Avrupa Bilim ve Teknoloji Dergisi
Sayı 27, S. 292-302, Kasım 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No.27, pp. 292-302, November 2021

Research Article

Blokzincirde Anonim ve Devredilemez Biyometrik Dijital Kimlik

Neyire Deniz Sarier*

B-IT, Cosec, Bonn, Almanya, (ORCID: 0000-0003-2129-0222), denizsarier@yahoo.com

(İlk Geliş Tarihi: 20 Mart 2021 ve Kabul Tarihi 23 Ağustos 2021)

(**DOI:** 10.31590/ejosat.896960)

ATIF/REFERENCE: Sarier, N. D. (2021). Blokzincir Tabanlı Anonim ve Devredilemez Biyometrik Dijital Kimlik. *Avrupa Bilim ve Teknoloji Dergisi*, (27), 292-302.

Öz

2017 yılında Augot et al. tarafından Bitcoin Blokzinciri üzerinde ilk kullanıcı odaklı Kimlik Yönetimi sistemi tanımlanmıştır. Ancak Bitcoin kripto para birimi anonim değildir, dolayısıyla mahremiyeti saglamamaktadır. Bu nedenle, kimliği oluşturan unsurlardan biri olan biyometrik verilerin mahremiyeti sağlayan bir platformda ve şifreli olarak yönetilmesi gereklidir. Böylelikle hem devredilemezlik özelliği sağlanmış olacak, hem de kişisel verilerin en başında gelen hassas biyometrik veriler kriptografik yöntemler ile korunarak, anonim şekilde işlem görücektir. Esasen, bu özellikleri sağlayan ilk anonim biyometrik tanımlama sistemi, 2018 yılında Zerocoin blokzinciri üzerinde tasarlanmıştır. Bu sistemde biyometrik veriler (parmak izi, yüz, iris) şifreli olarak blokzincirde tutulmakta, kullanıcıdan bir servise erişim amaclı kimlik tanımlama talebi geldiğinde, biyometrik tanımlama madenciler tarafından şifreli alanda yapılmakta ve bir eşleşme bulunduğunda sonuç blokzincire kayıt edilir. Özetle, anonim transferler ile, servis saglayıcılar anonim biyometrik tanımlama işlemini tamamlayarak kullanıcının talep ettiği erişim iznini sağlarlar. Bu araştırma makalesinde, Zerocoin ile birlikte güncel diğer anonim kripto para birimleri olan Zerocash ve Monero analiz edilerek, biyometrik verilere dayalı dijital kimlik yönetim sistemlerinde performans ve mahremiyet açısından daha iyi çözümlerin mevcut olup olmadığı incelenecektir. Bu inceleme sırasında önce anonim kriptoparalara ait blokzincirler üzerinde biyometrik tanımlama uygulaması, akabinde bu uygulama üzerinde basit bir modifikasyon ile anonim dijital kimlik yönetimi sistemi elde edilecektir. Son olarak bu çözümlerden en az maliyetli olanı, analiz edilen anonim kripto para sistemleri karşılaştırılarak tespit edilecektir. İlk sonuçlara göre, Cryptonote tabanlı Monero en uygun sistem olup, gelecekte daha yüksek güvenlik sağlayan RingCT tabanlı sistemler de değerlendirilecektir.

Anahtar Kelimeler: Blokzincir, Biyometri, Mahremiyet, Anonimlik, Dijital Kimlik, Bitcoin, Zerocoin, Zerocash, Monero

Anonymous and Non-transferable Biometric Digital ID on Blockchain

Abstract

The first user centric Identity Management system on the Bitcoin Blockchain was introduced in 2017 by Augot et al. However, Bitcoin is not an anonymous cryptocurrency, therefore, privacy is not guaranteed. Hence, one aspect of the identity, namely biometrics should be processed in a privacy preserving manner and as encrypted. This way, non-transferability is guaranteed in addition to the anonymous processing of the most important personal identifier, namely sensitive biometric data. In fact, the first anonymous biometric identification system that guarantees these notions was described in 2018 on top of Zerocoin protocol. In this system, biometric data (fingerprint,face, iris), are stored as encrypted on the Blockchain. If there is an incoming identification request from the user to access a service, the biometric matching is performed by the nodes/miners in the encrypted domain and if a match is found, it is recorded on the Blockchain. In summary, through anonymous transfers, service providers complete the anonymous biometric identification procedure and provides the necessary access to the service. In this research article, we evalute recent privacy coins of Zerocash and Monero in addition to Zerocoin, and examine whether there exists better solutions in biometric based Identity Management systems with respect to efficiency and privacy. First, we describe anonymous biometric identification/authentication systems based on anonymous cryptocurrencies and then we modify them slightly to obtain anonymous Digital ID. Finally, we compare the analyzed privacy coins in order to find the cheapest solution. Initial results show that Cryptonote based Monero provides the most ideal system, leading to the evaluation of RingCT based systems guaranteeing a higher security level.

Keywords: Blockchain, Biometrics, Privacy, Anonymity, Digital ID, Bitcoin, Zerocoin, Zerocash, Monero

* Sorumlu Yazar: denizsarier@yahoo.com

1. Giriş

Blokzincir teknolojisi, verilerin haricinde değer atfettiğimiz varlıkları da transfer etmemizi sağlayan dağıtık bir veritabanıdır. Satoşi Nakamoto lakaplı gizli bir yazarın 2008 yılında önerdiği Bitcoin dijital parası (Nakamoto, 2008) ile birlikte dünyada yeni bir uluslararası para biriminin varlığından bahsedilmeye başlandı. Bitcoin, başlangıçta sadece kripto para olarak algılanmış, ancak sonradan Bitcoin'in dayandığı Blokzincir teknolojisinin daha genel kullanım alanları olabileceği farkedilmiştir. En genel ifadeyle, blokzincir, merkezi bir sunucunun veya güvenilir bir otoritenin kaldırılmasına olanak sağlayarak, merkezi güvenin internet ortamında dağıtılmasına denir. Blokzincir teknolojisi yaygın olarak Bitcoin ve Ethereum gibi sanal paraların altındaki teknoloji olarak bilinmektedir. Fakat bu teknoloji sağladığı olanaklar ve çeşitlendirilebilir uygulamaları ile çok daha geniş bir yelpazeye sahiptir (BZLab, 2021). Blokzincir ile alakalı tüm akademik araştırmaların yaklaşık % 80'i Bitcoin odaklıdır. Çalışmaların %20'si ise akıllı kontratlar dahil olmak üzere yeni blokzincir uygulamalarına odaklanmıştır. Bu çalışmalar, ileri kriptografi mekanizmaları (özet fonksiyonlar (hash functions), dijital imza), açık anahtar altyapısı (asymmetric cryptography), taahhüt şemaları (commitment schemes), sıfır bilgi protokolleri (zero knowledge protocols), dağıtık sistemleri ve oyun kuramını araç olarak kullanır (BZLab, 2021).

Bitcoin (BTC) ve Blokzincir: Ideal bir dijital para 3 özellikle betimlenir: Birincisi, tamamen merkezsizleşmiş, yani bankanın olmadığı, ikincisi, güvenlidir, yani taklit edemez ve üçüncüsü ise mahremiyetin sağlanmasıdır, diğer bir deyişle dijital parayı anonim olarak kullanabilirsiniz, işlemlerinizi takip eden insanlar için endişelenmenize gerek kalmaz. Bitcoin, sistemdeki oyuncuların (miners yani madenciler) çoğu dürüst davrandıkları sürece işe yaramaktadır.

