5.0 Zcash ve Bitcoin'e Giriş

Satoshi Nakamoto'nun Gizemi: Bitcoin ve Gizlilik Devrimi

Satoshi Nakamoto, gizemli ve parlak bir yenilikçi olarak, finansal işlemlerin sınır tanımadığı, şeffaf ve güvenli bir geleceği hayal etti—hükümetlerin ve bankaların kontrolünden uzak. 2008 yılında Satoshi, Bitcoin beyaz kitabıyla bir Özgürlük Devrimi'ni ateşledi. Bu belge, blockchain teknolojisinin ilk pratik uygulamasını tanımlıyordu. Bitcoin, finansal krizlerin etkisi altında ve merkezi kuruluşlara olan güvenin erozyona uğradığı bir dünyada umut ve dayanıklılık sembolü olarak ortaya çıktı. İlk Bitcoin işlemi Ocak 2009'da gerçekleşti.

Merkeziyetsiz bir finansal sistem kurma arzusuyla hareket eden Satoshi'nin Bitcoin'i, gücü insanlara geri verdi ve mevcut durumu sorgulayan, finansal özgürlüğü savunan küresel bir hareketi ateşledi.

5.1. Zcash ve Bitcoin'e Giriş

Yedi yıl sonra, 2016'da, bir grup bilim insanı ve araştırmacı Zcash'i piyasaya sürdü. Amaçları, Satoshi'nin Bitcoin'inin devrim niteliğindeki gücünü geliştirmekti; özellikle gizlilik özellikleri ekleyerek. (Buna daha sonra değineceğiz.)

Zcash, aslında Bitcoin'in bir çatalıdır; yani Bitcoin'in kodu esasen kopyalanmış ve değiştirilmiştir. Zcash fikri, 2014 yılında MIT, Johns Hopkins Üniversitesi, Technion ve Tel Aviv Üniversitesi'nden profesörler ve akademik araştırmacılar tarafından yayımlanan bir beyaz kitapta ilk kez tanımlanmıştır ve Zooko Wilcox-O'Hearn ile Electric Coin Co. (ECC; daha önce Zcash Şirketi olarak adlandırılıyordu) ekibi tarafından birkaç yıl boyunca geliştirilmiştir.

İnsanlar, ZEC'i düşük ücretlerle verimli ve güvenli bir şekilde işlem yapmak için kullanır. Zcash gizlidir, hızlıdır, esnektir ve herkesin erişimine açıktır; dijital çağ için tasarlanmıştır. Bagel'den plaj tatillerine kadar neredeyse her şeyi satın almak için kullanabilirsiniz.

Mobil telefonunuzu kullanarak bir arkadaşınıza Zcash ile özel bir ödeme yapabilir, yurt dışına para gönderebilir, market alışverişi yapabilir veya değerli bir amaca bağışta bulunabilirsiniz. Lowe's, Nordstrom, Baskin Robbins ve daha birçok yerde Zcash ile ödeme yapmak için Flexa SPEDN gibi üçüncü taraf uygulamaları kullanabilirsiniz. Moon gibi hizmetler, Zcash'i çevrimiçi olarak Visa'nın kabul edildiği her yerde kullanmanıza olanak tanır.

5.1.1 Bitcoin Nedir? Zcash Nedir?

Bitcoin (BTC), Bitcoin ağında herkes tarafından gönderilip alınabilen bir elektronik nakit biçimidir. Bitcoin, dijital cüzdanlarda, mobil telefonlarda veya masaüstü bilgisayarlarda

saklanabilir ve bu cüzdanlar, dağıtık bir defter sistemine erişim sağlar. Bunu, herkesin erişebildiği dev bir çevrimiçi elektronik tablo olarak düşünün; burada tüm işlemler kaydedilir.

Bitcoin gibi Zcash de, açık kaynaklı ve blockchain tabanlı bir deftere dayanan dijital bir para birimidir, ancak Bitcoin'den farklı olarak Zcash, defteri dolandırıcılığa karşı koruyan ve kullanıcıların işlem bilgilerini gizli tutmalarına olanak tanıyan sofistike bir sıfır bilgi ispatı sistemi sunar.

