CLOAK

ENIGMA V2.1

Whitepaper (Revised)

February 2018

ENIGMA

A PRIVATE, SECURE AND UNTRACEABLE TRANSACTION SYSTEM FOR CLOAKCOIN

1. ÖZET

CloakCoin, Enigma ile özel, güvenli, takip edilemeyen ve merkezi olmayan transferleri kolaylaştırmak için tasarlanmış bir kripto para birimidir.

Cloak, PoW / PoS (Proof of Work, Proof of Stake) özelliklere sahip para birimidir. Şu anda Proof-of-Stake (faiz kazanımı) aşamasındadır.

Enigma, CloakCoin'in gelecekteki gelişiminin temelini oluşturan ve CloakCoin ağında çalışan merkeziyetsiz uygulamalar için temel işlem sistemini sağlayan özel, güvenli ve takip edilemeyen bir ödeme sistemidir.

Bugün gizlilik belki de her zamankinden daha önemli. Teknolojik ilerlemenin inanılmaz hızı, ufkumuzu hızla genişletmiş ve dünyayı daha önce hiç olmadığı şekilde birbirine bağlamıştır. Bitcoin'in 2009'daki tanıtımı sayesinde, kripto para birimi sürekli olarak yaygınlaşıyor ve bu nedenle blockchain gücünü kullanarak artık dijital parayı dünya genelinde güvenli bir şekilde anında aktarabiliyoruz.

Kripto para birimi kullanımının benimsenmesi daha yaygın hale geldikçe, artan düzenleme ihtiyacı kaçınılmazdır. Bu düzenlemeler yaygınlaştıkça içerikleri de herkesce görülecektir. Ancak, birçok kişi düzenlemelerin aşırı derecede caydırıcı olabileceğini ve asıl amacının kripto para birimlerinin özgürlükçü yanını baskı altına almak için tasarladığını düşünmektedir.

ENIGMA

Enigma, merkezi olmayan, bir ‘off-blockchain’ karıştırma algoritmasıdır. CloakCoin ağındaki kullanıcıların Cloak’ı özel ve güvenli bir şekilde birbirlerine iletmelerini sağlar.

Enigma, iletim sırasında kullanılan karıştırma işleminin üçüncü taraf gözlemciler için hem güvenli hem de izlenemez olmasını sağlamak için tasarlanmıştır. Bu durum, bir kullanıcının Cloak coinlerinin transfer sırasında güvende tutulmasını sağlar ve bu karıştırıcı işlem sayesinde gönderici ve alıcı eşlendirilemez ya da ilişkilendirilemez., Cloaking sırasında CloakCoin’ler hiçbir zaman herhangi bir aracı tarafa transfer edilmez, bu yüzden Cloak Coin’ler güvende kalmaya devam eder. Enigma sisteminin, Cloaking transferlerinin gerçekleşmesine destekte bulunan kullanıcıları ödüllendirmesini sağlama konusunda sıkı bir şekilde çalışmaktayız. Bu süreci geliştirmeye ve aktif olarak katıılan kullanıcıları daha fazla teşvik etmeye devam edeceğiz. Cloak Coin sahibi olan herkes, isterlerse, cüzdanlarında yer alan Cloak Coin’leri Staking/Cloaking modunda saklayarak Cloaking işlemlerine pasif olarak destekte bulunabilir. Kullanıcılar bu destek sonucunda ödül kazanmaktadır.

2. ENIGMA V1.0 GENEL BAKIŞ

Enigma, Cloak'ın; özel, güvenli ve takip edilemeyen ödeme sisteminin erişilebilir ilk iterasyonudur. Enigma işlemleri, yardımları karşılığında ödül alan diğer kullanıcılar tarafından gizlenir. Bu duruma verilen isim ise "cloaked"'tur . Diğer kullanıcılar, Enigma işlemine girdi ve çıktılar sağlayarak, cloak aktarımının gerçek kaynağını ve hedefini belirlemeyi imkânsız kılar. Ağdaki tüm Enigma mesajları, veri güvenliğini ve bütünlüğünü sağlamak için CloakShield'ı kullanan alıcı için hashlenmiş ve şifrelenmiştir. Daha fazla bilgi için Bölüm 3- "CloakShield" bölümüne bakınız.

2.1. ENIGMA SÜRECİ (ENIGMA AKTİF NODE'LAR İÇİN)

ENİGMA DUYURULARI

Enigma düğümleri (node'lar) Cloak ağı üzerinden iletişim kurar ve bir düğüm, diğer aktif Enigma düğümlerini takip eder. Enigma Duyuru Yayınları, halka açık oturum anahtarımızın ve mevcut Enigma gizleme bakiyesinin diğer Enigma düğümlerini uyarır.

ENIGMA CLOAKİNG İSTEKLERİ

Bir kullanıcı, Cloaked Enigma işlemi göndermek istediğinde, bir dizi Enigma düğümünü (yeterince yüksek bir Enigma bakiyesiyle) seçer ve gizleme konusunda yardım talep eder. Bir Enigma düğümü, cloaking için yardımcı olmayı ve bunu belirtmek için talep sahibine bir kabul cevabı göndermeyi seçebilir. Bir Enigma düğümü cloaking işlemine katılmayı reddederse veya zamanında yanıt vermezse, alternatif bir Enigma düğümü seçilir ve temasa geçilir.

