asimetrik şifreleme sırasında açık anahtar şifrelemesinin bir parçası olarak oluşturulur ve bir mesajın şifresini çözmek ve okunabilir bir formata dönüştürmek için kullanılır.

Çalışma İspatı (PoW) - üretilmesi maliyetli ve zaman alıcı olan; ancak başkaları tarafından doğrulaması kolay olan ve belirli gereksinimleri karşılayan bir veri parçası. Çalışma ispatları çoğunlukla kripto para madenciliğinde blok oluşturma işleminde kullanılan bir algoritmadır.

Genel Anahtar - açık anahtarlı şifreleme, şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğeri açık anahtardır.

RAM - işletim sistemi, uygulama programları ve mevcut kullanımdaki verilerin tutulduğu bir bilgisayarda, veri depolama yongalarına cihazın işlemcisi tarafından hızlıca erişilebilmelerini sağlayan bilgisayar bileşeni..

Rangeproof - bir işlem girişlerinin, toplamının işlem çıkışlarının toplamından daha büyük olduğunu ve tüm işlem değerlerinin pozitif olduğunu doğrulayan bir onay mekanizması.

(Dijital) İmza - temel olarak işlemlerin ve işlemlerin gerçekleştiği bloklarının güvenliğinin sağlanması, bilgilerin aktarılması, sözleşme yönetimi ve herhangi bir dış müdahalenin tespit edilmesi, önlenmesinin önemli olduğu diğer durumlar için kullanılan bir blokzinciri protokolünün standart bir parçasıdır. Bilginin blokzincirinde saklanması ve aktarılması için üç avantaj sağlar:

- Gönderilen verinin değiştirilmiş olup olmadığını açıklar;
- Belirli bir tarafın işleme katılımını doğrular;
- Yasal olarak bağlayıcı olabilir.

SRAM - güç sağlandığı sürece verileri belleğinde tutan Rastgele Erişim Belleği'ne (RAM) verilen isim.

Verimlilik - bir kripto para birimi protokolü tarafından gerçekleştirilebilen saniye başına işlem miktarı.

Güvenilirlik - merkeziyetsiz bir şekilde sürdürülen bir protokolün kurallarına uyması için oluşturulan şifreleme ağının kalitesi.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH