BİTCOİN'DE MAHREMİYETİ SAĞLAMA YÖNTEMLERİ

Süleyman KARDAŞ[1*], Mehmet Sabır KİRAZ[2]

[1*] Batman Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Batman, Türkiye

[2] TÜBİTAK BİLGEM, Kocaeli, Türkiye

Özet

Bitcoin, para transfer işlemlerini blokzincir olarak adlandırılan dağıtık, halka açık ve sadece eklenebilir bir deftere kaydeden yaygın bir kripto para birimidir. Bitcoin'in güvenliği, madenci ağ düğümleri tarafından çalıştırılan teşvik uyumlu emek kanıtı tabanlı dağıtık uzlaşma protokolüne dayanır. Kazanç karşılığında, madencilerin ağdaki sorumluluklarını yerine getirmeleri beklenir. Öte yandan, 2009 yılında piyasaya sürüldüğünden beri, Bitcoin ekonomisi çok büyük bir hızla büyümektedir ve şu anda pazar değeri 130 milyar dolara ulaşmıştır. Pazar ekonomisinin bu kadar yüksek olması, kişi ve kurumların mahremiyetinin sağlanabilmesi için transfer işlemlerinin anonim bir şekilde gerçekleşmesi istenir. Mevcut durumda Bitcoin'inin özü ile yapılan işlemlerin takip edilebilmesi mümkün olmaktadır. Transferlerde gönderici/alıcı ve işlem miktarlarının herkes tarafından görülebilmesi mahremiyet problemini ortaya çıkarmaktadır. Transfer işlemlerinin anonim hale getirilmesi için pek çok farklı yöntem geliştirilmiştir. Bu makalede, öncelikle Bitcoin'in ana bileşenlerine genel bir bakış sunulmuş ve sistemdeki işlevselliği ile beraber etkileşimleri açıklanmıştır. Daha sonra, Bitcoin'in mevcut anonimlik değerlendirmeleri sunulmuş, var olan çözümlerin analizi ve olası güvenlik tehditleri ne yer verilmiştir. Son olarak, sonuçlar değerlendirilmiştir.

Anahtar Kelimeler: Blokzincir, Bitcoin, mahremiyet, anonimlik.

TECHNIQUES FOR PROVIDING ANONYMITY IN BITCOIN

ABSTRACT

Bitcoin is a widespread cryptocurrency that records crypto money transfer transactions in a distributed, publicly open, and only addable registers, named blockchain. Bitcoin's security relies on an incentive-compliant proof-of-work based distributed consensus protocol run by mining network nodes. The mining nodes are exptected to fulfill their responsibilities in the network because of incentives. On the other hand, since launching the market in 2009, the Bitcoin economy has grown at a tremendous pace, and now the market value has reached 130 billion dollar. Since the market economy is so high that it is desirable to make money transfers anonymously in order to provide privacy of individuals and enterprises. In the present case, it is possible to trace the transactions made with the Bitcoin's core. The fact that the sender / receiver and transaction amounts are visible to everyone in transfers reveals the problem of privacy. Many different methods have been developed so far to provide anonymization of transactions. In this article, we first give an overview of the main components of the Bitcoin and their interactions with the functionality in the system. Subsequently, Bitcoin's current anonymity evaluations, analysis of existing solutions and potential security threats are presented. Finally, the work is concluded.

Keywords: Blockchain, Bitcoin, privacy, anonymity.

I. GİRİŞ (INTRODUCTION)

Bitcoin, bir banka, bir yeminli mali müşavir, noter veya herhangi bir diğer merkezi hizmet olarak görünebilecek herhangi bir güvenilir üçüncü taraf otoritesi olmadan çalışan eşler arası bir teknolojidir [1]. Özellikle, Bitcoin sahipleri, kripto paraları üzerinde tam kontrole sahiptir ve bunları, herhangi bir merkezi otorite içermeden, her an ve her yerde harcayabilirler. Bitcoin teknolojisinin tüm tasarımı açık kaynak kodla ile tasarlanmıştır ve hiç kimse bu kodların sahibi değildir veya bu sistemi tek başına kontrol edemez. Ayrıca, bir yandan kriptografik olarak güvenli bir elektronik ödeme sistemi olarak görü-

lürken bir yandan da altın gibi saklama aracı olarak görülmektedir.

Bitcoin, 2009 yılında kurulmasından bu yana hem akademi hem de endüstri tarafından büyük ilgi görmektedir. Piyasa değeri 130 milyar olan ve 223.000 adetten fazla teyit edilmiş günlük toplam işlem sayısı ile (block chain.info, Mayıs 2018), Bitcoin bugüne kadar ki en başarılı kripto para birimi olarak göze çarpmaktadır. Söz konusu para transferlerin miktarı ve değeri göz önüne alındığında, Bitcoin saldırganlar için açık bir hedef haline gelmiştir. Gerçekten de sistemin farklı yönlerini hedefleyen çok sayıda çift harcama [2], netsplit [3], işlem bütünlüğünü bozma [4], ağ saldırıları [5], madenciliği hedef alan saldırılar [6-8], madencilik havuzları hedef alan saldırılar [9] gibi saldırılar gerçekleştirilmiştir.

Ödeme sistemlerinde iki temel güvenlik kriter önemli olmaktadır. İşlemi gerçekleştiren kişilerin mahremiyeti ve işlemlerin gizliliğidir. İşlemler ile ödemeyi yapan kişiler arasında ilişkiyi ortadan kaldırılması ile anonimlik sağlanır. İşlemlerin şifrelenmesi ise işlemlerin gizliliğini sağlar. Geleneksel bankacılık sistemi, ilgili taraflara ve güvenilir üçüncü tarafların işlem bilgisine erişimi sınırlandırarak bir anonimlik seviyesi sağlamaktadır. Bitcoin'de, tüm işlem verileri ağa bağlı herhangi bir kullanıcıya açık bir şekilde gösterilmektedir. Bununla birlikte, mahremiyet, Bitcoin işlem zincirinde bir yerdeki bilgi akışını kırarak belirli bir seviyeye kadar korunabilmektedir. Bitcoin, açık anahtarları anonim olarak tutarak bunu başarmaktadır. Diğer bir deyişle herhangi bir kişi yeni anahtarlar üreterek bir başkasına bir miktar bitcoin yollayabilir, ancak yapılan işlem gönderen kişi ile ilişkilendiren bilgi olmadan gerçekleştirilmektedir. Ancak önceki işlem sıralarının tamamının açık olması bu anahtarların anonim olmasının önemini ortadan kaldırmaktadır. Yani, kullanıcı mahremiyetini sağlamak için, işlemlerin belirli bir kullanıcıya bağlı olmalarını engellemek için her işlem için yeni bir anahtar çifti kullanılması önerilmektedir. Bununla birlikte, çok girişli işlemlerde, yine de bunların sahiplerinin aynı kripto para sahibine ait olduğunu gösteren bağlantıların ortaya çıkarılması mümkün olmaktadır. Ayrıca, bir anahtarın sahibinin ifşa edilmesi durumunda, bağlantının aynı kullanıcıya ait diğer işlemleri ortaya çıkarma riski bulunmaktadır. Özellikle, Bitcoin kısmi ilişkilendirilemezliği (yani, takma numara ile) sağlar. Bu sayede, sağlam bir blokzinciri analiz prosedürü vasıtasıyla para akışını takip ederek bir takım işlemlere bireysel bir kullanıcı ile ilişkilendirilmesi mümkün olmaktadır.