DDoS (dağıtılmış hizmet reddi) koruması, oturumun geri kalanı için hatalı davranan düğümleri kara listeye alacaktır. Bir düğüm, bir Enigma işlemini imzalamayı sürekli reddediyorsa veya Enigma mesajlarını aktarmayı reddediyorsa, yanlış davranıyor olarak kabul edilir. Enigma cloaking - gizleme nodları bir cloaking nodu ve gönderici nodu arasında simetrik RSA-256 veri şifrelemesi için paylaşılan bir gizli anahtar oluşturmak için kullanılan Enigma başlatıcı nodu ile paylaşılan bir gizlilik türetmek için Elliptic Curve Diffie Hellman anahtar değişimi yöntemini (ECDH) kullanır.

ENIGMA CLOAKING KABULÜ

Bir Enigma nodu “cloaking” gizleme isteğini kabul ettiğinde, bu nod, Enigma işleminde kullanılmak üzere bir dizi islem girdilerinin ve çıktılarının bir listesini temin eder. Bir gizleme noduyla sağlanan girdi miktarları Enigma gönderim miktarına eşit veya daha büyük olmalıdır (artı ücretler). Çıktılar, Enigma işleminin gerçek çıktısı ile mümkün olduğu kadar eşleşecek şekilde dikkatlice seçilir. Enigma output adresi daha önce kullanılmamışsa, “Cloaker” tarafından yeni bir değişim adresi oluşturulur. Enigma output adresi daha önce kullanılıp bakiye aldıysa, benzer faaliyeti olan mevcut bir adres ‘Cloaker’ tarafından input fonlarını iade etmek ve Enigma ‘cloaking’ ödülünü almak için seçilir.

‘CLOAKED’ ENIGMA İŞLEMİ

Enigma Sender, Enigma Cloaker nodları tarafından sağlanan girdileri ve çıktıları kullanarak “gizlenmiş” bir işlem oluşturur. Daha sonra, Enigma Sender, “cloaking ” aşamasında gizlemeyi kolaylaştırmak adına tüm işlem girdilerini ve çıktılarını karıştırmadan önce, kendi girdi ve çıktıları işleme ekler. Sonrasında, “Cloaked” işlemi şifrelenir ve herbir katılımcı Cloaker’a (Cloakshield aracılığıyla) gönderilir.

Cloaker nodları, sağladıkları girdi ve çıktıların “gizlenmiş” işlemlerde mevcut olduğundan ve çıktılarının bir veya daha fazlasının da yeterli ücretlerle ödüllendirildiğinde emin olmak için işlemi kontrol eder.İşlem kontrolleri olumlu sonuçlanırsa, işlem (SIGHASH_ ALL+SIGHASH_ANYONECANPAY) şeklinde imzalanır, şifrelenir ve Enigma Sender’a geri gönderilir.

2.2.1. ENIGMA CLOAKING NODLARINI İZLEME

Cloak ağında etkinleştirilmiş Enigma nodları diğer nodlara duyurular yayınlar. Bu Enigma duyuruları, nodun ortak ek anahtar kimliğini (ec-key ID) ve Enigma cloaking operasyonları için mevcut olan kullanılabilir bakiyeyi içerir. Nodlar, ağ üzerindeki diğer aktif Enigma nodlarının bir listesini tutar, böylece cloaking için iletişim kurabilirler. Nod kimlikleri oturum bazında oluşturulur; İstemciyi yeniden başlatmak geçerli kimliği yenileyecektir.

1. Her bir cüzdan, başlangıçta oturum için bir genel / gizli (secp256k1) anahtar çifti oluşturur.

2. Cüzdan, Cloak ağında yer alan diğer nodlara Cloak bakiyesini ve public key'ini bildirir.

3. Nodlar diğer aktif Enigma Cloaking nodlarını takip eder ve onlarla doğrudan veya dolaylı olarak iletişim kurabilir (CloakShield Onion Routing üzerinden)

2.2.2. ENIGMA İŞLEMİNİ BAŞLATMA

ALICE, 5 dağıtıcı nod kullanarak BOB'a 10 CLOAK yollamak istiyor.

1. Alice, ağa halka açık Enigma oturum anahtarını ve göndermek istediği Cloak miktarını içeren bir Enigma talebi yayınlar. Alice'in bu isteği, kaynağı gizlemek için 5 Enigma seri noduyla güvenli bir şekilde yönlendirilir.

2. Catherine'de "Cloaking Modu" etkindir ve Alice ile güvenli iletişim için güvenli bir CloakShield şifreleme kanalı oluşturur. Catherine daha sonra bir Enigma yanıt paketi oluşturur ve Alice'e güvenli bir şekilde gönderir. Catherine'nin gönderdiği yanıt, Alice'in gerçekleştirdiği işlemi "Cloaked" yapmak için Catherine'nin gönderdiği girdi ve çıktıları içerir.

3. Alice, Catherine'in Enigma yanıtını çözer ve işler. Daha sonrasında Catherine'in girdileri ve çıktılarıyla karıştırılmış kendi girdileri ve çıktılarını kullanarak bir Enigma işlemi oluşturur. Bu şifrelenir ve imzalamak için Catherine'e gönderilir.

4. Catherine, Enigma işleminin şifresini çözer ve tedarik ettiği girdilerin ve çıktıların doğru bir şekilde kullanıldığından ve yeterince ödüllendirildiğinden emin olmak için işlem üzerinde bir dizi bütünlük kontrolü gerçekleştirir. Enigma işlemi testleri geçerse, Catherine imzalar, şifreler ve Alice'e iletir.

5. Alice bunu kendini imzalamadan önce imzalanan işlemdeki diğer denetimleri gerçekleştirir. İşlem daha sonra bir bloğa dahil edilmek üzere ağa sunulur. (Enigma düğümlerinden güvenli bir şekilde yönlendirilir)

6. İşlem tamamlandığında, Bob, Alice'den fonları alacak ve Catherine, Enigma işlemine yardımcı olduğu için bir "Cloaking" ödülü alacaktır.