5.1.2 Bitcoin ve Zcash Arasındaki Fark Nedir?

Zcash'i tanımlamanın en basit yolu, onun Bitcoin gibi bir dijital para birimi olması, ancak kullanıcıların gizliliğini korumasıdır; bu sayede finansal geçmişleri açığa çıkmaz.

Bitcoin 2009 yılında piyasaya sürüldüğünde, bu, ilk merkeziyetsiz kripto para birimi oldu. Tüm Bitcoin işlemleri, herkesin erişebileceği bir kamu blockchain üzerinde doğrulanır ve kaydedilir. Bu, dünyanın herhangi bir yerindeki herkesin kullanıcı bakiyelerini ve işlem verilerini görebileceği anlamına gelir. Gizlilik eksikliği, Zcash bilim insanlarını daha iyi bir şey geliştirmeye teşvik etti ve 2016 yılında bu kriptografi uzmanları, Bitcoin'in açık kaynak kodunu alarak sıfır bilgi ispatları (ve diğer iyileştirmeler) ekleyerek Zcash'i oluşturdu. Zcash, kullanıcıların finansal bilgilerini korumak için tam şifreleme ile birlikte Bitcoin'in tüm avantajlarını sunar.

Ayrıca, Zcash geliştirmeleri için kendine yeterli bir finansman mekanizması, daha kısa onay süreleri, özel bir not alanı, daha hızlı işlemler gibi diğer önemli farklılıklar da bulunmaktadır.

5.1.3 Neden Zcash hakkında bilgi edinmelisiniz?

Zcash, insanlara dijital nakit ve diğer verileri özel bir şekilde, izin gerektirmeden, banka veya hükümet gibi bir aracı olmaksızın transfer etme fırsatı sunar. Özel, eşler arası ve izin gerektirmeyen bir para sistemi, insanlara paralarını saklama ve başkalarıyla işlem yapma yeteneği verir; bu, genellikle kontrol ve ücretler uygulayan merkezi otoritelerden bağımsızdır. Zcash, insanların finansal bilgileri hakkında başkalarına ne zaman ve ne şekilde bilgi vereceklerini seçme özgürlüğünü tanır.

Zcash, Bitcoin'in en büyük kusurunu çözmektedir: veri sahipliğinin ve transferinin gizliliği. Blockchain uygulamaları ve kripto paraların daha geniş bir şekilde kabul gördüğü bir dünyada, Bitcoin'deki gibi takma adla yapılan işlemler, kullanıcı gizliliğini korumak için artık geçerli bir seçenek değildir. Gözetim uygulamaları her geçen gün daha sofistike hale gelmekte ve insanlar ile kurumlar tarafından blockchain işlemlerini analiz etmek ve takip etmek için yaygın bir şekilde kullanılmaktadır.

5.1.4 Zcash'e Değerini Ne Verir?

İnsanlar, ZEC'i sert, gizliliği koruyan bir varlık olarak servetlerini saklamak için kullanabilirler. Toplamda yalnızca 21 milyon ZEC birimi olacak, bu da varlığın sabit bir arzı olduğu anlamına geliyor. 21 milyonuncu ZEC madenciliği yapılıp dolaşıma girdiğinde, varlık enflasyona karşı

dayanıklı hale gelecektir. Enflasyona karşı dayanıklı varlıklar, merkezi otoritelerin ulusal para arzlarını artırdığı durumlarda enflasyona karşı iyi bir korunma sağlar.

Zcash, 2016'nın sonlarında orijinal ağ lansmanından bu yana uzun bir yol kat etti ve blockchain ile kripto kullanıcılarına gizlilikleri üzerinde kontrol sağlamaya devam ediyor. Zk-SNARK kriptografik kanıtları, küresel pazardaki blockchain tabanlı kullanım durumları için gizlilik standardını belirlemeye yardımcı oldu. Geniş bir kullanıcı ve kurumsal müşteri yelpazesi, Zcash protokolünün sağladığı gizlilik, esneklik ve performans türünü talep etmektedir.