Bitcoin teknolojisi gizlilik söz konusu olduğunda kendini gösterir ama Bitcoin'de mevcut olan tek gizlilik, sözde adreslerden (ortak anahtarlar veya bunların karmaları) gelir. Kişilerin mahremiyeti, Bitcoin adreslerin yeniden kullanımı, "leke" analizi ve blokzincir analiz yöntemleri, IP adresi izleme düğümleri, bir kaç isim için izleme ödemeleri gibi farklı teknikler aracılığıyla ortadan kaldırılabilmektedir. Bir kez kırıldığında, gizliliği tekrardan sağlamak zor ve çok pahalı olabilmektedir. Bitcoin'in işlemle ilgili diğer bilgileri korumak için herhangi bir dizinin bulunmadığını (günce (log) tutulmadığı) bilinmektedir. Ancak, bir saldırgan e-posta ve gönderim adresleri gibi çevrimdışı verileri çevrimiçi bilgilerle ilişkilendirebilir ve eşler hakkındaki özel bilgilere erişebilir. Daha açık bir ifade ile hâlihazırdaki Bitcoin tasarımı mahremiyeti tam olarak sağlamamaktadır. Bitcoin protokolünün en temelinde transfer işlemleri yatmaktadır. Gerçekleşen tüm işlemler blokzincirde saklanmakta ve herkese açıktır, yani hangi adreslerin hangi adreslere ne kadar bitcoin gönderildiği görülmektedir. Bu adreslerden bazıları gerçek dünya kimlikleriyle bağlantılıysa, kimler arasında para transferi olduğu ortaya çıkabilir. Bu, kişiler ve kurumlar arasındaki mahremiyeti sağlama ile çelişmektedir. Ayrıca, birden fazla bitcoin adreslerinden girdiler aynı işlem üzerinden başka adrese gönderilmektedir. Bu da aynı kişinin hangi adreslere sahip olduğunu da göstermektedir. Bu sebeplerden ötürü, bu çalışmada, Bitcoin kullanıcılarının mahremiyetine yönelik çeşitli güvenlik tehditlerini ve bunları geliştirmek için önerilen en son teknoloji ürünü çözüm yöntemleri verilmiştir. İşlemlerdeki miktarlar ile gönderici/alıcı adresleri şifrelenerek mahremiyet sağlanabilmektedir. Bu çalışmada Bitcoin'in özü ile kişilerin mahremiyetini sağlamak için önerilen yöntemler üzerinde duruldu.

Bu makalede, öncelikle Bitcoin ve altyapısındaki bileşenler Bölüm II detaylı bir şekilde anlatıldı. Daha sonra, Bitcoin'deki işlemleri anonimleştirmek için önerilen yöntemler anlatıldı. Son olarak, yöntemlerin karşılaştırmalı tablosu sonuç bölümünde tartışılarak verildi.

II. BITCOIN'E GENEL BAKIŞ (BITCOIN IN GENERAL)

Bitcoin, 2008 yılında Satoshi Nakamoto tarafından sunulan merkezi olmayan bir elektronik ödeme sistemidir [1]. Güvenliği eşler arası ağa ve olasılıklı dağıtık *emek kanıtı* uzlaşma protokolüne dayanmaktadır. Bitcoin'de, elektronik ödemeler, kullanıcılar arasında bitcoin transfer eden işlemler ile yapılmaktadır. Bitcoin adresi kullanıcının ortak anahtarında geri dönüşü olmayan kriptografik özet fonksiyonlar ile işlemler gerçekleştirilerek oluşturulur. Bir kullanıcı birden çok ortak anahtar oluşturarak birden fazla adrese sahip olabilir ve bu adresler cüzdanlarından biri veya birkaçıyla ilişkilendirilebilir. Kullanıcının özel anahtarı, sahip olunan bitcoin transfer işlemlerini elektronik olarak imzalanmasında kullanılmaktadır. Açık anahtardan üretilen bir adres alıcısı kullanıcılara belirli bir seviyede anonimlik sağlar ve her bir alım işlemi için farklı Bitcoin adresle-

rinin kullanılması önerilmektedir.

İşlemler, "*madenciler*" adı verilen bir grup becerikli ağ düğümleri tarafından bütünlük, özgünlük ve doğruluklarını asıllamak için işlenir. Gerçekte, tek bir işlem yerine bir grup işlemin bir araya getirilerek blok oluşturulur ve bu blok *madenciler* tarafından işlenir. İşlenen bloktan ödül almak için madenciler diğer düğümlere işlenmiş bloğu gönderirler. Bu blok, blokzincire başarıyla eklenmeden önce ağdaki *madencilerin* çoğunluğu tarafından doğrulanması beklenir. Bir blok deftere başarılı bir şekilde eklenmesi durumunda o bloğu kim işlemişse hesabına ödül eklenir. Bir sonraki alt bölümlerde, Bitcoin'in pratik olarak gerçekleştirilmesi için gerekli olan temel teknik bileşenler hakkında bir genel bakış verilecektir.

A. Özet Fonksiyonları

Özet alma işlevi, neredeyse her boyutta bir girdi değerlerini (örn. dosya, metin veya resim) kullanarak nispeten benzersiz sabit büyüklükte bir çıktıya eşleyen bir yöntemdir. Genel bir deyişle, bir özet fonksiyonu, $H: \{0,1\}^* \rightarrow \{0,1\}^n$ herhangi uzunluktaki ikili sayıyı, n uzunluğundaki ikili sayıya eşleyen bir fonksiyondur. Bu fonksiyonun beş temel özelliği bulunmaktadır:

- Özet fonksiyona giren bir veri her zaman aynı sonucu verir.
- Özet fonksiyonları hızlı bir şekilde verinin özetini hesaplar.
- Girdi üzerindeki yapılan en ufak bir değer değişimi bile (örn. tek bir bitlik değişim) tamamen farklı çıktıya sahip özetle sonuçlanacaktır.
- Özet fonksiyonun çıktısından girdi verinin ne olduğunu bulmak polinom zamanda mümkün olmamalıdır (tek yönlü fonksiyon).
- Özet algoritmaları da çarpışmaya dirençli olarak (ikincil ön-imaj (second preimage)) tasarlanmalıdır: *aynı çıktıyı* üreten iki veya daha fazla girdi bulmak polinom zamanda bulmak mümkün olmamalıdır.