7. Catherine'in Alice'in girdi ve çıktılarını ikizleyen (mirroring) girdi ve çıktıları nedeniyle, Enigma işleminin gerçek göndereni ve alıcısını belirlemek mümkün değildir.

ENIGMA TRANSACTION EXAMPLE

ALICE wants to send coins anonymously to BOB.

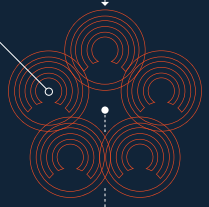
ALICE (–10.0992) CLOAK

(–10) CLOAK + (–0.0992) Enigma fee
= (–10.0992) CLOAK total

ENIGMA mixer nodes begin communicating.

CATHERINE

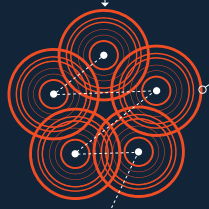
Every coin holder can announce themselves as a Mixer Node, also known as a "Cloaker".



Every participant remains anonymous and communicates through an encrypted channel.

ALICE's wallet is now connected to mixer nodes.

Each mixer node helps ALICE by shuffling around the transaction.



This network of nodes creates decentralized anonymization similar to TOR Onion Routing.

Mixer nodes get rewarded for Cloaking ALICE's transaction.

(+0.0992) CLOAK

A linear fee from .2% (>1000 coins) to 1% (0 coins) is shared amongst all participating Cloakers.

The system works seamlessly to ensure complete anonymity and total privacy.

BOB then receives ALICE's encrypted payment

BOB (+10) CLOAK

BOB successfully receives 10 CLOAK anonymously.

3. CLOAKSHIELD

CloakShield, bir Elliptic Curve Diffie Hellman anahtar değişimi (ECDH) tarafından desteklenen simetrik RSA şifrelemesi kullanarak Cloak ağındaki nodlar arasında güvenli iletişim sağlar. Bu, nodların güvenli bir şekilde veri alışverişi yapmasına, snoopers (ortadaki adam) ve sahtekârlara (siber saldırı) karşı koruma sağlanmasına olanak tanır. CloakShield hem Enigma hem de merkezi olmayan CloakCoin uygulamalarını güvence altına almak için tasarlanmıştır ve verilerinizin mümkün olduğunca gizli kalmasını sağlayacaktır.

CloakShield, bir veya daha fazla alıcıya şifreli veri gönderilmesine izin verir. Tek bir alıcıya gönderirken, yararlı yük (payload), ECDH paylaşılan gizlilik kullanılarak RSA ile şifrelenir. Birden fazla alıcıya gönderirken, yararlı yük (payload) bir kerelik anahtar kullanılarak şifrelenir ve daha sonra anahtar, her alıcı için ECDH / RSA yöntemi kullanılarak şifrelenir.

PAYLAŞIMLI ŞİFRELEME ANAHTARI OLUŞTURMA

Alice ve Bob'un güvenli bir şekilde iletişim kurması için, paylaşılan bir şifreleme anahtarı üzerinde anlaşmaları gerekir. CloakShield, bunu gerçekleştirmek için ECDH'yi kullanır:

- Alice'de Enigma özel anahtarı dA ve Enigma public key QA = dAG vardır (burada G elliptic-curve için üreticidir). Bob'da Enigma özel anahtarı dB ve Enigma public key QB = dBG vardır.

- Alice, Bob'un gizleme yardımı için kullanılabilirliğini duyurmak için ağa gönderdiği Enigma duyurularından Bob'un Enigma açık dB anahtarına sahiptir. Paylaşılan gizliliği dAQB=dAdBG (ECDH_compute_key in OpenSSL) hesaplamak için özel dA anahtarını ve Bob'un ortak QB anahtarını kullanır.

- Alice daha sonra bir SHA256 hash yaratır ve şifreleme anahtarı ve IV türetmek için hash'i OpenSSLEVP_BytesToKey yöntemine geçirir. Bu Bob'un verilerini şifrelemek için kullanılacaktır (simetrik RSA şifrelemesi kullanarak).

- Alice artık Bob için CloakShield korumalı mesajlar oluşturabilir.

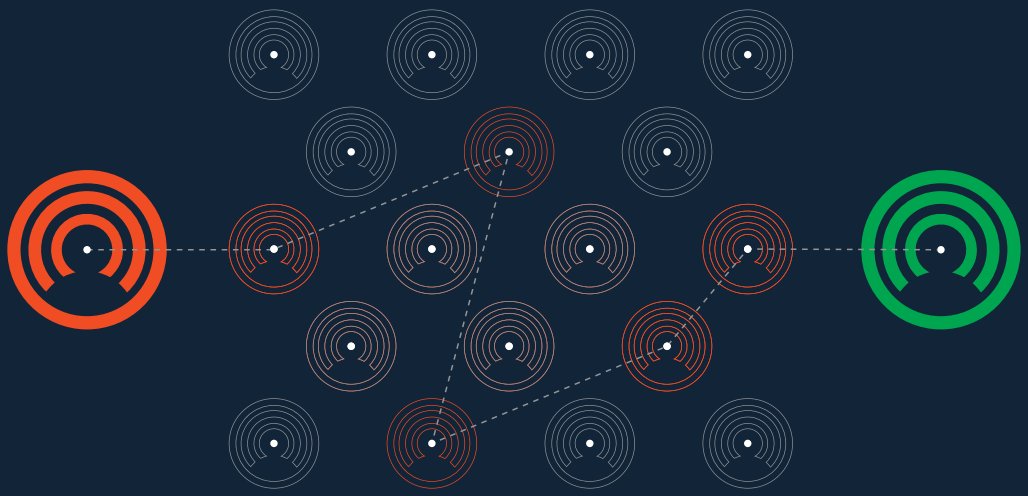
Bob, Alice'den Cloak Korumalı bir mesaj aldığında, Alice'in ortak anahtarını mesaj başlığından okur ve yukarıdaki adımlara göre (Alice'in yerine gizli anahtarı ile) Alice ile aynı paylaşılan gizli anahtarı oluşturur.