Bir bankamız olduğunu varsayalım ve Alice (A), Şekil 1' deki 0.32 BTC değerindeki çeke sahip olsun. Alice (A), Bob'a (B) bu çeki göndermek istiyor. Alice çeki ters çevirir ve arka tarafına "Bu çek Bob'a ödenecektir" yazarak imzalar. Alice'in imzası kimliğini doğrulamak içindir. Bu çekin önü ve arkasını kontrol eden herhangi bir kişi, imzaları kontrol eder ve Bob'un gerçekten bu çeke sahip olduğundan emin olur. Bu sayede, artık bu belirteçleri (token) bir kişiden diğerine aktarabilen bir mekanizmaya sahibiz. Aynı işlemi elektronik olarak yapmak için, Alice'in adını Alice'in açık anahtarı (public key) ve Alice'in ıslak imzasını ise dijital imzası ile değiştirmek yeterlidir. Özetle banka çeki artık bir dosya olmuş ve eğer ilk dosyaya güvenirsek, dijital imzalar kullanarak zincirleme sahiplik transferleri yapabiliriz. Benzer şekilde Bob (B) aynı çeke biraz daha fazla bilgi ekleyip imzalayarak Charli'ye (C) 0.23 BTC değerinde ödeme yapabilir. Para üstü olan 0.98BTC 'yi ise, Bob kontrol ettiği başka bir Bitcoin adresine (D) gönderir. Bitcoin'deki dijital imza, asimetrik anahtar şifreleme sistemine dayanır. (*pk; sk*) asimetrik bir anahtar ikilisi olsun, *pk* açık anahtarı (public key), *sk* gizli anahtarı (secret key) ifade eder ve bu iki anahtar birbiri ile matematiksel olarak ilişkilidir. Standart kriptografik imzalarda, *sk* gizli anahtarı kullanılarak atılan bir imza *pk* açık anahtarı kullanılarak doğrulanır. Yani, imzanın doğrulanabilmesi için hangi açık anahtarın kullanılacağının bilinmesi gerekir. Asimetrik şifrelemede açık anahtarın kamu ile paylaşılmasında mahsur bulunmazken, özel anahtarın sadece sahibi tarafından bilinmesi gerekir. Bir veriye (olayımızda çek) elektronik imza atarken, o verinin özeti (hash) gizli anahtar ile şifrelenir. Veri ve imza paylaşılır. Sistemdeki herhangi bir kişi (olayımızda madenciler) ilintili açık anahtar ile imzanın doğruluğunu kontrol eder.

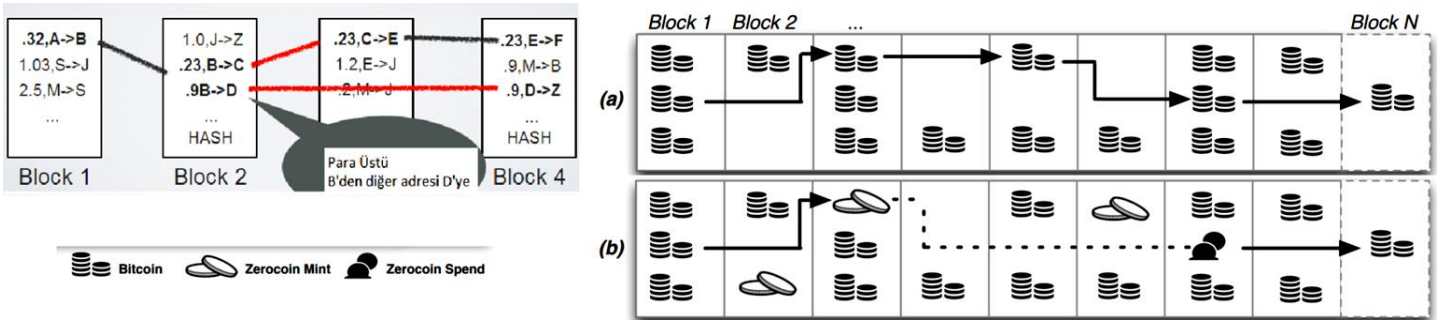
Çifte harcama sorunu (Double Spending). Bu sorun Alice'in aynı çeki alarak iki kopyasını çıkarıp, birini Bob'a, diğerini ise Charlie'ye göndermesidir. Bu sorun, ağdaki tüm harcamaları takip eden merkezileştirilmiş bir veritabanımız olduğunu varsaydığımızda kolayca çözülebilir. Alice, Bob'a transfer yaptığında, bu havale veritabanında kayıtlı olur, böylece Bob aynı çekin daha önce transfer edilip edilmediğini kontrol edebilir ve çift harcama önlenir. Fakat bu yaklaşımla merkeziyetçi olmayan bir sisteme sahip olamayız. Bitcoin bunu dağıtılmış bir fikir birliği yaklaşımıyla çözer. Merkezi bir veritabanı yerine bu veritabanını böler ve peer-to peer (P2P) ağda aynı bilgiyi çoğaltan birçok farklı taraf yer alır. Herkesin veritabanı hakkında aynı görüşe sahip olması, veritabanının güncellenmesi ve yeni blokların oluşması, emeğin ispatı anlamına gelen proof-of-work yaklaşımı ile çözülmektedir. Madenciler, tüm bu işlemleri yaparken kriptografik hesaplamaların zorluğunu arkasına alarak harcanan emeğin bir varlık/emtia/değer olmasını sağlamaktadır (BZLab, 2021).

1.1. Literatür Taraması

Giriş bölümünde de ifade edildiği gibi, Bitcoin, başlangıçta sadece kripto para olarak algılanmış, ancak sonradan Bitcoin'in dayandığı Blokzincir teknolojisinin daha genel kullanım alanları olabileceği farkedilmiştir. Bunlardan en güncel uygulama alanı Dijital Kimlik, diğer bir deyişle, Blokzincir tabanlı kimlik yönetimi uygulamasıdır. 2017 yılında, Bitcoin blokzinciri üzerinde ilk kullanıcı odaklı dağıtık kimlik yönetim sistemleri (Augot et al., 2017a,b) tanımlanmıştır. Sistemdeki farklı partiler (Augot et al., 2017a) Bitcoin transferleri ile haberleşir. Böylece, Kimlik sağlayıcılar (*IP*) sistem için gerekli altyapıyı Bitcoin ağından temin ederek, madencilerin emeği sonucunda, verilerin bütünlüğünü garanti ederler. (Othman and Callahan, 2018) sistemindekine benzer şekilde, (Augot et al., 2017a) kimlik verilerini taahüt şeması kullanarak blokzincirde tutar, ve ilgili sıfır bilgi ispatlarını blokzincir dışında tutar, ya da ispatların tutulduğu link bilgisini kimlik doğrulama transfer işleminin extra bölümünde (`OP_RETURN`) belirtir.

Diğer taraftan, biyometrik verilere dayalı kimlik tanıma uygulamaları 2015 yılında başlamıştır. Örneğin, CryptID (CryptID, 2018) girişimi şifreli parmak izine dayalı kişi tanımlama verilerini Factom blokzincirinde tutarak, parmak izi tanımlama sistemlerinde yer alan geleneksel merkezi sunucuyu elimine eder. (Othman and Callahan, 2018) projesi ise biyometri tabanlı kimlik üzerine inşa edilmiştir ve merkezi olmayan tanımlayıcı (DIDs) ve kişi egemen kimlik konseptini blokzincir tabanlı olarak tasarlamıştır. Biyometrik şablon'un (template) parçaları, blokzincir dışı (off-chain), i.e. Dropbox, Google drive gibi platformlara dağıtılarak, blokzincir aracılığıyla bu platformlardan güvenli şekilde referans edilir. Biyometrik kimlik verilerine dayanan diğer blokzincir tabanlı biyometrik tanımlama/doğrulama ve kimlik yönetim sistemleri (Toutara and Spathoulas, 2020; Zhou et al., 2018; Liu et al., 2019; Augot et al., 2019; Bernabe et al., 2019; Lesavre et al., 2019; Sarier, 2021) yayınlarında yer almaktadır.