Özet fonksiyonları veri bütünlüğü kontrolü sağladıkları için blokzinciri veritabanında büyük öneme sahiptir. Bitcoin'de SHA256 ve RIPEMD160 özet fonksiyonları kullanılmaktadır.

B. Asimetrik Anahtarlı Kriptografi

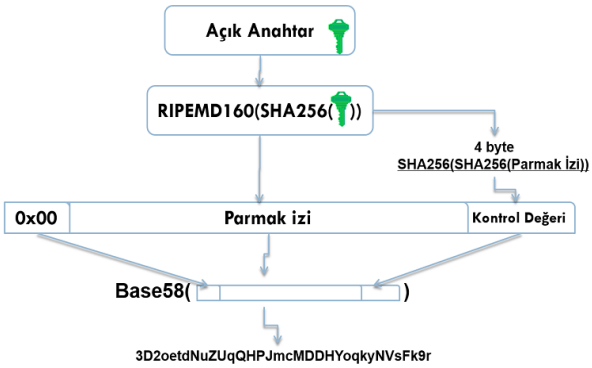
Bitcoin'de asimetrik anahtar şifrelemesini işlemlerin elektronik olarak imzalanmasında kullanılmaktadır. Bu imzalama ile bitcoin transferi yapacak olan kişinin hangi adresten gönderim yapıyorsa o adrese ait özel anahtarı bilmesi gerekmektedir ve bu anahtar ile imzalamayı gerçekleştirir. Asimetrik şifreleme/imzalamada her bir kullanıcının *açık* ve *gizli*/*özel* olmak üzere bir çift anahtarı bulunmaktadır. Bu iki anahtar matematiksel olarak birbiri ile ilişkili olup açık anahtarın kamu ile paylaşılmasında mahsur bulunmazken *özel* anahtarın sadece sahibi tarafından bilinmesi gerekir. Açık anahtarı kullanarak polinom zamanda *özel* anahtarı elde etmek mümkün olmamaktadır. Fakat *özel* anahtar kullanılarak açık anahtara erişmek mümkün olmaktadır. Asimetrik anahtarlar ile şu işlemler gerçekleştirilmektedir:

- **Şifreme:** Bir veri gönderilecek kişinin *açık* anahtarı ile şifrelenir ve o kişiye gönderilir. Alıcı, gelen şifreli verinin *özel* anahtarına sahip ise mesajı çözer.
- **İmzalama:** Bir veriye elektronik imza atmak için o verinin özeti *özel* anahtar ile şifrelenir. Veri ve imza değeri paylaşılır. Sistemde herhangi bir kişi *açık* anahtar ile imzanın doğruluğunu kontrol eder.

Bitcoin'de eliptik eğri tabanlı imzalama algoritması olan 'Elliptic Curve Digital Signature Algorithm' (ECDSA) kullanılmaktadır [1].

C. Adresler ve Adres Üretimi

Bir bitcoin adresi veya basitçe adres, ödeme yapmak için olası bir hedefi temsil eden 1 veya 3 numaralı numaradan başlayarak 26-35 tane rakam ve harflerden oluşan bir numaradır. Adresler, herhangi bir bitcoin kullanıcısı tarafından ücretsiz olarak çevrimiçi olmadan üretilebilir. E-posta gönderir gibi istenilen adrese bitcoin gönderilebilmektedir. Ancak, e-posta adreslerinden farklı olarak, kullanıcıların birçok farklı Bitcoin adresi bulunabilmektedir ve her işlem için benzersiz bir adres kullanılmaktadır. Çoğu bitcoin transfer yazılımı ve web sitesi, her transfer işlemi talebi oluşturduğunuzda yepyeni bir adres üreterek bu konuda yardımcı olacaktır. Çoğu Bitcoin adresleri 34 karakterdir. Rastgele rakamlar ve büyük ve küçük harflerden oluşurlar, istisna olarak 'O' harfi, büyük harf 'I', küçük harf 'l' ve '0' sayısı görsel belirsizliği önlemek için asla kullanılmaz. Bitcoin adresi açık anahtarın birden fazla özet değerinin alınması ile oluşturulmaktadır (Bknz. Şekil 1).



Şekil 1. Bitcoin'de Adres Üretimi

D. İşlemler

Bir işlem, taraflar arasındaki varlıkların bir kullanıcıdan diğer bir kullanıcıya transferinin bir kaydıdır. Yani, para yatırıldığında veya çekildiğinde her zaman için bir işlem oluşturulur. Bir blokzincirdeki her blok, birden fazla işlemi içerir (örn. 2000-3000 işlem). Bir işlemde bir veya birden fazla girdi bulunduğu gibi bir veya birden fazla çıktı hesabı da olabilmektedir. Diğer bir deyişle, aynı anda birden fazla farklı hesaba bitcoin transferi yapılabilmektedir. Girdiler, önceden hesaba gönderilen bitcoin transferleridir, yani daha önceki başka işlemlerin çıktılarıdır. Girdilerin toplamı ile çıktıların toplamı birbirine eşit olmalıdır (Bknz. Tablo 1).

Tablo 1.Örnek Bitcoin Transfer İşlemi

İşlem #1699			
Girdiler	**Çıktılar**		
#1040 Nolu İşlem	3BTC	Bitcoin Adresi #1234…	2BTC
#1453 Nolu İşlem	7BTC	Bitcoin Adresi #2341…	6BTC
		Bitcoin Adresi #2452…	2BTC
Toplam **10** BTC	Toplam **10** BTC		

Bir işlemin geçerliliğini belirlemek önemlidir. Birinin işlem gerçekleştirdiğini iddia etmesi, bunun gerçekleştiği anlamına gelmez. İşlemi yapan kişi, tüm girdileri ve transfer yapılacak olan bitcoin adreslerini, *özel* anahtarıyla elektronik olarak imzalaması gerekir. Bitcoin özelinde bir işlemin gerçekleşmesi için en az 6 onay olması gerekmektedir. Gerçekleşen işlem, işlemi yapan kişinin açık anahtarı ile herhangi bir zamanda doğrulanır.