Cloak cüzdanı aktif CloakShield anahtarlarının bir listesini tutar ve bir tane oluşturmadan önce varolan bir CloakShield anahtarının listesini kontrol eder.

CLOAKSHIELD VERİSİ

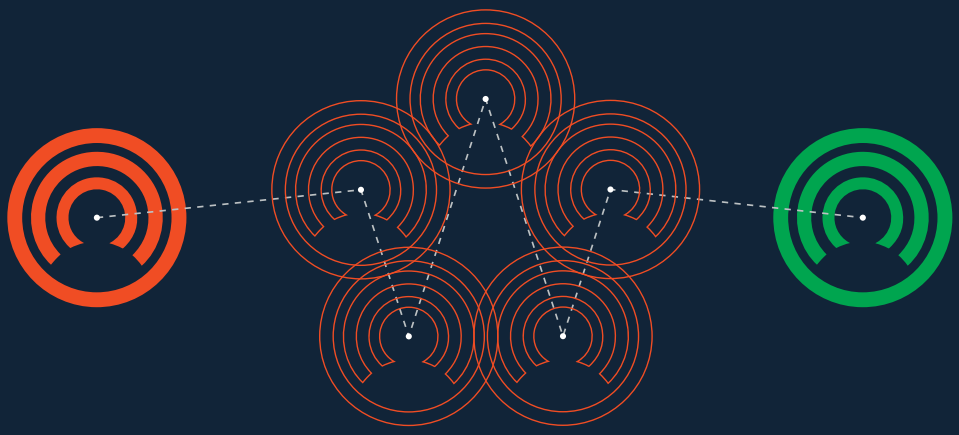
CloakShield, herhangi bir Cloak veri nesnesinin serileştirilmesine ve bir veya daha fazla alıcıya güvenli bir şekilde aktarılmasına izin verir. CloakShield veri paketi başlığı, gönderenin Enigma genel anahtarını ve alıcıların ortak anahtar hashlerini içerir.

CloakShield üstbilgileri, gönderenin ortak anahtarı ve işlenmemiş şifrelenmemiş veriler kullanılarak oluşturulan bir doğrulama hash'i içerir. Bu hash, başlıktaki alıcı bilgisinin şifreleme anahtarıyla eşleştiğinden ve verilerin değiştirilmedi- ğinden emin olmak için CloakShield verilerinin şifresini çözme sırasında doğrulanır.



CLOAKSHIELD ONION ROUTING

Onion routing bilgisayar ağı üzerinden anonim iletişim için kullanılan (TOR tarafından kullanılan) bir tekniktir. Bir onion ağında, mesajlar bir soğanın katmanlarına benzer şifreleme katmanları içinde kapsüllenir. Şifrelenmiş veri, onion routers adı verilen bir dizi ağ noduyla iletilir. Bunların her biri, verilerin bir sonraki hedefini ortaya çıkararak tek bir katmanı "siler". Son katman şifresi çözüldüğünde, mesaj hedefine ulaşır. Gönderici anonim kalır, çünkü her aracı sadece anlık olarak önceki ve sonraki nodların yerisini bilir.



ONION ROUTING ANALOJİSİ

Enigma ağına (CloakShield kullanarak) ‘onion routing’ işlevselliğinin eklenmesi, nodların dolaylı olarak trafik analizini atlatmasına izin verir. Bu, hangi nodların birbiriyle iletişim kurduğunu belirleme girişimlerini veya CloakCoin ağına işlem gönderen nodları belirleme girişimlerini engeller. Bir Enigma nodu, başka bir Enigma nodu ile iletişim kurmak istediğinde, iletişim için aktarıcı olarak hareket etmek üzere bir dizi başka Enigma nodunu seçer. Her şifrelenmiş katman sadece istenilen aktarıcı tarafından çözülebilir [Belirli katmanın şifrelenmiş olduğu yer]. Bir katmanın şifresini çözdükten sonra, aktarıcı, verileri bir sonraki aktarım noduna geçirir. Bu yönlendirme, veriler hedeflenen alıcıya ulaşıncaya kadar devam eder ve tüm katmanlar seçilen aktarım nodları tarafından şifrelenmiştir. Enigma ağının kendine özgü yapısı nedeniyle çıkış nodları gerekli değildir ve CloakShield, bir aktarım nodunun şifrelenmiş verileri okuması veya değiştirmesi riski olmadığını garanti eder.

4. STEALTH ADRESLERİ

Cloak, özel / güvenli işlemleri düzeltmek için Enigma sistemini kullanır.

CLOAKSHIELD – NOD'DAN NOD'A İLETİŞİM

Başlangıçta her bir Cloak cüzdanı ad-hoc gizliliklerini elde etmelerini sağlamak için kendi özel anahtarı ve alıcının ortak anahtarı ile ECDH'yi kullanarak bir [NID_secp256k1] keypair (Cloaking Şifreleme Anahtarı / CEK-Cloak Encryption Key) üretir. Bu iletişim Enigma ile ilgili tüm nod'dan nod'ad iletişimlerde temel oluşturur. Bununla ilgili daha fazla bilgi için 'src/enigma/ cloakshield.h/. cpp'adresine bakınız. Bu ECDH tabanlı şifreli iletişim, CloakShield tarafından ele alınan onion-routed veriler için kullanılmaktadır.