Şekil 1: Blokzincir'de tersine anonimleştirme ve (a) Bitcoin blokzinciri: Her transfer önceki transferle bağlantılıdır (b) Zerocoin blokzinciri (Miers et al., 2013) (mint) basılan ve harcanan (spend) zerocoinler arasındaki bağlantı (kesik çizgi ile gösterilen) blokzincir transfer tarihçesinden anlaşılamaz.



(Augot et al., 2017a) de tanımlanan kimlik yönetim sistemi kimlik işlemlerinin bağlantısızlığını sağlamak için farklı bitcoin adresi kullanmasını zorunlu kılar. Ancak yukarıdaki örnekte gözlemlediğimiz üzere Bitcoin transferleri tersine anonimize edilebildiğinden, ancak mahremiyeti sağlayan kripto paralar üzerinde kurulacak kimlik yönetimi sistemleri kişisel mahremiyeti sağlayacaktır. Nitekim bu özellikleri sağlayan ilk biyometrik kimlik saptama sistemi (Sarier, 2018) 2018 yılında Zerocoin blokzinciri üzerinde tasarlanmıştır. Bu sistemde biyometrik veriler (parmak izi, yüz, iris vs.) şifreli olarak blokzincirde tutulmakta, kullanıcıdan bir servise erişim amaclı kimlik saptama talebi geldiğinde, kimlik eşleşmesi madenciler tarafından şifreli alanda yapılmakta ve eşleşme bulunduğunda sonuç blokzincire kayıt edilir. Sonuçta, anonim transferler ile, servis sağlayıcılar anonim biyometrik eşleşmeyi tamamlayarak kullanıcının talep ettiği erişim iznini sağlarlar. Zerocoin (Zcoin) (Miers et al., 2013), Zerocash (ZEC) (Sasson et al., 2014) ve Monero (XMR) (van Saberhagen, 2013) kullanıcı anonimitesini sağlayarak bu sorunu çözebilecek mevcut platformlardır.

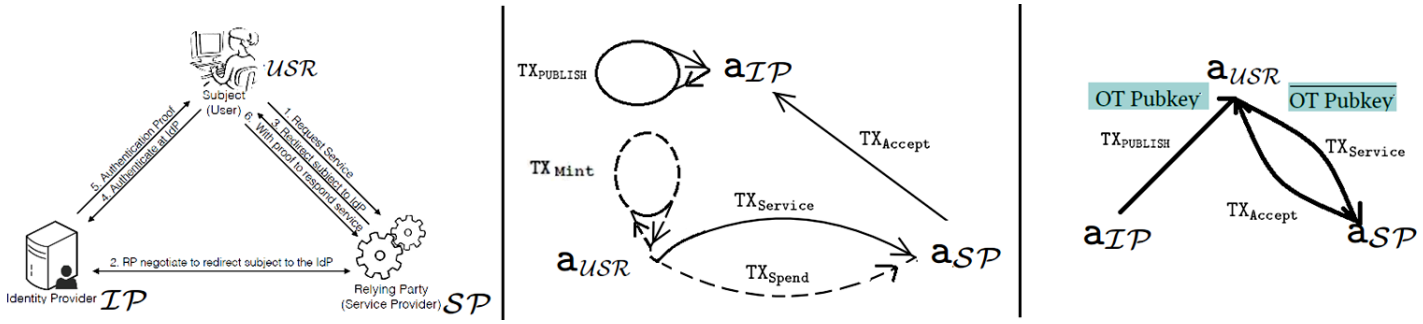
1.2. Motivasyon ve Katkı

2012 yılına kadar çıkan kripto paralar, gizlilik ve mahremiyet gibi özelliklere sahip değildi. Örneğin Bitcoin'de bir adresin yapmış olduğu işlemlerin izlenebilmesi Şekil 1'de görüleceği üzere mümkündür. Gizlilik söz konusu olduğunda Bitcoin'in yapısında bazı içsel kusurlar vardır. Bunun en iyi örneği, 'çift harcama' (double spending) olarak bilinen problemi çözme yönteminin, tüm Bitcoin işlemlerini bir kamu muhasebesinde depolamaktır. Bu, her işlemin gizliliğini feda ederek görünür olduğu anlamına gelir. Ayrıca, birçok çalışma Bitcoin'in ağ topolojisini analiz etmek için çeşitli teknikleri kullanabileceğinizi göstermiştir. Aslında, bunlar sosyal ağ topolojisini analiz etmek için kullanacağınız aynı yöntemlerdir, bu da birçok kişinin bunlara aşina olduğu anlamına gelir.
Herkes, kayıt defterine (ledger) erişebildiğinden, mahremiyet yoktur. Bu durumun önüne geçebilmek amacıyla her transfer için başka adres (pseudonym) kullanılması, transferlerin karıştırma servisleri aracılığıyla yapılması gibi yöntemler önerilmiş olsa da, önerilmiş olan yöntemler hem tam bir çözüm getirmemekte hem de sisteme ekstra yük bindirmektedirler. Kullanıcılar, mahremiyetlerini artırmak için birçok kimlik (pseudonyms) kullanabilirken, işlem grafiğinin yapısı, işlemlerin değeri ve tarihleri gibi blok zincirindeki bilgiler kullanılarak Bitcoin tersine anonimleştirilebilir.

Bu makalede transfer tutarını da gizleyen komplike çözümler yerine, yalnızca kullanıcıları anonimleştiren sistemlere odaklanılacaktır. Her ne kadar 2018 yılında Sarier tarafından yazılan ilk anonim biyometrik eşleşme sistemi ile analize başlansa da, tasarlanan Zerocash ve Monero tabanlı sistemler, biyometrik eşleşmenin ötesinde, biyometrik veriye dayalı kimlik güven belgelerinin yönetimi olarak genelleştirilecektir. Bu nedenle, Önbilgi bölümünde kimlik güven belgesi ve bu belgeye fuzzy extractor yapı taşı kullanılarak biyometrik verinin eklenmesi konuları kısaca ele alınacak ve bu konudaki bir örnek uygulama (Şekil 3) sunulacaktır. Daha sonra Şekil 3'de yer alan ve Bitcoin tabanlı olması nedeniyle sadece transfer edilemezlik özelliğini taşıyan kimlik yönetim sistemi, Zerocoin, Zerocash ve Monero anonim kripto para sistemleri üzerinde yeniden tasarlanacaktır. Böylece, KVKK (Kişisel Verilerin Korunması Kanunu) dikkate alınarak anonim ve transfer edilemez dijital kimlik yönetim sistemleri her bir kullanıcı açısından gerekli transfer sayısı, toplam transfer maliyeti, ölçeklenme konularında analiz edilecektir.

Zerocoin tabanlı biyometrik eşleşme sisteminde olduğu gibi, yeni tasarlanan blokzincir tabanlı anonim kimlik tanımlama sistemlerinde transfer tutarı sembolik değerde ve önemdedir. Esas amaç, biyometrik tabanlı kimlik tanımlama işleminin anonim şekilde yapılmasıdır. Zerocoin (Miers et al., 2013), Zerocash (Sasson et al., 2014) ve Cryptonote bildirisinde yer alan şekliyle Monero (van Saberhagen, 2013) kullanıcı anonimitesini sağlayarak bu sorunu çözebilecek mevcut platformlardır. Her üç sistemin avantaj ve dezavantajları değerlendirilmeli, kimlik tanımlamaya olanak tanıyacak ekstra bilgi alanlarının mevcut olup olmadığı, betiklerinin tasarlanacak sistemle uyumu, sembolik transfer miktarının dışında, her bir transfer işlemi karşılığı madencilerin aldığı komisyon tutarı (fee) karşılaştırılmalı, ve mahremiyeti en yüksek seviyede, en az komisyon tutarıyla, en hızlı transfer onaylama ve her bir transferin gerektirdiği matematiksel hesap ve kB miktarını minimum tutarak ölçekleme sorununu en aza indirgeyen çözüm bulunmaya çalışılmalıdır. Bu esaslar çerçevesinde, her üç yeni tasarım transfer ücretleri, transfer büyüklüğü, ve işlemlerin sonuçlanması açılarından değerledirilip, karşılaştırmalı olarak sunulacaktır. Sonuç bölümün de ise gelecek çalışmalar hakkında öngörüler sunularak makale sonlandırılacaktır.