5.1.5 Neden önemsemeliyim?

Zcash, insanlara sansür uygulayabilen ve/veya insanları sömürebilen merkezi sistemlerin dışında işlem yapma seçeneği sunar ve finansal bilgilerini başkalarıyla paylaşma veya bu bilgileri özel tutma imkanı tanır.

Bu sansür direncine sahip dijital ödeme mekanizması, ifade özgürlüğünü ve dernek kurma özgürlüğünü korur; aynı zamanda insan olma, eğlenceli olma veya istedikleri gibi olma özgürlüğünü sağlar! Zcash kullanıcıları, kimliklerini açığa çıkarmadan ve karşılaşabilecekleri olumsuz sonuçlardan korkmadan, kuruluşlara bağış yapabilir, yurt dışına para gönderebilir veya sadece bir arkadaşa para yollayabilir.

Ve Zcash'in tıpkı Bitcoin gibi 21 milyonluk sabit bir arzı olduğu için, kullanıcılar ZEC'lerinin merkezi bir taraf tarafından keyfi olarak daha fazla basılarak değersizleştirilmeyeceğinden emin olabilirler.

5.2 Zcash Nelerden Oluşur?

Zcash, kullanıcılara iki işlem türü sunar: şeffaf (herkesin görebileceği) ve korumalı (özel). Her ikisi de aynı Zcash blockchain'inde gerçekleştirilir, ancak işlemlerin miktarları ve kanıtları farklı şekillerde işlenir. Korumalı işlemleri özel tutmak için Zcash, "sıfır bilgi kanıtları" olarak bilinen bir yöntemi kullanır.

Özellikle, Zcash zk-SNARK'ları kullanır, bu da bir tür sıfır bilgi kanıtıdır. zk-SNARK kısaltması, "Sıfır Bilgi Kısa Etkileşimsiz Bilgi Argümanı"nı ifade eder ve belirli bir bilginin, örneğin bir gizli anahtarın, sahipliğini kanıtlamak için kullanılan bir kanıt yapısını ifade eder; bunu yaparken bu bilgiyi ifşa etmeden ve kanıtlayıcı ile doğrulayıcı arasında herhangi bir etkileşim olmadan gerçekleştirir.

Daha basit bir ifadeyle, sıfır bilgi kanıtı, bir şeyin doğru olduğunu kanıtlayabilen bir kriptografik yöntemdir; bunu yaparken o şeyi doğru kılan bilgiyi ifşa etmez. Örneğin, Zcash'te iki taraf arasında bir işlem yapıldığında, sıfır bilgi kanıtı, göndericinin toplam gönderilen miktarı karşılayacak kadar parası olduğunu doğrulamak için kullanılır; ancak bu işlem sırasında alıcıya, blockchain'e veya başka birine göndericinin cüzdan bakiyesini ifşa etmez.

Bir an için gözlerinizi kapattığınızı ve arkanızda iki dama taşını tuttuğunuzu hayal edin. Bu taşların ikisinin de aynı renkte mi yoksa farklı renkte mi olduğunu bilmiyorsunuz. Birini uzatıp

karşı tarafınıza gösteriyorsunuz; o gözleri açık olan kişi size rengini söylüyor, ancak onun yalan söyleyip söylemediğini bilmiyorsunuz. Sonra taşı tekrar arkanızda tutarak ya değiştirmiş oluyorsunuz ya da değiştirmeden işlemi tekrarlıyorsunuz. Bu işlemi birçok kez yaparak, diğer kişinin yalan söyleyip söylemediğine dair güven kazanmaya başlayabilirsiniz. Örneğin, aynı taşı iki kez çıkardığınızda, ilkinde “siyah”, ikinciinde “kırmızı” dediğinde onun yalan söylediğini bilirsiniz. Eğer verdiği yanıtlar, hangi parçayı gösterdiğinize dair bilginizle tutarlılık gösteriyorsa, diğer kişinin dürüst bilgi verip vermediğine dair oldukça emin olabilirsiniz.