Onion routing etkinleştirildiğinde, istemci, bildiği Enigma peers listesini kullanarak veriler için geçerli bir onion route oluşturmaya çalışacaktır. Node, Enigma peers ile doğrudan bir bağlantıya sahip olmayabilir, ancak CloakData (CloakShield ile yönlendirme için paketlenmiş veriler) paketler eşler arası olarak aktarılırken bu gerekli değildir. Bir Onion Route varış noduna ulaşana kadar her bir route'ta 3 atlama nodu içeren genelde tipik olarak 3 farklı route'tan oluşur. Yönlendirme nod'ları çevrimdışı kaldığı durumlarda bunlarla başa çıkmak için çoklu route'lar kullanılır.

Nodlar onion routing hizmetlerini tanıtmak adına, peer'lara düzenli olarak Enigma Announcement'lar (src/enigma/enigmaann.h) gönderir. Ağ üzerindeki diğer nodlar duyuruları saklar (sona erene veya bir güncellemeyle değiştirilene kadar) ve onion route'ları oluşturmak için bunları kullanır.

STEALTH - GİZLİ ADRES İŞLEM ÖRNEĞİ

Bir nod Enigma işlemini stealth/gizli bir adrese gönderdiğinde, aşağıdakiler gerçekleşir:

1. Gönderici gönderilen tutarı, Enigma ödül ve ağ ücretini karşılamak için girdilerini oluşturur (0 coin ile1000 arasında % 1 oranında. 1000 ve üstü coin % 0.2).

2. Gönderici bir Gizleme İsteği - Cloaking Request nesnesi oluşturur. (Bu istek tekil Stealth Nonce içerir).

3. Gönderici alıcının stealth (gizlilik) adresi aracılığıyla 2 ile 4 arasında tek kullanımlık Stealth (gizlilik) ödeme adresi oluşturur ve gönderilen tutarı bu adresler arasında raslantısal olarak bölüştürür.

4. Gönderici, kaç katılımcının kullanılacağına karar verir. En düşük 5 en çok 25 katılımcı seçilebilir. (her katılımcı eşit bölünmüş Enigma ücretinin % 80-120'sini alır).

5. Gönderici ağa Cloak Request'i onion routes yolu ile gönderir. İstek, "gönderim tutarı" nı içermektedir, bu sayede Cloaker'lar bakiyelerinden ne kadar ayrılacağını bilmektedir.

6. Cloaker CloakRequest'i alır ve katılmaya karar verir.

7. Cloaker, göndericiye X girdileri ve gizli bir adres ve gizli hash (değişim için) sağlar.

8. Cloaker, Gönderen'e Gizleme Kabul Yanıtı - CloakingAcceptResponse gönderir. Bu gizli adres, Stealth (gizli) Nonce ve TX girdileri içerir.

9. Gönderici, yeterli Cloaker kabul edene kadar bekler.

10. Gönderici kendi ve Cloaker'ın girdilerini kullanarak Enigma transfer işlemi oluşturur. Tüm girdiler karıştırılmıştır.

11. Gönderici tüm Cloaker'lar iin TX çıktıları oluşturur. Çıktılar değişimlerini raslantısal olarak ayırır ve onlara geri gönderir. Bu aynı zamanda, Cloaker'lara ödüllerini bölüştürür.

12. Gönderici Enigma TX için kendi değişim iadelerini oluşturur. Bunlar tek seferlik gizli ödeme adresleridir.

13. Gönderici ağ TX ücretini hesaplar ve bunu kendi değişim geri dönüşlerinden çıkarır.

14. Gönderici Enigma TX'i imzalamak için Cloaker'lara gönderir.

15. Cloaker'lar, girdilerinin mevcut ve doğru olduğundan emin olmak ve girdi tutarını aşan ödeme ile birlikte gizli adreslerinden birine bağlı tek seferlik ödeme adresleri olduğundan emin olmak için TX'i kontrol ederler.

16. Cloaker'lar TX'i imzalar veya reddeder ve Gönderici'ye imzalar gönderir.

17. Gönderici imzaları toplar ve tamalanmış, imzalanmış TX'i ağa iletir.

18. Nodlar, gizli ödemeler ve Enigma ödemeleri için gelen işlemleri tarar ve herhangi bir ödeme veya değişikliği tespit eder. Eşleşen ödemeler için anahtar çiftleri ve adresler oluşturulur ve oluşturulan anahtar / adresler yerel cüzdanda saklanır.

5. ENIGMA'NIN GELECEĞİ- İLERİDEKİ GELİŞMELER

Enigma, CloakCoin'in temelini oluşturur ve CloakCoin yaşamını sürdürdükçe Enigma geliştirilmeye devam edilecektir. Gelecekte geliştirilmesi öngörülen bazı özellikler şunlardır:

GELİŞTİRİLMİŞ PROOF-OF-STAKE-ALGORİTMASI

Proof-of-Stake, blok imzalamak amacıyla kripto para ağını birbirine bağlama yöntemidir ve kullanıcıların coinlerin sahipliğini göstermesi üzerine kurulmuştur. Uzun vadede blok imzalama olasılığı, sahip olunan coin sayısına bağlıdır. Örneğin, toplam coin arzının %1'ine sahip olan biri, teknik olarak tüm proof-of-stake bloklarının da %1'ini imzalar.

Proof-of-Stake, Proof-of-Work yaklaşımına kıyasla son derece daha az aritmetik güce ihtiyaç duyar ve dolayısıyla daha az enerji kullanır.