Şekil 2: Geleneksel (Zhu and Badr, 2018) ve Blokzincir tabanlı (Augot et al., 2017a, 2019; Sarier, 2018) kimlik yönetimi: Kesik çizgili transferler (Sarier, 2018)'e mahsustur. Son grafik Bölüm 3'de tasarlanan Monero tabanlı kimlik yönetim sistemini temsil eder.



2. Materyal ve Metot

2.1. Önbilgi: Brands DLRep Şeması

Brands DLRep şeması (Brands, 2000), $n-1$ alanlı bir kimlik için $(X_1, ..., X_{n-1})$, seçmeli olarak açık edilen dijital kimlik sistemlerinin temelinin oluşturan bir kriptografik yapıtaşıdır. Burada, q bir asal sayıyı ve $\mathbb{G}$ ise grubu temsil eder, Bitcoin imza protokolündeki grup ile aynı grup temel alınabilir (Augot et al., 2017a,b).

Credential (Kimlik Güven belgesi) oluşturulması: $g_0, g_1, ..., g_n \in \mathbb{G}$ olarak seçilir. Burada X_0 alanı, bir saldırganın diğer kimlik alanlarına $X_j$ler ilişkin veriler hakkında öncelikli bilgi edinmesini önler (Augot et al., 2017b). $(X_0, X_1, ..., X_{n-1}) \in \mathbb{Z}_q^n$ veri grubu, $h = \prod_{j=0}^{n-1} g_j^{X_j}$ verisinin $(g_0, g_1, ..., g_{n-1})$ bağlamında/tabanında DLRep yapıtaşı olarak adlandırılır.

Credential (Kimlik Güven belgesi) gösterilmesi: Gösterim protokolü, bir kullanıcıdan kanıtlanması talep edilen bazı kullanıcı kimlik verilerinin, talep edilmeyen diğer kullanıcı kimlik verilerini açık etmeden, yani sıfır bilgi kanıtı (zero knowledge proof) yöntemi kullanılarak, kullanıcı tarafından ilgili merciye gösterilmesidir. İspat, ancak akıllı kartta saklanan taahüt edilmiş Kimlik Güven belgesindeki veriler ile aynı olursa yapılabilir. Bir doğrulayıcıya h verisinin DLRep'i kanıtlanırken , ispatlayan aşağıda sıralanan protokol adımlarını işleme koyar (Brands, 2000). (j, X_j) açık edilen kimlik verilerini ifade eder ve bu veriler $j \in D \subseteq \{1, ..., n-1\}$ tüm kimlik alanlarına ait index kümesinin bir alt kümesidir. Böylece gizli kalması istenen kimlik alanları $C = \{1, ..., n-1\} \backslash D$ terimi ile ifade edilir.

DL taahütlerinin çarpımları gerek gizli kalan gerek açık edilen kimlik verileri için aşağıdaki şekilde temsil edilir. $h^C = \prod_{j \in C} g_j^{X_j}$ ve $h^D = \prod_{j \in D} g_j^{X_j}$ ve $h = g_0^{X_0} h^C h^D$. $j \in D$ için (j, X_j) ile temsil edilen kimlik verileri gerek ispatlayan $\mathcal{P}$ ve gerekse $\mathcal{V}$ tarafından bilindiğinden, her iki aktör de h^D verisini hesaplayabilir.

Aşağıdaki protokol bir doğrulayıcı $\mathcal{V}$'e, $H = h(h^D)^{-1} = g_0^{X_0} h^C$ verisinin DL değerini g_i'lar bağlamında/tabanında ispatlar. Burada $i \in C$ değerleri sadece ispatlayacı $\mathcal{P}$ tarafından bilinir.

1) İspatlayan $\mathcal{P}$ rastsal ve gizli $a_0 \in \mathbb{Z}_q, a_j \in \mathbb{Z}_q$ sayılarını $j \in C$ için üretir. $A = g_0^{a_0} \prod_{j \in C} g_j^{a_j}$. İspatlayıcı $\mathcal{P}$, A değerini doğrulayıcı $\mathcal{V}$'te iletir.
2) Doğrulayıcı $\mathcal{V}$ rastsal c değerini gönderir.
3) İspatlayan $\mathcal{P}$, $b_0 = a_0 + cX_0$, ve $b_j = a_j + cX_j$ değerlerini, $j \in C \subseteq \{1, ..., n-1\}$ için hesaplar ve $\mathcal{V}$'e gönderir.
4) Doğrulayıcı $\mathcal{V}$, $A = g_0^{b_0} \prod_{j \in C} g_j^{b_j} H^{-c}$ eşitliğinin sağlanıp sağlanmadığını kontrol eder.

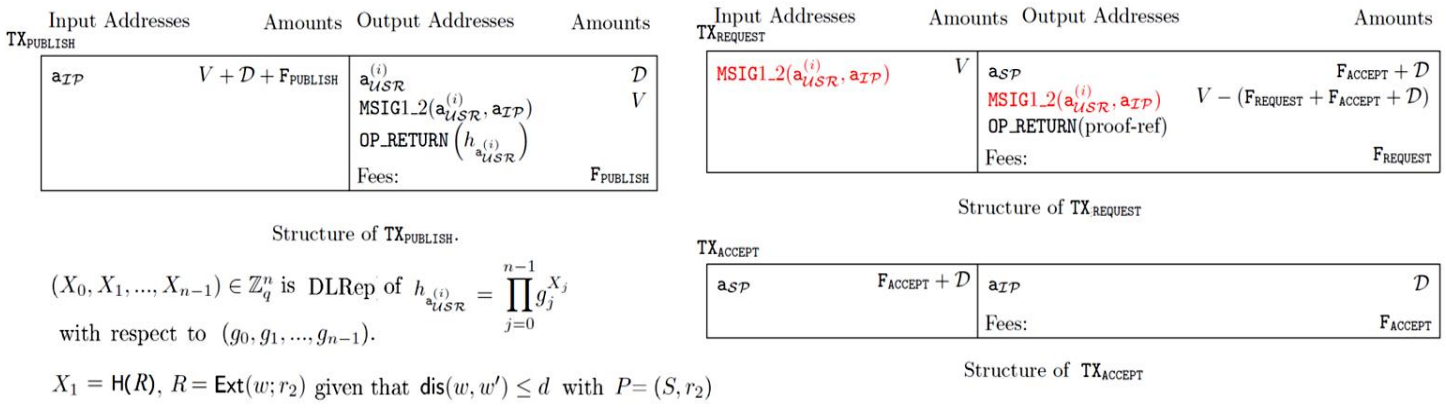
Blokzincir tabanlı kimlik yönetim sistemlerinde, doğrudan kimlik güven belgesi gösterimine ilişkin ispatlayanın hazırladığı sıfır bilgi kanıtının yer aldığı link bilgisi, servis talebini içeren transferin (`TXService`) ekstra kısmına, diğer bir deyişle `OP_RETURN` bölümüne (proof-ref) olarak eklenir. Böylece, Bitcoin blokzincirine maksimum 80 Byte büyüklüğünde veriyi yazdırabilme olanağı sağlayan `OP_RETURN` betiği, kimlik güven belgesinin gösterimine ilişkin ispat bilgisinin de bütünlüğünü proof-ref ile garanti altına almış olur. Örnek bir uygulama, Şekil 3'de sunulmuştur.