Bu tür bir süreç, belirsiz karmaşıklıkta muazzam miktarda bilgiyi korumak için kullanılabilir (örneğin, bir blockchain’in küresel durumunun Merkle kökünü saklamak için tekrarlayıcı SNARK'ların kullanımı; ancak bu kitabın kapsamının dışındadır).

5.2.1 Yeni Zcash coinler ağa nasıl girer?

Zcash'ın para tabanı, 21 milyon ZEC para birimi ile sabit bir arzdan oluşur. Her 75 saniyede bir, Zcash blockchain'ine yeni bir blok eklenir ve bu blok ödülü olarak 3.125 ZEC dolaşıma girer. Bu blok ödülü, madencilere ve Zcash geliştirme fonuna dağıtılır.

Blok ödülünün miktarı, her yaklaşık dört yılda bir yarıya düşer ve tüm 21 milyon ZEC dolaşıma girene kadar bu devam eder. Zcash enflasyonu, neredeyse tam olarak Bitcoin'in enflasyonunu taklit eder. Önemli bir nokta, yeni madeni paralar oluşturulduğunda enflasyonun azalmasıdır ve her yarılanmada bu oran önemli ölçüde düşer.

5.2.2 Zcash Gizliliğine Giriş

Korumalı Zcash adresleri, finansal bilgilerinizi gizli tutar. Şeffaf adresler ise bu bilgileri kamuya açık hale getirir.

Çoğu blockchain, tüm işlem ve bakiye bilgilerini herkese açık bir şekilde sergiler. Bu, utanç verici bir sır değil; bu, onların tasarım şeklidir. Korumalı Zcash ile saklamak ve işlem yapmak, kullanıcılara varlıkları üzerinde daha fazla kontrol sağlar ve dolandırıcılara ve diğer kötü niyetli aktörlerden korunmalarını sağlayabilir.

Zcash’i dijital cüzdanınızdan gönderdiğinizde, adresinizin uzun bir sayı ve harf dizisi olduğunu göreceksiniz. Alıcınızın da uzun bir sayı ve harf dizisi içeren bir adresi olacaktır. Adresiniz “z” ile başlıyorsa ve alıcı adresi de “z” ile başlıyorsa, işlem bilgilerinin tamamen gizli olduğundan emin olabilirsiniz. Değişim tutarı ve her cüzdanın adresleri, kamu blockchain’inde korunmaktadır. Gizlilik gerektiğinde ZEC göndermek ve almak için genellikle en iyi yol budur.

Eğer “t” ile başlayan bir adresten gönderim yapıyor veya “t” ile başlayan bir adrese alım yapıyorsanız, gizlilik seviyesi her zaman yüksek değildir; çünkü bazı bilgiler blockchain’de görünür olacaktır. T-t işlemleri, Bitcoin işlemleri gibi tamamen kamuya açıktır.

Zcash kullanıcıları ayrıca “u” ile başlayan cüzdan adresleriyle de karşılaşacaklardır. Bunlar birleşik adresler olarak adlandırılır ve evrensel bir seyahat adaptörü gibi çalışır. Birleşik

adreslerle, cüzdanlar otomatik olarak paraları en son korumalı havuza taşıyabilir. Örneğin, bir kullanıcı bir borsa üzerinden bazı Zcash satın alırsa, o borsa “t” adresinden sizin birleşik adresinize şeffaf Zcash gönderebilir. Ancak eğer cüzdanınız otomatik koruma (autoshielding) destekliyorsa, bu fonları otomatik olarak özel depolama alanına taşıyacaktır.

Zcash Adres Türleri

Şu anda kullanımda olan üç ana adres türü bulunmaktadır. Bunlar şunlardır ;

MAKSIMUM GIZLILIK IÇIN HER ZAMAN Z- VEYA U-ADRESLERINI KULLANIN.