E. Bloklar

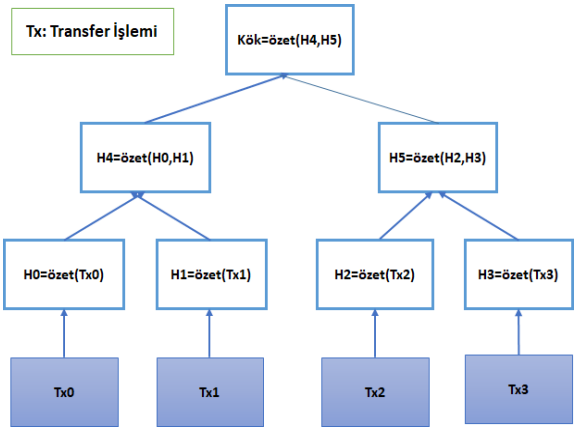
İşlem verileri, blok adı verilen dosyalara kalıcı olarak kaydedilir. Bloklar zaman içinde doğrusal bir sıra halinde düzenlenir. Yeni işlemler, madenciler tarafından sürekli olarak zincirin sonuna eklenen yeni bloklarda işlenirler. Bloklar blokzincirine eklendikçe, zinciri değiştirmek veya önceki blokları zincirden çıkarmak zorlaşmaktadır. Bu durum bitcoin'deki işlemlerin bütünlüğünün sağlanmasına ve hiçbir şekilde değiştirilmesine izin vermemektedir. Bloklar, 5 farklı kategoride bilgi içermektedir (Bknz. Tablo 2).

Tablo 2. Blok Yapısı

Alan	**Açıklama**	**Boyutu**
Sihirli No	Değer: her zaman 0xD9B4BEF9	4-byte
Blok Büyüklüğü	Bloktaki toplam byte sayısı	4-byte
Blok Başlığı	6 alt maddeden oluşur	4-byte
İşlem Sayacı	Pozitif bir sayı	4-byte
İşlemler	İşlemler listesi	4-byte

Bir blok başlığı ise bir önceki blok başlığının kriptografik özet değeri, bloğun yayınlanma zamanı, bloktaki işlemlerin *Merkle* kök özet değeri, tek kullanımlık sayı (*teksa*), hedef zorluk derecesi ve blok sürüm numarası olmak üzere 6 farklı alandan oluşmaktadır. Her işlemin özet değerini bir bloğun başlığına depolamak yerine, bir *Merkle* ağacı olarak bilinen bir veri yapısı kullanılır. Bir *Merkle* ağacı, verilerin karma değerlerini tekil kök olana kadar birleştirir (Bknz. Şekil 2). Kök, bir bloğun işlemlerini özetlemek ve bir blok içindeki bir işlemin varlığını doğrulamak için kullanılan etkili bir mekanizmadır. Bu yapı, dağıtık bir ağda gönderilen verilerin geçerli olmasını sağlar. Zira temel verilerdeki herhangi bir değişiklik algılanır ve atılabilir. Şekil 2'de, bir *Merkle* ağacın bir örneği gösterilmektedir:

- En alttaki satır, özetlenecek işlemleri temsil eder.
- Alt satırda ikinci veri özetlenmiş olduğunu gösterir.
- İkinci sıradaki özet veriler daha sonra birleştirilir ve daha sonra üçüncü sıradan alttaki satıra özeti alınır.



Şekil 2. Bir Merkle Kök Ağacı Örneği

Son olarak, üstteki satır, H4 ve H5'i birleştiren ve birleştiren Kök karmasını gösterir. Böylece, kök özet değeri, önceki tüm işlemlerin ve özetlerin bir özetidir.

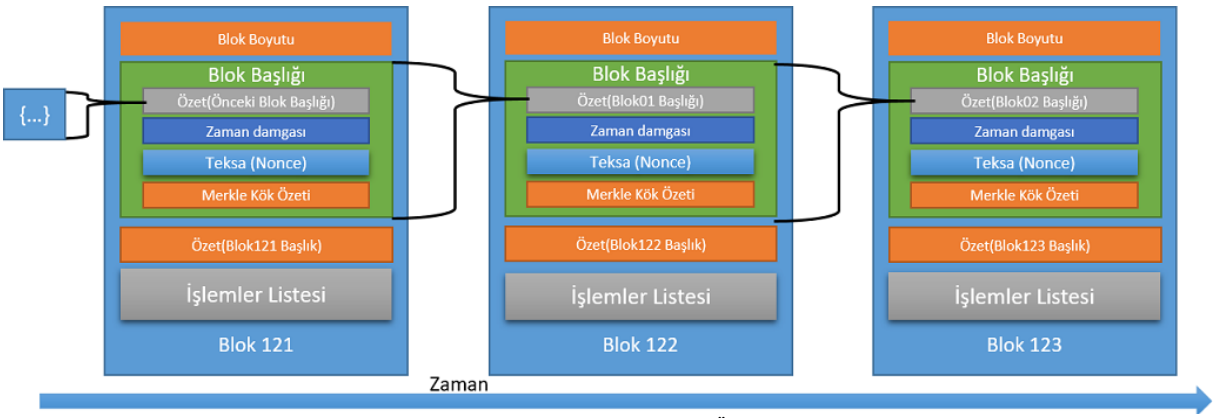
F. Blokzincirin Oluşturulması

Her blok, bir önceki bloğun başlığının özetini içererek önceki bloka bağlanarak, blokzincir oluşturulmaktadır (Bknz. Şekil 3). Daha önce yayınlanmış bir bloktaki herhangi bir işlem değiştirilirse, o bloğun farklı bir özet değeri oluşacaktır. Bu değişim, sonraki tüm blokların, önceki blok özetini içermesinden dolayı da farklı özet değerlerinin oluşmasına neden olur. Bu sebeple, sonraki tüm blokların tekrardan oluşturulması gerekmektedir.

III. MAHREMİYETİ İYİLEŞTİRME TEKNİKLERİ (PRIVACY IMPROVING TECHNIQUES)

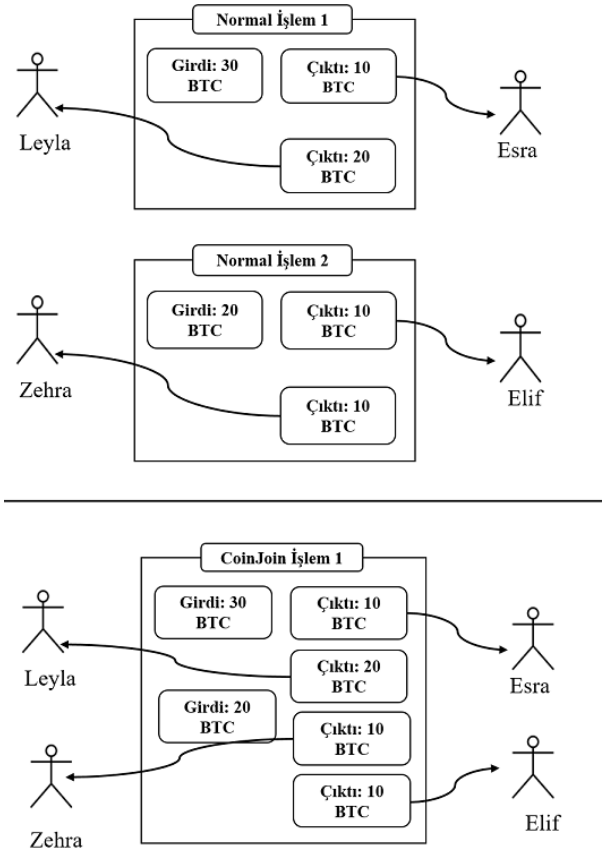
A. CoinJoin Protokolü

CoinJoin [10], birden fazla harcama yapandan gelen



Şekil 3. Bitcoin Blokzincir Örneği

birden fazla Bitcoin ödemesini tek bir işlemde birleştiren güvenilir bir yöntemdir ve dış alıcılar için hangi alıcı veya alıcıların kime ödeme yaptıklarını belirlemesini daha zor hale getirir. CoinJoin çalışma prensibi oldukça basittir. Esasen, CoinJoin birden fazla kullanıcının işlemlerindeki tüm girdi ve çıktılarını birleştirerek tek bir büyük işleme dönüştürür (Bknz. Şekil 4). Bu tek işlem ile farklı adreslerden farklı adreslere bitcoin transferi gerçekleştirilir.