2.2. Fuzzy extractors

Fuzzy extractor (Dodis et al., 2004) yapıtaşı, kullanıcıya ait biyometrik veriye *w* dayanan bir mekanizmadır. Spesifik olarak, kullanıcıya ait başka ve benzer bir biyometrik veriden *w'*, daha sonra orjinal verinin *w* aynen tekrar oluşturulması amacıyla kullanılan bir metotdur. Fuzzy extractor Gen algoritması ile orjinal biyometrik veriyi girdi olarak alır, ve rastsal bir dizini R ve yardımcı veri P'yi çıktı olarak verir. Herhangi başka bir zamanda rastsal dizin R, bu defa Rep algoritması yardımıyla yeniden oluşturulabilir. Eğer tanımlanan metrikte dis(*w;w'*) < d uzaklık koşulu sağlanırsa, Rep algoritmasına orjinal biyometrik veriye benzer bir *w'* ve yardımcı veri P girdi olarak verildiğinde aynı R verisi elde edilir. Gen ve Rep algoritmalarının detayları için okuyucu (Blanton and Hudelson, 2009; Dodis et al., 2004) yayınlarından faydalanabilir.

2.3. Blokzincir'de biyometrik veriye dayalı kimlik yönetim ve ödeme sistemleri

Şekil 3: (Augot et al., 2017a) kimlik yönetim sisteminin, biyometrik veri w ve fuzzy extractor yapı taşları kullanılarak devredilemez hale getirilmesine dair örnek uygulama (Sarier, 2021). $TX_{REQUEST}$ *, Şekil 2'de yer alan* $TX_{Service}$ *ile aynı fonksiyonu yerine getirir.*



Literatür taramasında yer alan yayınlanmış bir çok bilimsel çalışmaya ilaveten, teknoloji firmaları da biyometri ve blokzinciri bir araya getiren birçok ürün geliştirme faaliyetini gerçekleştirmektedir (BCTR, 2021). Bu konuda, Şekil 3'de sunulan uygulamada, Brands credential şeması (Brands, 2000), Fuzzy extractor (Dodis et al., 2004; Blanton and Hudelson, 2009) algoritması ve Bitcoin tabanlı kimlik yönetim sistemi (Augot et al., 2017a) bir araya getirilerek, Blokzincir tabanlı biyometrik veriye dayalı transfer edilemez kimlik yönetim sistemi uygulaması gerçeklenmiştir.

2.4. Anonim Kripto paralar

Zerocoin (Miers et al., 2013) Bitcoin'deki tersine anonimleştirme sorununu isimsiz/anonim para birimi işlemlerine izin verecek şekilde Bitcoin'i genişleterek çözer. Zerocoin, sıfır bilgi kanıtına dayalı, Bitcoin forku olarak tanımlanan ilk anonim kripto para birimidir. Sıfır bilgi kanıtları, söz konusu bilgileri fiilen ifşa etmeden bilginin varlığını kanıtlama yöntemleridir.

Mint (Para basma): Bu teknoloji ile, halka açık defterde bulunan bir bitcoin özel bir madeni paraya (zerocoin) dönüştürülür. Bu dönüştürme taahüt şeması kullanılarak yapılır. Benzetme yaptığımızda, mint işlemi, herhangi bir parada bulunan tek bir seri numarasının sadece sahibi tarafından üretilip bilinerek, mühürlü bir zarfa konup zarfın kapatılması şeklinde düşünülebilir.

Spend (Harcama): Daha sonra, bu "dar" parayı harcamayı seçtiğinizde, sahibini açığa çıkarmaya gerek yoktur. Zerocoin, sıfır bilgi kanıtları ile doğrulamadan sonra bitcoin'e geri dönüştürülür. Bu sistemi bir çamaşırhaneye benzetebiliriz. Tamamen eş zerocoinler (beyaz gömlekler) aynı makinede (Akümülatör) toplanarak yıkanır ve sahipleri gömleğini giymek istediğinde, sıfır bilgi kanıtıyla makinedeki bir gömleğin sahibi olduğunu kanıtlayan kişi, herhangi birini makineden alır ve kullanır (zerocoin harcama). Yeni basılan Zerocoin'lerin sahiplerine bağlı bir işlem kaydı yoktur ve kullanıcılar yeni paraları herhangi bir mezhebe harcama özgürlüğüne sahiptir. Tam gizlilik için bu işlemi tekrar tekrar yapabilirsiniz. Yeni zerocoin'in iptali süreci, işlemin eski işlemlere bağlı olmadığı anlamına gelir. Bu blokzinciri bozar (Şekil 1 (b), kesik çizgi) ve zerocoinlerin sahibini belirlemek için blok zincirini analiz etme seçeneğini ortadan kaldırır.

2.5. Zerocoin tabanlı Anonim Biyometrik Kimlik Tanımlama

(Sarier, 2018)'de yayınlanan blokzincir tabanlı ilk anonim biyometrik kimlik tanımlama sistemi, üç ana aktör (kullanıcı *USR*, kimlik sağlayıcı *IP* ve servis sağlayıcı *SP*) ve üç adımda, Kurulum, kayıt ve tanımlama algoritmaları ile çalışır.

Kullanıcı kaydı: $\mathcal{USR}$, $\mathcal{IP}$'ye kimliğini kanıtlar ve bitcoin adresini $a_{\mathcal{USR}}$ ve biyometrik verisini şifreleyecek açık anahtarını sunar. $\mathcal{IP}$, kullanıcının şifreli biyometrik şablonunu $b_{\mathcal{USR}}$ içeren $TX_{PUBLISH}$ transferini şekil 4 deki gibi yayınlar. Kullanıcı sistemden çıkmak isterse, $\mathcal{IP}$ kullanıcı kaydını TX_{REVOKE} transferi ile iptal eder.

Biyometrik tanımlama: işlemi için ilave dört transfer gerekir: TX_{Mint}, TX_{Spend}, $TX_{Service}$ ve de $\mathcal{SP}$'nin onay/red kararını bildirdiği, TX_{Accept} ya da TX_{Reject}.

1- *Zerocoin basma* (TX_{Mint}): Kullanıcı $\mathcal{USR}$, kendi bitcoin adresini $a_{\mathcal{USR}}$ kullanarak bir Zerocoin basar. Bitcoin giden adres bölümünde yer alan scriptPubKey, talimat olarak ZEROCOIN_MINT verisini ve basılan parayı c_1 içerir. Bu transferi alan madenciler basılan c_1 parasının doğru şekilde üretildiğini teyit eder.

2- *Zerocoin harcama* (TX_{Spend}): Kullanıcı girdi olarak sahipsiz bir zerocoin mint transferini $\overline{TX}_{Mint}$ seçer ve $\mathcal{SP}$'nin açık anahtarına gönderecek şekilde ilgili transferi hazırlar. Bu aşamada önce sistemdeki tüm zerocoinleri akümüle eder (C) ve Spend algoritmasını çalıştırır.

$$\text{Spend}(params, \overline{b}_{\mathcal{USR}}, c_1, skc_1, hash(ptx), C) \rightarrow (\pi_1, S_1).$$

Son olarak, TX_{Spend} transferinin gelen bölümünde (π_1, S_1), yani sıfır bilgi kanıtı ve bastığı paraya ilişkin seri numarasını S_1 dijital imza yerine yazar. Aynı bölümde, sıfır bilgi kanıtı π_1 hesabında kullanılan akümülatörün yer aldığı bloğa referans verir. TX_{Spend}'in giden adres bölümünde yer alan ekstra kısmına (OP_RETURN) ise, şifrelenmiş güncel biyometrik şablon $\overline{b}_{\mathcal{USR}}$, ve ikinci bir seri numrasına taahüt eden c_2 'yi ekler. Böylece, şifrelenmiş güncel biyometrik şablon ve ikinci bir taahüt kayıt altına alınır. Bu taahüde ilişkin sıfır bilgi kanıtı daha sonra bir $TX_{Service}$ talebi ile anonim biyometrik tanımlamada kullanılacaktır.