COIN AGE (COIN YAŞI) VE DOĞRUSAL PROOF-OF-STAKE

Aslında Coin Age yani Coin Yaşı terimi tüm Proof-of-Stake uygulamalarının temelinde yer alır ve CoakCoin de bunlardan biridir. Temel olarak basit bir şekilde açıklamak gerekirse, Coin Age, coin sahibinin elindeki coini harcamadan ya da başka bir yere transfer etmeden ne kadar uzun sure elinde bulundurduğu anlamına gelir. Bir transfer işlemi gerçekleştirilirse, bu coinlerin Coin Yaşı, yeniden sıfırdan başlar. Coin Yaşı hesaplamaya örnek vermemiz gerekirse, diyelim ki bir kullanıcı 365 adet CloakCoin'I 100 gün elinde bulunduruyor, bu CloakCoin'lerin yaşı 365x100 hesabından, toplam "36,500 Coin Günü" ya da yaklaşık "100 Coin Yılı" olur (Coin Yılı, artık yıl hesabı üzerindenyapılır ve tam olarak 365 gün olarak hesaplanmaz. Coin yılı 365.24 gün üzerinden hesaplanır).

Doğrusal Proof-of-Stake tasarımları Coin Age ile ilgili eleştirilere konu olmuştur. Pek çok kişi, doğrusal Proof-of-Stake'in coinlerin stoklanmasının/saklanmasının teşvik ettiğini savunmaktadır (bunun trade ve transfer hacmine olumsuz bir etkisi olabilir). Doğrusal Proof-of- Stake'e yöneltilen bir başka geçerli eleştiri ise ağ güvenliğine etki edebileceği ile ilgilidir. Kullanıcıların coinleri kazandıkları sırada düzenli olarak Cloak ağına bağlanması ve daha sonra tüm Coin Age imha edildiğinde bağlantının kesilmesi nedeniyle Doğrusal Proof of-Stake uygulamaları genellikle sıkıntı çekmektedir. Kullanıcı daha sonra, connect-stake-disconnect işlemini tekrar etmeden önce Coin Age yenilene kadar bekler. Bu durum, ağ için en iyi güvenliği sağlayan bir durum değildir ve sık ya da sürekli staking yapmayı ödüllendiren bir Proof-of-Stake algoritması, CloakCoin ve Proofof-Stake ile çalışan diğer para birimleri için de faydalı bir yöntem olarak gündeme gelmektedir.

Enigma Cloaker'ların mümkün olduğu kadar ödüllendirildiğinden emin olmak için Coin Age, CloakCoin'in Proof-of-Stake algoritmasından kaldırılmalıdır. Bu, Cloaker'ların hem tam staking ödülünü hem de Enigma Cloaking ödüllerini almasını sağlar. Staking ödüllerinin hesaplanmasında bir hız bileşeninin eklenmesi, aktif Enigma Cloaking nodlarını daha da fazla ödüllendirecektir. Bu, kullanıcıları Cloaking aracılığıyla kazandıkları gelirleri arttırmak adına Enigma transfer ağına yani Enigma Cloaking'e katılmaya teşvik edecektir. Aktif olarak katılan kullanıcılara daha fazla ödül sağlamanın yanı sıra, gelişmiş bir Proof-of-Stake algoritması ayrıca yukarıda belirtilern ağ güvenliği konusunda da geliştirmeleri sağlar.

ENIGMA İŞLEMLERİNİN BİRLEŞTİRİLMESİ VE AYRILMASI

Enigma şu anda transfer başına tek bir "Cloaked" işlemi oluşturuyor. Şu anda Enigma çerçevesinde çoklu Enigma işlemlerinin bir Enigma süper işlemine birleştirilmesine izin verecek bir güncelleme üzerinde çalışıyoruz. Bu, etkin bir şekilde birden fazla "Cloaked" işlemi içerecek ve Cloak kullanıcıları için daha da fazla anonimlik sağlayacaktır. Bu uzantı, kullanıcıların Cloaker sayısına ek olarak ihtiyaç duydukları işbirlikçi Enigma işlem sayısını seçmelerine izin verecektir.

Bu ek, elbette tamamen merkezi olmayan, özel ve güvenli olarak kalacaktır. Cloak Takımı tarafından şu anda yapılan bir başka Enigma gönderme iyileştirmesi de büyük miktarlardaki CloakCoin'i bir dizi küçük Enigma işlemi aracılığıyla "Cloaked"lamak yani gizliliğini sağlamaktır. Bunu gerçekleştirmek isteyen bir kullanıcı herhangi bir Cloak adresine gizli göndermek istediği yani orijinal terim ile Cloaked' lamak istediği miktarı seçecektir. CloakCoin arka planda, kullanıcının Cloaked olarak transfer etmek istediği miktara totalde eş olacak şekilde bir çok küçük Enigma işlemleri oluşturarak belirli bir sürede Cloked'lanan miktarın ağ üzerinde gizli transferini gerçekleştirecektir. Bu toplu işlem, "birleştirilmiş" Enigma işlemleriyle uyumlu olacak ve transferler için daha fazla Cloaking koruması sağlayacaktır.

6. SSS

S. CLOAKER'LAR BİR ENIGMA İŞLEMİNE NASIL YARDIM EDERLER?

Cloaker'lar, göndericiden gelen girdiyi "gizlemek" için kullanılan bir veya daha fazla girdi sağlar. Cloaker'lar ayrıca girdilerini döndüren ve ayrıca Cloaker'ı bir ücret karşılığında ödüllendiren bir dizi dönüş adresi de sağlar. Aktivite ile adresleri önceliklendirmek için geri dönüş adresleri dikkatle seçilir. Bu, Enigma işleminin gerçek çıktısını saptamak için blockchain analizi yapan herkes için durumu çok daha zor hale getirir. Enigma sistemi hedef adresi de kontrol edecektir böylece "gizlenmiş" çıktılar, gerçek çıktıyı olabildiğince benzer şekilde ikizler.