Şekil 4. Örnek Bir CoinJoin İşlemi

Gönderici adreslerden hiçbiri direkt olarak alıcı adresleri belirlemediği için alıcı ve göndericiler arasında bağlantı kurulamamaktadır. Oluşturulan tek işlemdeki tüm katılımcılar gerçekleşecek transfer işlemini toplu halde imzaladıktan sonra işlem yayınlanır. CoinJoin'in önemli bir özelliği: işlem yayınlandığında ve blokzincire dahil edildiğinde, hangi bitcoinlerin nereye gittiğini bilmenin bir yolu yoktur; işlemin alıcıları bile, hangi adreslerden ödeme aldıklarını bilememektedirler.

Diğer birçok mahremiyet odaklı çözümlerinden farklı olarak, Coinjoin işlemleri için bitcoin protokolünde bir değişiklik yapılması gerekmemektedir. Bir CoinJoin işlemi oluşturmanın en kolay yolu özel bir sunucu oluşturmaktır. CoinJoin kullanmak isteyen herkes işlemin hangi giriş ve çıkışları içermesi gerektiğini göstermek için sunucuya bağlanır. Sunucu daha sonra büyük bir toplu işlem oluşturur ve bunu imzalatmak için tüm katılımcılara geri gönderir.

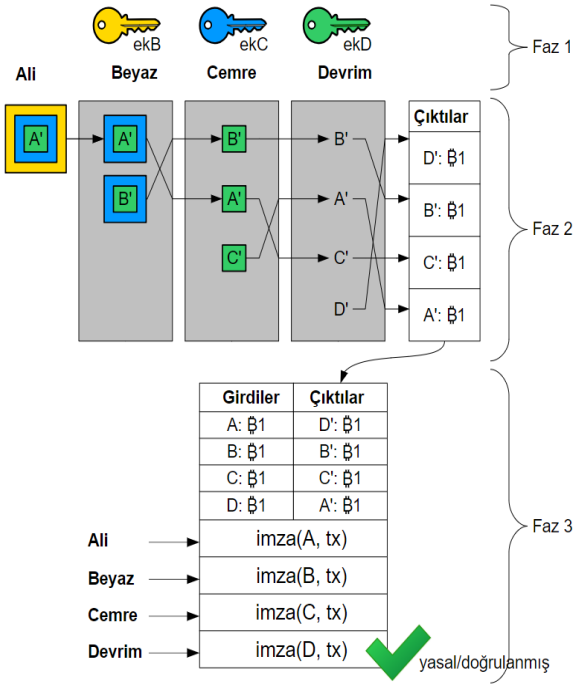
Sunucu tabanlı modelle ilgili temel sorun, sunucuyu her kim kontrol ederse tipik olarak bireysel katılımcılar tarafından sağlanan verilere erişebiliyor olmasıdır. Bu da mahremiyet probleminin hala tehdit altında olduğu anlamına gelmektedir. İşlem verilerini sunucudan bile kriptografik olarak maskelemek için potansiyel çözümler vardır, ancak bu şu an için hala teorik olarak görülmektedir.

Bu Yöntemin Kısıtları: CoinJoin yöntemi mahremiyet problemi için yararlı olabilirken mükemmel bir çözüm olarak görmek doğru değildir. En önemlisi, CoinJoin, girdi ve çıktıları karıştırırak harika bir iş çıkarırken, miktarlar açığa çıkarsa bu yeterli çözüm değildir. Örneğin, bir adres 3.9 bitcoin göndersin, başka biri 1.7 bitcoin göndersin, üçüncü biri 2.8 bitcoin göndersin ve bir çıktı 3.9 bitcoin alsın, başka biri 1.7 bitcoin alsın, üçüncü biri 2.8 bitcoin alsın. Böyle bir senaryoda girişleri çıkışlara bağlamak çok basit olacaktır.

Diğer bir risk ise Sybil saldırılarıdır. Görünüş bakımından, bir CoinJoin işleminde birden fazla katılımcı bulunmaktadır ama belirli bir katılımcıyı izleyen tek bir ve aynı varlık olabilir. Örneğin, 10 girişli bir CoinJoin işleminin 9'u aynı kişiye ait ise 10. kişinin kime bitcoin gönderdiğini her zaman takip edilir. Sybil saldırılarının çözümü için kolay bir çözüm yoktur, ancak daha akıllı kullanıcılar paralarını karıştırdıkça, başarılı bir şekilde ortaya çıkmaları daha da zorlaşmaktadır.

B. CoinShuffle Protokolü

CoinShuffle protokolü [11] basitçe anlatabilmek için dört katılımcılı Ali, Beyaz, Cemre ve Devrim ile küçük bir örnek düşünelim. Ali *A* adresine, Beyaz *B* adresine, Cemre *C* adresine ve Devrim *D* adresine sahip olsun. *A, B, C, D* adreslerinin her birinde tam olarak 1 BTC bulunmaktadır. Katılımcıların protokolü birbirleriyle çalıştırmak istediklerini ve birbirlerinin adreslerini önceden bildiklerini varsayalım.



Şekil 5. Basit Bir CoinShuffle İşlemi

Protokolün başında tüm katılımcılar yeni adresler A', B', C', D' oluştururlar, ancak bu adresleri birbirlerinden gizlerler. CoinJoin tabanlı karıştırma metodunun amacı, *A* ve *B, C, D* adresleri ve çıktı adresleri A', B', C', D' ile bitcoinler ve sahipleri arasındaki ilişkiyi gizlemek için tek bir karıştırma işlemi oluşturmaktır. Bununla birlikte, çıktı adreslerinin söz konusu A', B', C', D' düzenine sadık kalırsak, herkes A' ifadesinin *A*, B' ifadesinin *B*'ye ait olduğunu ve böyle devam ettiğini öğrenebilir. Bu yüzden, giriş ve çıkış adreslerinin bağlantısının gizlendiğinden emin olmak için çıktı adreslerinin listesinin karıştırılması gerekmektedir. Ancak sadece oluşturulan adreste çıktı adreslerini karıştırmak yeterli olmayacaktır. Örneğin, eğer herkes protokoldeki çıkış adreslerini ifşa ederlerse, yani Ali A' ifadesini açıklarsa, herkes A' ifadesinin Ali'ye ait olduğunu öğrenirdi. Bu yüzden, protokol sırasında gönderilen mesajların anonimliği bozmadığından emin olunması gerekmektedir. CoinShuffle tam olarak bu sorunu çözmektedir.