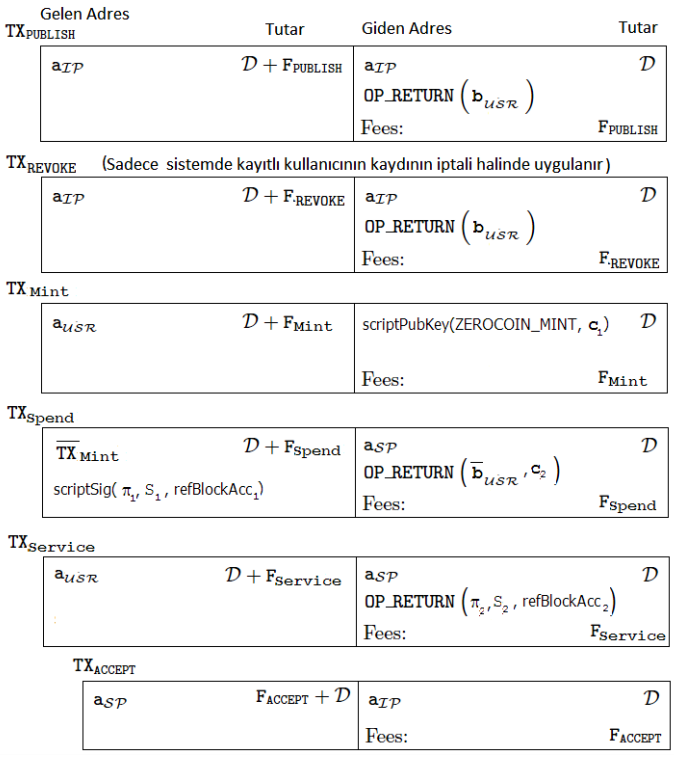
TX_{Spend} ağda göründüğünde, madenciler referans verilen bloktan elde ettikleri akümülatörü kullanarak, harcama işlemini Verify($params, \pi_1, S_1, hash(ptx)$,C) = 1 ile doğrular ve S_1 seri numarasının daha önceki bir transferde kullanılmadığını teyit eder.Tüm bu koşullar sağlandığında, ağ, harcama transferini onaylar ve kullanıcının bitcoin ödemesine izin verir.

Bu doğrulama işlemine paralel olarak, madenciler $\overline{b}_{USR}$ biyometrik şablonunu sistemde kayıtlı tüm şablonlarla şifreli alanda karşılaştırır. Eğer tek bir eşleşme kararı oluşursa (çünkü iki eşleşme bulunması, kullanıcı kaydının iptal edildiği anlamına gelir), S_1 seri numarası ve ağın kararı harcanan seri numarası listesine konur. Bu liste kullanıcı ve $\mathcal{IP}$ tarafından tutulur. Eğer eşleşme kararı listelenirse, ilgili ikinci taahüt c_2 madenciler tarafından ikinci bir akümülator kullanılarak biriktirilir ve bu ikinci akü gerçekte sadece biyometrik olarak eşleşmiş paraları içerir.

3- *Servis talebi* ($TX_{Service}$): Kullanıcı TX_{Mint}'dekinden farklı bir bitcoin adresi ile $a_{\mathcal{SP}}$' Şekil 4'deki $TX_{Service}$ transferini yapar. Aynı işlemler bu defa S_2 seri numaralı para üzerinden ve $a_{\mathcal{SP}}$'nin doğrulayıcı olmasıyla blokzincir dışında (offchain) tamamlanır. Böylece, kullanıcı ikinci bir seri numarasını S_2 taahüt eden c_2 parasını bildiğini sıfır bilgi protokolü ile servis sağlayıcıya $\mathcal{SP}$ offchain olarak ispatlar ve anonim biyometrik tanımlama gerçekleşir.

4- *Servis sağlayıcının kararı* $\mathcal{SP}$ (TX_{Accept} or TX_{Reject}): Kullanıcının sıfır bilgi ispatlarının doğrulanması ile $\mathcal{SP}$ kabul ya da red kararını verir ve ilgili kararın trasnferini TX_{Accept} yada TX_{Reject} transferi olarak $a_{\mathcal{IP}}$'ye ve offchain olarak kullanıcıya bildirir. (Sarier, 2018)'de anonim biyometrik tanımlama sistemine ilişkin kriptografik yapı taşları detaylı olarak sunulmuştur. Özetle, homomorfik olarak şifrelenen biyometrik veri, ilgili sıfır bilgi ispatları ile birlikte yine şifreli olarak karşılaştırılarak işlem görür (processing in the encrypted domain).

Şekil 4: Zerocoin tabanlı anonim biyometrik tanıma sistemi

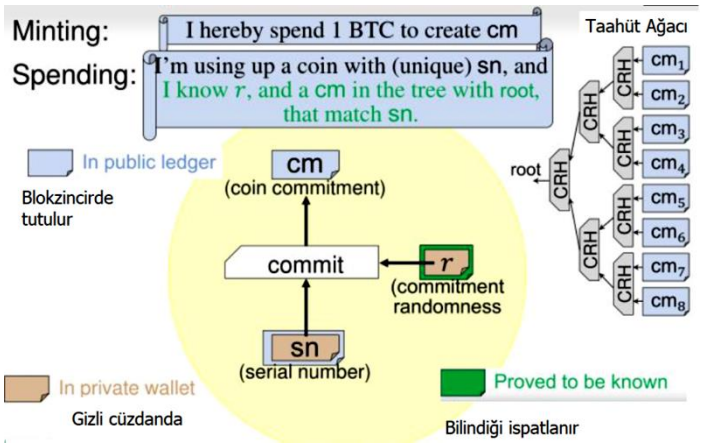


3. Mahremiyeti sağlayan kripto paralar üzerinden kimlik yönetimi

3.1. Zerocoin yerine daha güvenli bir çözüm: Zerocash

Miers vd. tarafından tasarlanmış Zerocoin (Miers et al., 2013), paraların izlenebilirliğini bozarak Bitcoin'i anonimlikle beraber sunmayı amaçlar. Ancak sonuç olarak ortaya çıkan kripto para tam teşekküllü anonim ödemeleri çeşitli nedenlerden dolayı destekleyemez. Ilk olarak, Zerocoin sadece gönderici mahremiyetini sağlar ve sabitlenmiş nominal değerleri kullanır. Bu, anonim kimlik tanımada esasen bir dezavantaj yaratmaz, çünkü anonim kimlik tanımada gönderilen transfer tutarları semboliktir ve birbirine eşit tek bir değere *D* sahiptir. Ayrıca, alıcı hesapların kimliğinin gizlenmesine gerek yoktur çünkü bunlar zaten servis sağlayıcının kendisidir. Ikinci olarak, ödemeden önce anonim paralar anonim olmayan bir hesaba transfer edilmelidir. Son olarak, işlemlerin içindeki para miktarını belirten veya diğer anlamlı veriler gizlenmez (Sasson et al., 2014) ve Zerocoin protokolüne ilişkin bazı güncel saldırılar tasarlanmıştır (Ruffing et al., 2018).