S. ENIGMA İŞLEMLERİNİN TAMAMLANMASI NE KADAR SÜRÜYOR?

Enigma işlemlerinin şu anda bir dakika içinde tamamlanmaktadır. Cloaking nodları Enigma işlemi tamamlanana veya ayrılan süre sona erene kadar bir Enigma işleminin gerekli fonları rezerve etmesi için 'Cloak' yapılmasına yardımcı olur. Süresi dolan veya iptal edilen bir Enigma işlemi durumunda, yeniden kullanım için fonlar yerel olarak açılır.

S. ENIGMA STAKING'İ NASIL ETKİLER?

Bir Enigma işleminde kullanılan herhangi bir coin için coin-age sıfırlanması olacaktır. (Gönderici veya Cloaker olarak). Ancak, Cloaking'e katılmanın, staking'e kıyasla çok daha yüksek bir getiri sağlama olasılığı unutulmamalıdır. Cloak Takımı, yaklaşan hardfork sürümü için Enigma algoritmasını revize etmek için çalışıyor (Enigma 1.1). Daha fazla bilgi için Bölüm 5- 'Enigma'nın Geleceği - İlerideki Gelişim'e bakınız.

S. ENIGMA CLOAKER'I OLMAK İÇİN CÜZDANIMDA BELİRLİ MİKTARDA BİR BAKİYE OLMASI GEREKİYOR MU?

Cloaking hizmetlerinizi CloakCoin cüzdanınızdaki bakiyeden bağımsız olarak sunabilirsiniz. Enigma Cloaking etkinleştirildiğinde,CloakCoin, Enigma Cloaking'e katılmak için bakiyenizin bir kısmını rezerve edecektir ve buna ilşkin olarak Cloaking ödülü kazanacaksınız. Varsayılan rezerv miktarı ~% 50 olmakla birlikte, bu değer kullanıcı tarafından ayarlanabilir. Enigma duyurularının ilan edilen Cloaking bakiyesi ile bağlanmasını önlemek için seçilen değer rasgele seçilecektir.

Daha yüksek bir bakiyeye sahip olan cüzdanların daha büyük Enigma işlemleri için gerekli Cloaking bakiyesine sahip olma olasılıklarının daha yüksek olması nedeniyle bir Cloaker olarak seçilme şansının daha yüksek olduğu belirtilmelidir.

S. HERHANGİ BİRİNİN BLOCKCHAIN'DE BENZER GİRDİ VE ÇIKTILAR ÜZERİNDEN ZAMAN BAZLI BİR SALDIRI GERÇEKLEŞTİRMESİ DURUMUNDA ENIGMA NASIL KORUMA SAĞLAR?

Enigma işlemleri, çıktıları gruplandırır ve alıcının çıktısına "cloak" yapmak için birden fazla eşleme çıktısı miktarına sahip olmasını sağlar.

S. ENIGMA İŞLEMİNİN YARATICISI İMZA SIRALAMASINI BELİRLEMEK İÇİN SCRIPT İMZASINI İNCELEYEREK BELİRLENEBİLİR Mİ?

Hayır. İmzalama sürecinde imzaları birleştirirken script - komut dizini imza sırası rastgele seçilir. Gönderici ve katılımcı Cloaker'lar bunu yapar.

S. GERÇEK GÖNDERİCİYİ BELİRLEMEK İÇİN AĞA GÖNDERİLEN ENIGMA İŞLEMLERİNİ İZLEMEK İÇİN EAVESDROPPER AĞI İZLEYEBİLİR Mİ?

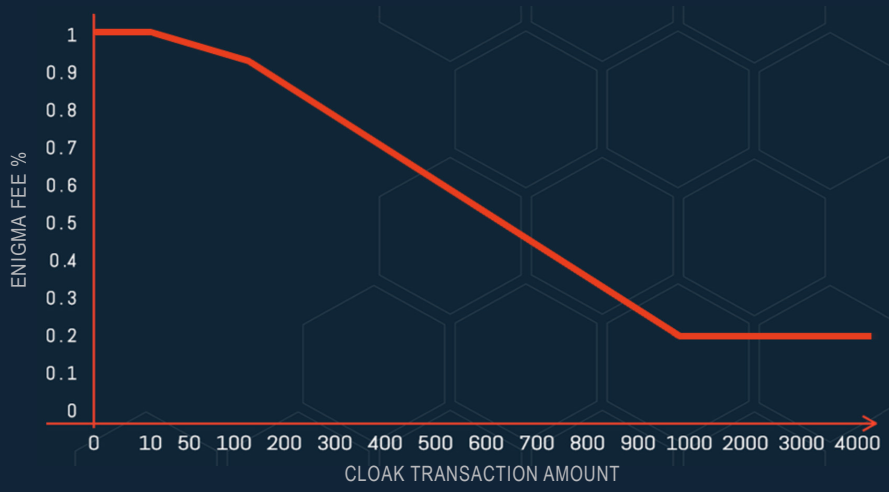
Hayır. Tüm taraflar Enigma işlemlerini ağa rastgele sırayla gönderir. Bu, eavesdropping saldırılara karşı hafifletme sağlar.