Protokolün aşağıdaki adımlardan oluşmaktadır [11] (Bknz. Şekil 5). Protokoldeki tüm mesajlar göndericisinin giriş adresine ait özel imza anahtarı kullanılarak imzalanır.

Faz 1: Anahtar değişimi: Her katılımcı (Ali hariç) bir genel şifreleme anahtarı ve *özel* şifre çözme anahtarı oluşturur. Açık şifreleme anahtarlarını ek_B, ek_C ve ek_D olarak adlandırıyoruz. Her katılımcı kendi açık anahtarını, açık adresine karşılık gelen *özel* anahtarı ile imzalar.

Faz 2: Karıştırma: Herkes genel şifreleme anahtarını öğrendiğinde, karıştırma işlemi başlayabilir:

- Ali, tüm şifreleme anahtarlarını katmanlı bir şekilde A' çıkış adresini şifreler. Yani Ali, Devrim için $Enc(ek_D, A')$ şifreyi oluşturur. Daha sonra bu şifreli metin Cemre için şifrelenir ve Beyaz $Enc(ek_B, Enc(ek_C, Enc\ (ek_D, A')))$ için şifreler. Bu ortaya çıkan mesaj Beyaz'a gönderilir.
- Beyaz mesajı alır, kendi şifresini çözer ve şunu elde eder $Enc(ek_C, Enc\ (ek_D, A'))$. Ayrıca, kendi adresinin bir şifrelemesini oluşturur ve $Enc(ek_C, Enc\ (ek_D, B'))$ elde eder. Artık Beyaz'ın A' ve B' içeren iki şifreli bir listesi var. Bob bu listeyi rastgele karıştırır, yani iki girişi değiştirir veya bırakır. Bob, karıştırılmış listeyi Cemre'ye gönderir $(Enc(ek_C, Enc(ek_D, B')), Enc(ek_C, Enc(ek_D, A')))$.
- Cemre aynı şeyi yapar: Listedeki iki girişi deşifre eder, kendi girişini ekler ve listeyi karıştırır $(Enc(ek_D, B'), Enc(ek_D, C'), Enc(ek_D, A'))$.
- Devrim yine aynısını yapar: B', C', A' elde ederek tüm kayıtların şifresini çözer. Kendi adresini D' ve listeyi karıştırır. Ortaya çıkan karıştırılmış listeyi herkese gönderir (D', B', C', A').

C. XIM Protokolü

XIM [12], bitcoin hırsızlığını önleyen dürüst karıştırıcılara dayanır ve DoS ve Sybil saldırılarına direnmek için ücrete dayalı bir reklam mekanizması kullanır. Bu protokolde, blokzincirine eklenen reklamlara dayalı olarak karıştırıcı ortaklarını anonim olarak bulmak için merkezi olmayan bir sistem bulundurmaktadır. Dışardaki hiç kimse, hangi katılımcıların kimler ile eşleştiğinin kanıtını bulamaz veya kanıtlarını doğrulayamaz. Bu saldırılara direnmenin yanında, tek bir

XIM kullanıcısı tarafından yapılan iptal, diğer kullanıcıların karışım yapmalarını engellemez. Bununla birlikte, XIM blokzincir üzerinde birden fazla işlem gerektirir.

Bu Yöntemin Kısıtları: Yalnızca iki katılımcı arasında bir karıştırma turu tamamlamak bile Bitcoin blokzincirde birkaç Bitcoin işlemi yayınlamayı gerektirir ve bunun gerçekleşmesi de saatler sürmektedir.

D. CoinShuffle++/DiceMix Protokolü

Bu çalışmada [13], iletilerini anonim olarak gönderen katılımcıların anonimliğini ve protokolün feshedilmesini sağlayan bir dizi iletiyi yayınlamalarını sağlayan DC-nets (Dining Cryptographers Network) ağlarına dayanan bir eşten eşe (Peer-to-peer, P2P) karıştırma protokolü olan DiceMix yöntemi sunulmaktadır. CoinShuffle++ protokolündeki anonimlik, DC-Net protokolünün geliştirilmiş hali olan DiceMix protokolü ile sağlanmaktadır. Bu protokoldeki dürüst olmayan katılımcıların sayısı f olması durumunda bu protokoldeki tur sayısı $4 + 2f$ olarak tanımlanır. Tüm katılımcıların dürüst olması halinde sadece 4 turda karıştırma sağlanmış olur. DiceMix sayesinde CoinShuffle'daki yoğun hesaplamalardan önemli derecede kurtarıldı. Örneğin, 50 tane katılımcının olması durumunda bu yeni protokolün toplam yükü 7-8 saniyeler mertebesine indirildi.

CoinShuffle++, karıştırma katılımcıları üzerinde herhangi bir güven varsayımı yapmaz, ancak en az iki dürüst katılımcının olması gerekir; bu durum anonimlik sağlayan herhangi bir protokol için temel bir gerekliliktir. XIM protokolünün aksine CoinShuffle++, Bitcoin blokzincirine eşlerin sayısından bağımsız olarak sadece tek bir işlem gönderilir.

Bu Yöntemin Kısıtları: Sybil ve hizmet engelleme saldırılarına karşı güvensizdir. Ayrıca, işlem miktarlarının gizli olduğu durumları desteklememektedir.

E. ValueShuffle Protokolü

ValueShuffle [14], bitcoin karıştırma hizmeti olan CoinJoin üzerine kurulmuştur ve işlemlerin ödeme değerlerini gizleyebilen gizli işlemlerle uyumlu ilk bitcoin karıştırma protokolüdür. Dahası, protokole aynı zamanda *gizli adresler* de ekleyerek, ödeme anonimliği, alacaklı anonimliği ve ödeme değeri gizliliğini garanti eden kapsamlı bir bitcoin gizlilik çözümü sunmaktadır.

ValueShuffle, mevcut kripto para karıştırma hizmetlerinin sınırlamalarına çözümler sunar. Örneğin, transfer işlemlerinde anonimliği sağlamak için aynı miktarda bitcoinleri karıştırmanın gerekliliği sınırlamalarını kaldırır. Bu protokol ayrıca, mevcut karıştırma hizmetleri fonlarının yeni bir adrese gönderilmesi gerektiği gibi ekstra işlem ücretleri ödemesini de ortadan kaldırmaktadır.

Bu Yöntemin Kısıtları: Sybil ve hizmet engelleme saldırılarına karşı güvensizdir.