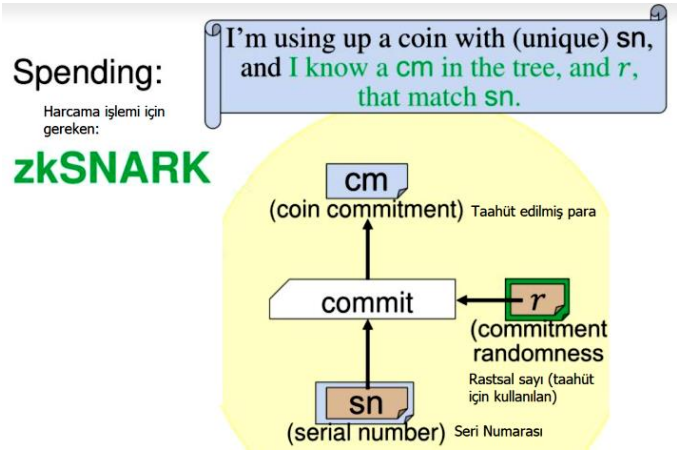
Şekil 5: Zerocash'de para basma: Mint. Sasson et al. (2014)



Tüm bu problemleri çözmek için Ben-Sasson vd. (Sasson et al., 2014) Zerocash'i tasarlamışlardır. Zerocash kullanıcının anonimliğini ve anonim paralarla işlem verisinin gizliliğini sağlar. Üstelik, Zerocash işlem boyutunu önemli boyutlarda küçültür (tek bir para için 1 KB'den daha az) ve onaylama zamanını 6 ms'den daha aza indirir (Sasson et al., 2014). Zerocash'te, işlemler üçe ayrılır: basecoin işlemi, mint (para basma) işlemi ve pour (spend) işlemi. Anonim kimlik tanımada, Zerocoin tabanlı (Sarier, 2018)'de olduğu gibi aşağıdaki iki temel işlem kullanılmaktadır.

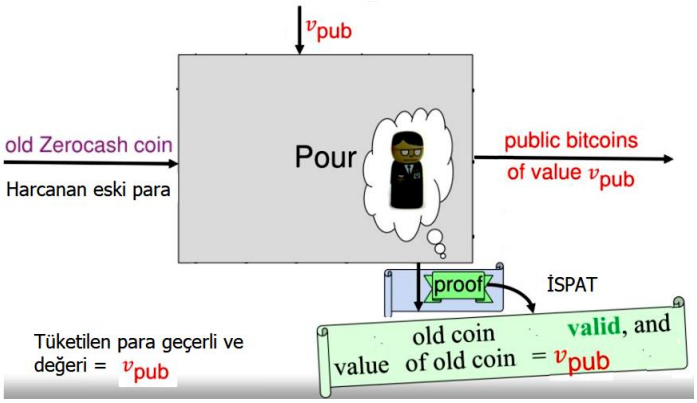
-Mint işlemi (Şekil 5): cm para taahhüdü, *v* para değeri ve * diğer gerekli bilgileri saklamak için ayrılmış alan olmak üzere, Zerocash'te bir mint işlemi (cm, *v*, *) verilerinden oluşur. Bir mint işlemi blokzincire eklendiği zaman, belli sayıda para blokzincire işlenmiş olur. Mint işlemini gerçekleştiren kişi, kendi adresini ya da transfer edilen değerleri açığa çıkarmadan blokzincire işlenmiş bu değerleri transfer edebilir. Anonim kimlik tanıma uygulamasında *v* değeri *D* sabit değerine eşittir ve Zerocash için 1BTC olarak sabitlenebilir.

Şekil 6: Basılan bir Zerocash'i harcama. Sasson et al. (2014)



-Pour (Spend) işlemi (Şekil 6): Verilen bir mint ya da pour/spend işlemi için, herhangi bir kullanıcı yeni bir pour işlemi üretebilir. Zerocoin'den farklı olarak, akümülator yerine, para taahhütleri Merkle ağacında tutulur, ve bu ağacın kökü rt olup, sn_1 ve sn_2 iki para seri numarası, cm_1 ve cm_2 iki yeni para taahhüdü, gizli girdiler üzerinde zk-SNARK kanıtı ve * diğer gerekli bilgileri saklamak için ayrılmış alan olmak üzere, Zerocash'te bir pour/spend işlemi (rt; sn_1; sn_2; cm_1; cm_2;v_{pub}; info) verilerinden oluşmaktadır (Sasson et al., 2014). Bir pour işlemi defteri kebire eklendiğinde söz konusu para kullanıcının adresi ve transfer edilen paranın miktarı açığa çıkmadan bir kullanıcıdan diğer bir kullanıcıya transfer edilir.

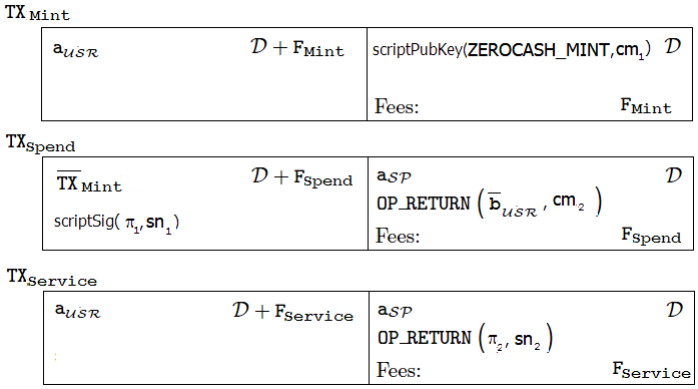
Şekil 7: Zerocash'den Bitcoin'e takas. Sasson et al. (2014)



Bir parayı harcarken, kullanıcı gizli olmayan açık bir v_{pub} değerini (örneğin *D*) ve bir transfer dizi bilgisini info $\in$ {0, 1} spesifik olarak belirterek, bu parayı bir basecoin yani Bitcoin'e çevirebilir (Sasson et al., 2014). Şekil 7'de özetlendiği üzere, v_{pub} açık değeri ile birlikte alıcı hedef adresi de açık olarak transfer dizi bilgisine eklenir. Burada, dizi bilgisi (transaction string info) Bitcoin alıcı hedef adresinini (e.g., a Bitcoin cüzdan açık anahtarı/adresi) içerir (Sasson et al., 2014). Şekil 5'den de görüleceği üzere, Zerocoin'in aksine, Zerocash, Akümülator yerine Merkle Taahüt Ağaçlarından faydalanır ve Akümülator'un gerektirdiği Çift Discrete Logarithm (Double Discrete Logarithm) ispatına gerek duymaz. Bunun yerine zk snark'ları kullanır. Esasen başka bir çalışmada (Sasson et al., 2014; Sarier, 2021), DDL ispatlarının ne kadar büyük yer tuttuğu detaylı olarak analiz edilmiştir.

Bu nedenle Şekil 4'de yer alan zerocoin tabanlı anonim biyometrik tanımlama sistemine ait transfer akışı, Zerocash yapıtaşları yönünden Şekil 8'de güncellenmiştir. Orjinal pour işleminden farklı olarak tek bir para cm_1 harcanır, ve bu para v_{pub} olarak *SP*'ın Bitcoin adresine Şekil 7'deki gibi takas edilir. Yine, Şekil 4'de olduğu gibi, *SP*'nin kabul/red kararı basecoin olan Bitcoin üzerinden tamamlanır.