S. ENIGMA İŞLEMİ İÇİN ÜCRET NE KADARDIR?

0 ile 1000 coin arasında aşağıdaki grafikte görüleceği şekilde % 1 oranından başlar ve 1000 coine yaklaştıkça bu oran azalır. 1000 ve üstü coin için ise sabit % 0.2. Bu bir Enigma işlemini gizlemeye yardımcı olan Enigma düğümlerini ödüllendirmek için kullanılır. Ücret daha sonra işlemle karıştırılır ve Cloaker'lar arasında bölünür. Bu sadece katılımcılar için bir ödül değildir; ancak işlem miktarının tespit edilmesinin imkansız hale getirilmesine yardımcı olmak için kullanılır. Her katılımcı, eşit bölünmüş bir enigma işleminin % 80-120'sini alır.

S. ENIGMA İŞLEMİ İÇİN ÜCRET NE KADARDIR?

Enigma ücreti % olarak şu oranlarla işlem başına ücretlendirilir:



TX AMOUNT	ENIGMA FEE %	CLOAK FEE
0	1.00	0
10	0.992	0.0992
50	0.96	0.48
100	0.92	0.92
200	0.84	1.68
300	0.76	2.28
400	0.68	2.72
500	0.60	3.00
600	0.52	3.12
700	0.44	3.08
800	0.36	2.88
900	0.28	2.52
1000	0.20	2.00
2000	0.20	4.00
3000	0.20	6.00
4000	0.20	8.00

S. ENIGMA, CLOAK AĞININ HARD-FORK OLMASINI GEREKTİRİR Mİ?

Hayır. Daha eski CloakCoin müşterileri Enigma işlemlerini sorunsuz bir şekilde ele alacaklardır ancak onları oluşturmaları veya bunları 'cloaking' işlemine katılmaları mümkün olmayacaktır. Bununla birlikte, Enigma'nın bir sonraki revizyonu, altta yatan Proof-of-Stake algoritmasında yapılan değişikliklerden dolayı bir hard-fork gerektirecek ve piyasa özellikleri için ek script opcode destekleyecektir. (Blok Escrow gibi).

S. ENIGMA İŞLEMİNDE YARDIMCI OLABİLECEK MAKSİMUM CLOAKERS SAYISI NEDİR?

Maksimum Cloaker sayısı 25 olarak sabitlenmiştir. Enigma sistemi esnektir ve bu sayı kolayca genişletilebilir.

S. ENIGMA, KÖTÜ AKTÖRLERE 'BAD ACTORS' KARŞI NASIL KORUMA SAĞLAR?

Enigma sistemi, bir oturum boyunca "kara liste- blacklist" düğümlerine kapsamlı DDoS koruması sunar. Bir Enigma düğümü tekrar tekrar imzalamayı reddederse, bunlar mevcut oturumun kalan kısmı için Enigma Cloaking davetlerinden çıkarılacaktır. Şu anda işbirlikçi olmayan Enigma düğümlerini cezai müeyyide altına almak için ek metodolojiler araştırıyoruz, Bir düğümün bir Enigma işlemini sonlandırılmış işlemi imzalamayı reddederek engellemeye çalıştığı durumlarda Cloakers'ların örneklerde ceza olarak talep edilebilecek, nominal, iade edilebilir bir ücreti emanet etmesi için bir sistem uygulayacağız. Dikkat çekilmesi gereken nokta, kötü niyetli nodlar Enigma işlemlerini engellemeye çalışsalar dahi, herhangi bir fonu çalamaz veya kötüye kullanamazlar.

S. GİZLİ VE ENIGMA İŞLEMLERİ NASIL ALGILANIR/ ALINIR?

Tüm gelen işlemler taranır. Gizli işlemler önce taranır (rasgele bir OP_RETURN TX çıktısında bulunan varsayılan geçici pubkey'in kullanılması ile). Bundan sonra, Enigma işlemleri taranır. Enigma işlemleri ayrıca standart geçici pubkey'i kullanır, ancak ödemeler bundan sonra türetilmiş bir anahtar içeren ek bir adım daha kullanır. Enigma çıktıları, ephemeral pubkey'in bir hash'ı, özel bir gizli adres hash'ı ve çıktı indeksi kullanılarak oluşturulur.

Enigma işlemlerini tararken, zero-index ödeme adresleri her bir gizli adres için üretilir.

[HASH(ephemeral_pubkey, hash_stealth_secret, 0)]. Gizli adresin zero-index - sıfır indeksi için bir eşleşme bulunursa, kalan dizinler için ek adresler oluşturulur [num_tx_outputs] ve bunlar ödemeleri tespit etmek için taranır. Daha fazla bilgi için wallet.cpp dosyasındaki FindEnigmaTransactions -Enigma İşlemlerini Bul bölümüne bakın.

Benzer bir tarama yöntemi, bir Enigma TX imzalamadan önce Cloaker'lar tarafından doğru şekilde geri ödeme yapıldığından emin olmak için kullanılır. Daha fazla bilgi için wallet.cpp adresindeki Enigma Çıktı Miktarlarını Al - GetEnigmaOutputsAmount'larına bakın.

7. REFERENCES

[01] http://bitcoin.org

[02] https://en.bitcoin.it/wiki/Category:Mixing Services

[03] https://wiki.openssl.org/index.php/Elliptic_Curve_Diffie_Hellman

[04] http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization

[05] https://bitcointalk.org/index.php?topic=279249.0
(CoinJoin: Bitcoin Privacy for the Real World)

[06] https://bitcointalk.org/index.php?topic=27787.0
(Proof of Stake Instead of Proof of Work)

[07] https://en.bitcoin.it/wiki/Proof_of_Stake

[08] https://en.bitcoin.it/wiki/Deterministic_wallet

[09] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[10] http://www.onion-router.net

www.cloakcoin.com

https://chat.cloakcoin.com

www.twitter.com/CloakCoin