F. Dandelion Protokolü

Bu protokol [15] ile uygulaması kolay ve en iyi anonimlik garantisine sahip olan Bitcoin ağının yeniden tasarlanmasını teklif edilmektedir. Bu prensiple, saldırgan tarafından elde edilebilecek maksimum bilgi kesinliği ve hatırlamayı en aza indiren dağıtık bir yayma protokolü önerilmektedir. Algoritmanın iki aşaması vardır: bir anonimlik fazı ve yayılma fazı. Bu çalışmada iki grafik önerilmektedir, bir anonimlik grafiği ve bir yayılma grafiği ve anonimlik grafiğini sık sık güncellenmektedir. Sık sık bu değişim, saldırganların grafiği öğrenmesini engellemektir. Ama bir saldırganın ne kadar hızlı bir şekilde grafiği öğrenebileceği açık değildir.

Bu Yöntemin Kısıtları: Bu protokolde, P2P grafik topolojisi hakkında sınırlı bilgiye sahip olan ve sadece düğüm başına bir işlemi gözlemleyen *dürüst ama meraklı* bir saldırgan olduğunu varsayar. Eğer saldırganlar bunun yerine kötü niyetliyse ve zamanla daha fazla bilgi toplarlarsa, anonimliği zayıflatabilmektedirler.

G. CoinParty Protokolü

CoinParty [16], Bitcoin için dağıtılmış karıştırma servisi için bir protokoldür. Bitcoin kullanıcıları, tüm günlük işlemlerinin Bitcoin'in blokzincirinde saydam olmasına rağmen finansal gizliliklerini korumak için fonlarını birleştirirler. Birleştirme ve karıştırma işlemi için eşler arasında Çoklu Güvenli Hesaplama Protokolleri (Secure Multi-Party Computation-SMC) koşturularak yapılmaktadır. Bu protokolde katılımcıların 1/3'üne kadar saldırgan olmasına tolerans gösterilmektedir. CoinParty, herhangi bir güvenilir üçüncü tarafın, yani bir hizmet sağlayıcının yokluğunda çalıştırıldığı için, herhangi bir karıştırma ücreti alınmamaktadır. Protokolde inkâr edemezliği de sağlamaktadır.

Bu Yöntemin Kısıtları: Hizmet engelleme saldırılarına karşı güvensizdir. Karıştırma süresi çok olmaktadır. Ayrıca, kısmi kripto para çalınma saldırısına maruz kalmaktadır.

H. MixCoin Protokolü

Bu protokolde [17], Bitcoin kullanıcıları, kripto paraların gönderileceği adres de dahil olmak üzere, güvenilir bir üçüncü taraf (Trusted third party, TTP) birlikte bir dizi parametre üzerinde anlaşırlar. Anonimlik sağlamak için, tüm kullanıcılar karıştırma sırasında aynı miktarda kripto para kullanmalı ve birden fazla kullanıcı aynı anda TTP kullanmalıdır. TTP, hizmetin kripto para çalması durumunda yayınlanabilecek imzalı bir garanti sunar. Mixcoin, Bitcoin ile uyumludur ve yeni şifreleme yöntemleri gerektirmemektedir. Merkezi bir karıştırma servisi olarak, hizmet engelleme saldırılarına karşı P2P

karıştırma protokollerine kıyasla tek kullanıcı tarafından korunmak daha kolaydır.

Bu Yöntemin Kısıtları: TTP kullanıcıların bitcoin'lerini çalabilir ve bu durum hırsızlık tespit edilebilir ancak önlenemez. Bu protokolde, TTP aynı zamanda girdi ve çıktılar hakkında bilgi sahibi olduğundan mahremiyeti ihlal edebilir.

I. BlindCoin Protokolü

Blindcoin [18], karışımın giriş ve çıkış adresini birbirine bağlayamadığından emin olmak için kör imzalar kullanarak Mixcoin'i geliştirmiştir. Yine de, karıştırılabilen kripto para miktarları her kullanıcıda hala aynı olma zorunluluğu bulunmaktadır ve anonimlik, eşzamanlı kullanıcıların sayısı ile doğru orantılıdır.

Bu Yöntemin Kısıtları: Transfer esnasında para çalınma durumu söz konusu olup tespit edilebilmektedir ama hala bu hırsızlık önlenememektedir. Diğer bir yandan anonim karıştırmada bekleme süresi çok fazla uzama durumu söz konusudur.

J. TumbleBit Protokolü

TumbleBit [19], Bitcoin'in karşı karşıya kaldığı iki büyük zorluğu çözmeyi, artan talebe ayak uydurmak için ölçekleme ve Bitcoin üzerinden yapılan ödemelerin gizliliğini koruma amaçlı anonim bir ödeme protokolüdür. TumbleBit, Bitcoin üzerine kurulu bir katman olarak uygulanır ve mevcut Bitcoin protokolünde değişiklik yapılmasına gerek yoktur. TumbleBit, RSA güvenlik varsayımlarını ve ECDSA standart güvenlik uygulamalarını kullanarak işlemlerde anonimliği sağlar.

Ayrıca Tumblebit'in blokzincirsiz (off-chain) yöntemi ile protokol, etkili bir şekilde ölçeklendirildiğini iddia etmektedir. Chaumian orijinal eCash protokolüne [20] benzer şekil de, TumbleBit, karıştırıcıda, Tumbler'ın bile hiç bir işlemin göndericisini alıcısına bağlayamamasını sağlayarak anonimleştirmeyi zorlar. 800 kullanıcıdan gelen ödemelerin karıştırılması, TumbleBit'in güçlü anonimlik ve hırsızlığa karşı dayanıklılık sağladığı ve ölçeklenebilir olduğunu göstermektedir.

Bu Yöntemin Kısıtları: Yüksek seviye anonimliği sağlaması iyi bir karıştırıcı olduğunu gösterirken bu işlemlerin gerçekleşme süresi çok uzun olabilmektedir.

IV. SONUÇ VE DEĞERLENDİRME (CONCLUSION AND EVALUATION)

Bitcoin, önceki yaklaşımlara göre çeşitli avantajlara sahip bir kripto para birimidir. İşlemler bir blokzincir'de eşler arası bir ağ tarafından onaylanır ve düğümler tarafından saklanır. Tam düğümler tüm işlem verilerini tutarken hafif düğümler sadece işlem başlıklarını saklarlar. Bu nedenle, yapılan tüm işlemler herkese açıktır ve tarafların mahremiyeti ihlal edilmiş olur. Bitcoin ile yapılan işlemlerin parasal değerinin çok büyük olması saldırganların bu sisteme olan merakını arttırmaktadır ve yapılan işlemlerin anonimliğin sağlanması önemli olmaktadır. Bu nedenle, Bitcoin'de işlemlerin anonimliğini sağlamak için pek çok farklı çözümler sunulmuştur. Bu çözümlerin çoğu, güvenilir bir üçüncü tarafa gereksinim duymaktadır veya Bitcoin'de değişiklik yapmak gibi bir takım olumsuzluklarla birlikte gelir. Bu makalede, sunulan bu çözümler incelenmiş olup herbir çözümün kendine özgü üstünlükleri ve kısıtları verilmiştir. Elde edilen bulgular özetle Tablo 3'te verilmiştir. Bulgularımıza dayanarak, Bitcoin'i anonimleştirmek için en iyi yaklaşımın hangisi olduğunu beklenen mahremiyet seviyesi ve diğer saldırıların ne derece önemli olup olmadığı belirleyecektir.