5.2.3 Blockchain, Zcash Harcamalarını Nasıl Takip Eder?

Bir hash ağacı veya Merkle ağacı, dallardan ve veri bloğunun kriptografik hash'i ile etiketlenmiş yaprak düğümlerden oluşur. Merkle ağaçları, kriptografik taahhüt şemalarının bir örneğidir. Ağaç kökü, bir taahhüt olarak görülür ve yaprak düğümleri, orijinal taahhütün bir parçası olduğunu kanıtlar.

Merkle ağaçları, P2P (eşler arası) ağlarda depolanan veya iletilen verileri doğrulamak için kullanılır; bu, kullanıcıların diğerlerinden aldıkları verilerin değiştirilmediğinden emin olmalarını sağlar.

Zcash'in Sapling ve Orchard korumalı havuzlarında, Not Taahhüt Ağacı kullanılarak işlemlerin geçerliliği, uzlaşma ile doğrulanırken, gönderen, alıcı ve harcanan miktarların tamamen gizli tutulmasını sağlar.

5.2.4 Zcash İşlemleri Güvenli Mi?

Evet. Zcash protokolü, dünyadaki en kapsamlı belgelenmiş sıfır bilgi ödeme protokollerinden biri olarak oldukça güvenli kabul edilebilir. Namada ve Penumbra gibi birçok diğer büyük kripto projeleri tarafından yeniden oluşturulmuştur. Ayrıca, Zcash kullanıcıları tarafından kullanılan ürünlerdeki cüzdanlar ve kriptografik bileşenler için birçok güvenlik denetimi gerçekleştirilmiştir.

5.2.5 Gerçek bir Zcash işlemi boyunca bana yol gösterin

- Cüzdanınızın en son blok yüksekliğiyle senkronize olduğunu onaylayın.
- Tamamen senkronize olduğunda, bakiyenizin güncel ve harcanabilir miktarın tam olduğunu bilirsiniz.
- Alıcının birleşik adresini "adres" alanına girin. Adresi panodan yapıştırabilir veya karşı tarafın QR kodunu tarayabilirsiniz.
- Göndermek istediğiniz miktarı doldurun; ücretler otomatik olarak hesaplanır.
- İşleminizle birlikte bir gizli not girin. Unutmayın: Şeffaf adresler not alamaz.
- İşlem detaylarını onaylayın ve ardından "gönder" butonuna tıklayın.

Zcash blok süresi 75 saniyedir, alıcının gelen fonlardan haberdar olması 1-2 dakika sürebilir. Alıcının cüzdanının gerektirdiği onay sayısına bağlı olarak, Zcash'i harcayabilmesi için biraz beklemesi gerekebilir.

5.2.6 Zcash işlemlerini iş başında uygulayın

Zcash'i bir arkadaşınızla değiştirmeyi denemek için şu adımları izleyin:

1. Her ikiniz de bir Zcash cüzdanı oluşturun.
2. "Gönder" seçeneğinde, arkadaşınızın adresinin QR kodunu tarayın veya U ya da Z adresini girin.
3. "Merhaba, Zcash'e hoş geldiniz!" yazılı bir not gönderin.

5.2.7 Zcash kapatılabilir mi?

Hayır. Zcash, dünya genelindeki bireyler tarafından yürütülen izin gerektirmeyen merkeziyetsiz bir internet ödeme protokolüdür. Düğüm yazılımı ücretsiz ve açık kaynaklıdır. Zcash işlemlerinin doğrulanmasında herhangi bir merkezi otorite yer almamaktadır. Aslında, Zcash'in geliştirilmiş gizliliği nedeniyle, ağı kapatma girişimlerine karşı daha dirençlidir

5.3
Zcash dünyasında kim kimdir ve neler vardır?

Zcash üzerinde çalışan birçok ekip ve bağımsız geliştirici bulunuyor, ancak burada birkaç önemli oyuncu var.