V. KAYNAKLAR (REFERENCES)

[1] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, (Erişim: 6 Haziran 2018).

[2] G. O. Karame, E. Androulaki, and S. Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security,* CCS'12, pp.906-917, New York, NY, USA, 2012. ACM.

[3] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. In *Proceedings of the 24th USENIX Conference on Security Symposium,* SEC'15, pp.129-144, Berkeley, CA, USA, 2015. USENIX Association.

[4] C. Decker and R. Wattenhofer. Bitcoin transaction malleability and mtgox. In *19th European Symposium on Research in Computer Security – Vol.8713,* ESORICS 2014, pp.313-326, Springer-Verlag, New York, NY, USA, 2014.

[5] M. Apostolaki, A. Zohar, and L. Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP),* pp.375-392, May 2017. San Jose, CA, USA

[6] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. *Financial Cryptography,* Vol.8437 of *Lecture Notes in Computer Science,* pp.436-454. Springer, 2014. Barbados

[7] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. *FC 2016: Financial Cryptography and Data Security,* pp.515-532, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.

[8] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *2016 IEEE European Symposium on Security and Privacy (EuroS P),* pp.305-320, March 2016. Saarbrucken, Germany

[9] I. Eyal. The miner's dilemma. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy,* SP'15, pp.89-103, Washington, DC, USA, 2015. IEEE Computer Society.

***Tablo 3**. Bitcoin'de Anonimleştime Yöntemleri*

Anonim Yöntemi	Özellikler	Üstünlükler	Kısıtlar
CoinJoin	Gizliliği artırmak için çoklu imza işlemleri kullanma	Hırsızlık önleme, düşük transfer ücreti	Hizmet engelleme saldırısına ve Sybil'e karşı güvensiz, anonimlik katılımcı sayısı ile orantılı
CoinShuffle	Bir şifreleme karıştırma protokolü aracılığıyla CoinJoin işlemlerini koordine etmek için merkezi olmayan bir yapıda olma	Hırsızlık önleme, hizmet engelleme saldırısına karşı güvenli	Sybil saldırısına karşı güvensiz, düşük anonimlik seviyesi
XIM	Anonim ortaklık ve çoklu karıştırma gerçekleştirme.	Sybil ve hizmet engelle saldırısına karşı güvenli	Yüksek karıştırma zamanı
CoinShuffle++	Kripto-para birimlerinde anonimliği geliştirmek için CoinJoin kavramına dayanan P2P karıştırma çözümüne sahip olma	Düşük karıştırma süresi, gönderici anonimliği, güvenli bitirme	Hizmet engelleme saldırısına ve Sybil'e karşı güvensiz, ölçeklenme sorunu
ValueShuffle	CoinShuffle++ çözümüne dayanan, gizli işlemler ile karıştırma yaklaşımı içerme.	Hırsızlık önleme, normal transfer	Hizmet engelleme saldırısına ve Sybil'e karşı güvensiz, ölçeklenme sorunu
Dandelion	Anonimliği sağlamak için ağ oluşturma politikasına sahip olma	Birden fazla saldırgan karşısında güçlü anonimliği sağlama	Hizmet engelleme saldırısına ve Sybil'e karşı güvensiz
CoinParty	CoinJoin kavramına dayanarak, eşik ECDSA ve şifre çözme karışımlarını kullanır.	Karıştırma ücreti yok, anonimliği sağlama	Yüksek karıştırma süresi, hizmet engelleme saldırısı, hırsızlığı engelleyememe
MixCoin	Güvenilir üçüncü taraf ile anonimlik sağlama	Sybil ve hizmet engelle saldırısına karşı güvenli	Hırsızlığı engelleyememe, mahremiyetin ihlal edilmesi
BlindCoin	MixCoin kavramına dayanma ve anonimlik sağlamak için kör imza şemasını kullanma	Sybil ve hizmet engelle saldırısına karşı güvenli	Kısmi olarak hırsızlığı engelleyememe, karıştırmalarda bekleme süresinin uzaması
TumbleBit	Güvenilmeyen bir arabulucuyu kullanarak anonimlik sağlama	Hırsızlığı engelleme, Sybil ve hizmet engelle saldırısına karşı güvenli	Normal transferlerde en az iki tane işlem gerektirmesi, işlemlerin gerçekleşme süresinin uzun olması

[10] G. Maxwell. Coinjoin: Bitcoin privacy for the real world, https://bitcointalk.org/index.php?topic=279249.0, (Erişim: 6 Haziran 2018)

[11] T. Ruffing, P. Moreno-Sanchez, and A. Kate. Coin-shuffle: Practical decentralized coin mixing for bitcoin. In Miroslaw Kutylowski and Jaideep Vaidya, editors, *Computer Security - ESORICS 2014,* pp.345-364, Cham, 2014. Springer International Publishing.

[12] G. Bissias, A. Pinar Ozisik, Brian N. Levine, and M. Liberatore. Sybil-resistant mixing for bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society,* WPES'14, pp.149-158, New York, NY, USA, 2014. ACM.

[13] T. Ruffing, P. Moreno-Sanchez, and A. Kate. P2p mixing and unlinkable bitcoin transactions. Cryptology ePrint Archive, Report 2016/824, 2016.

[14] T. Ruffing and P. MorenoSanchez. Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin. In *Financial Cryptography and Data Security,* pp.133-154, Cham, 2017. Springer International Publishing.

[15] S. B. Venkatakrishnan, G. Fanti, and P. Viswanath. Dandelion: Redesigning the bitcoin network for anonymity. *Proc. ACM Meas. Anal. Comput. Syst.,* 1(1):22:1- 22:34, June 2017. New York, NY, USA

[16] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle. Coinparty: Secure multi-party mixing of bitcoin. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy,* CODASPY'15, pp.75-86, New York, NY, USA, 2015. ACM.

[17] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for bitcoin with accountable mixes. *Financial Cryptography and Data Security*, pp. 486-504, 2014. Springer, Berlin, Heidelberg.

[18] L. Valenta and B. Rowan. Blindcoin: Blinded, accountable mixes for bitcoin. *Financial Cryptography and Data Security,* pp.112-126, 2015. Springer, Heidelberg

[19] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. Cryptology ePrint Archive, Report 2016/575, 2016.

[20] D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology,* pp.199-203, Boston, MA, 1983. Springer, Boston, MA.