Electric Coin Co. (ECC), Zcash dijital para birimini 2016 yılında oluşturmuş ve piyasaya sürmüştür. Bugün, ECC, diğer bağımsız ekipler ve geliştiricilerle birlikte, ürün geliştirme, farkındalık ve benimseme ile çeşitli araştırma türleri aracılığıyla Zcash topluluğunu desteklemeye devam etmektedir. ECC, dünya çapında en güçlü kriptografi ekiplerinden biri olarak geniş çapta bilinmektedir. 2016 yılında, sıfır bilgi kriptografisini gerçek dünya uygulaması olan Zcash'te başarıyla ilk kez uygulayan ekip oldu ve 2022'de ECC mühendisleri, Halo'yu keşfetti. Halo, gerçekten güvenilir olmayan blockchain şifrelemesi ve geliştirilmiş ölçeklenebilirlik sunan, yeni ve yinelemeli bir sıfır bilgi kanıtlama mekanizmasıdır. Halo'yu kendi sürümlerinde uygulamak için çalışan çeşitli bağımsız projelerde birçok ekip bulunmaktadır.

Zcash Vakfı (ZF), 501(c)(3) kamu yararına bir hayır kurumu olup, öncelikle Zcash protokolü ve blockchain kullanıcılarına hizmet ederek, kamu yararına finansal gizlilik altyapısı inşa etmektedir. ZF, diğerleriyle birlikte Zcash protokolünün ve onun güç sağladığı açık ağın merkeziyetsiz ve çeşitli kalmasını sağlamak için çalışmaktadır. ZF'nin ekosisteme yaptığı bazı dikkat çekici teknik katkılar arasında, modern, bağımsız bir Zcash düğümü olan Zebra'nın geliştirilmesi ve bir eşik imza şeması olan FROST bulunmaktadır.

Vakıf ayrıca, gizlilik teknolojisi ve Zcash ekosistemi etrafında düzenlenen yıllık Zcon konferansını düzenlemekte ve Zcon Vozes, A/V Kulübü gibi topluluk girişimlerini ve çeşitli açık topluluk çağrılarını ve SSS (AMA) etkinliklerini desteklemektedir. Ek olarak, Vakıf, Küçük Hibe programı, iç ve dış araştırma projeleri ve Zcash Topluluk Hibeleri (ZCG) için idari destek sağlayarak Zcash'in ilerlemesine katkıda bulunmaktadır.

Zcash Topluluk Hibeleri (ZCG), Zcash'in kullanılabilirliğini, güvenliğini, gizliliğini ve benimsenmesini artıran projeleri finanse etmektedir. ZCG, Zcash Vakfı'nın tüzüğüne göre oluşturulmuş bir teknoloji danışma kuruludur. Hibeler, Zcash Topluluk Danışma Paneli tarafından seçilen beş üyeden oluşan bir komite tarafından belirlenmektedir.

ZCG tarafından onaylanan son projeler şunlardır:

Zcash Shielded Varlıklar (ZSA), QEDIT ekibi tarafından yönetilmektedir ve Zcash'e DeFi getirerek yeni bir ödeme protokolü eklemektedir. Bu protokol, ana ağa ek özellikler kazandırmaktadır.

Zcash Medya, Edward Snowden, Zooko Wilcox ve Deirdre Connolly gibi dikkat çekici Zcash kullanıcılarını içeren kısa bir belgesel hazırlamıştır.

ZGo tarafından yürütülen, fiziksel mağazalar için kolay bir tıklama ile gerçekleştirilen korumalı ödeme ve satış noktası sistemi SDK'sı.

Küresel Elçi programı, Zcash'in uluslararası düzeyde daha geniş bir temsili kazanmasına yardımcı olur.

ZecHub, Zcash üzerine odaklanmış açık kaynaklı bir eğitim merkezi olup, özellikler, bültenler, bloglar, eğitimler, podcast'ler ve daha fazlasını yayınlayan küresel bir katkıcı topluluğuna sahiptir.