Şekil 8: Zerocash tabanlı biyometrik tanımlama uygulaması



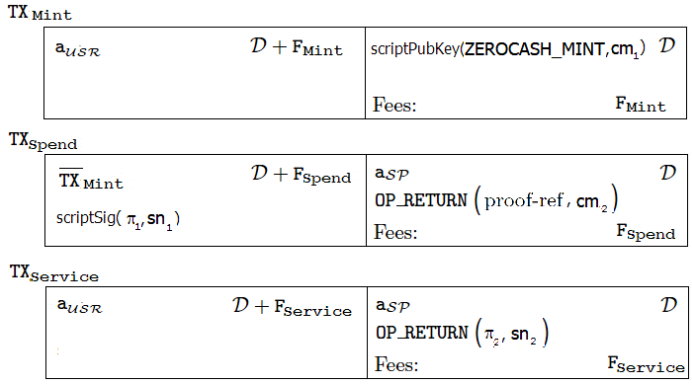
Yeni tasarlanan Zerocash ve Monero tabanlı kimlik yönetim sistemlerinde, (Sarier, 2018)' den farklı olarak b_{usr} verisi, kullanıcının şifreli biyometrik şablonu yerine, Önbilgi bölümündeki biyometrik veriye dayalı kimlik güven belgesini

$$h_{a_{usr}} = \prod_{j=0}^{n-1} g_j^{X_j}$$

temsil etmektedir, özetle $h = b'$ dir.

Bu durumda, biyometrik eşleşme/tanıma uygulması yerine kimlik yönetimi uygulaması baz alındığında, kimlik güven belgesi *h*' ın, şifreli biyometrik şablonu b'nin aksine sabit bir değer olması nedeniyle, Şekil 8'de yer alan TX_{Spend} transferindeki OP_RETURN bölümü, Şekil 3 'de olduğu gibi, doğrudan kimlik güven belgesi gösterimine ilişkin ispata ait link bilgisini (proof-ref) içerir. İlgili transfer akışı Şekil 9'da sunulmuştur.

Şekil 9: Zerocash tabanlı anonim kimlik yönetimi uygulaması



Zerocash, Zerocoin'e göre çok daha etkin, hızlı ve az yer tutan zk-snark'lara dayandığından, Şekil 8'de ve Şekil 9'da özetlenen zerocash tabanlı sistemler, zerocoin tabanlı eşdeğerlerine göre çok daha verimlidir. Ancak halen, her bir kimlik tanımlama işlemi için gerekli transfer sayısı, dolayısıyla toplam transfer tutarı azalmamıştır. Oysaki, daha az mahremiyet sağlayan blokzincir tabanlı anonim olmayan kimlik yönetimi sistemlerinde (Şekil 3), aktörler arasında gerçekleşen transfer akışı daha sade, dolayısıyla daha az komplike ve kullanıcı açısından daha ucuzdur.

3.2. Zerocash yerine daha pratik bir çözüm: Monero

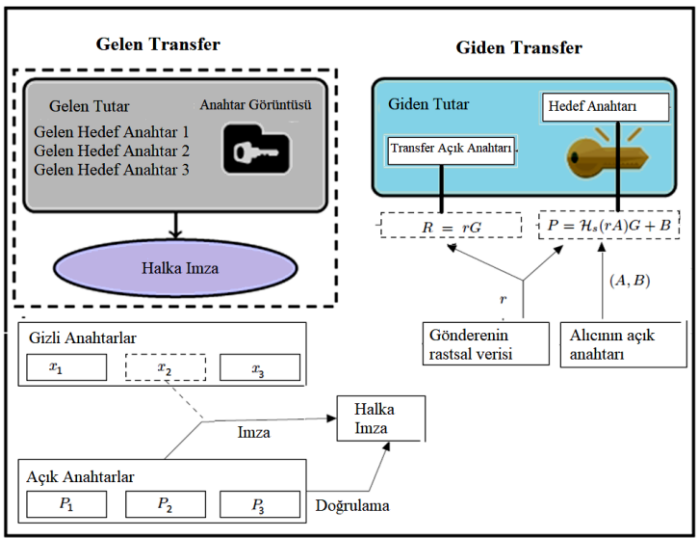
2013 yılında CryptoNote (van Saberhagen, 2013) adıyla bir teknik rapor yayınlanmıştır, yayınlanan bu raporda Bitcoin'de olmayan bazı gizlilik özelliklerini sağlayan bir sistem tanıtılmıştır. Bu sistemde, mevcut kripto paralardan farklı bir madencilik algoritması da tanıtılmıştır. Cryptonote'da önerilen sistemde transferlerde gönderici/alıcı adresleri gizlenmekte ve Bitcoin'den farklı bir emek ispatı (PoW) algoritması (CryptoNight) kullanılmaktadır. Ayrıca, Bitcoin'den farklı bir grup kullanıldığından, Önbilgi bölümünde yer alan parametreler yerine (örneğin, $g_0,g_1,\ldots,g_n,h$), büyük harf notasyonu kullanlacaktır (örneğin G). Spesifik olarak örneklendirirsek, bilindiği üzere, asimetrik şifreleme sistemlerindeki bir anahtar çifti, açık (örneğin $A = aG$) ve gizli (örneğin a) olmak üzere iki anahtardan oluşur. Monero'da ise, kullanıcıların 2 tane anahtar çifti $A = aG$, $B = bG$ bulunur. Monero'da da (Noether, 2015; Yuen et al., 2020), Zerocash'de olduğu gibi gönderilen miktarın gizlenmesi, IP adreslerinin gizlenmesi gibi özellikler eklenmiş olsa da anonim biyometrik tanımlama sistemlerinde gönderilen tutar sembolik anlamda olduğundan sadece (van Saberhagen, 2013) teknik raporu ile sınırlı kalınacaktır.

Özetle, Monero'da kullanıcıların 2 tane anahtar çifti $A = aG$, $B = bG$ bulunur. Bu anahtarlardan biri harcama anahtarı (b), biri de görüntüleme anahtarıdır (a). Bir kişiye transfer yapıldığında, kişi kendisine yapılan bu transferi görüntüleme anahtarı sayesinde tespit edebilir. Transferin kendisine yapıldığını belirledikten sonra harcama anahtarını kullanarak gönderilmiş olan parayı transfer edebilir. Bu anahtar çiftlerinin açık kısımları kullanıcı açık anahtarını, gizli kısımları da kullanıcı gizli anahtarını oluşturur. Kullanıcı gizli anahtarını oluşturan iki anahtardan biri kullanıcının kendisine yapılan transferleri tespit etme amacıyla kullandığı görüntüleme anahtarı, diğeri ise kendisine gelen transferleri harcama amacıyla kullandığı harcama anahtarıdır.

Alice, Bob'ın açık anahtarını ve kendisinin bildiği rasgele bir değeri (r) kullanarak; tek seferlik bir transfer açık anahtarı (R) ve Bob'a ait olduğu sadece Bob tarafından anlaşılabilecek olan bir hedef anahtarı (P=OT Pubkey) oluşturur. Bu şekilde transferi kime yaptığı bilgisi gizlenmiş olur. Alice Bob'a yaptığı her transferde farklı bir rasstsal sayı (r') seçtiğinden, her transferde farklı bir transfer anahtarı $(P = \overline{\text{OT Pubkey}})$ üretmiş olur.

Bob'ın kendisine bir transfer gelip gelmediğini, yayınlanan bloklardaki her bir transferi kontrol ederek anlar. Transferde bulunan transfer açık anahtarı R ve hedef anahtarı P=OT Pubkey değerlerini alır, kendi açık anahtarı ($A;B$) ve görüntüleme anahtarı (a) değerlerini de kullanarak, transferin kendisine yapılıp yapılmadığını tespit eder. Özetle, Bob, bir transferin kendisine gönderilip gönderilmediğini anlamak için görüntüleme anahtarını (a) kullanır. Diğer taraftan, Bob parasını harcayabilmek için, harcama anahtarını (b) kullanarak transfer gizli anahtarını hesaplar. Şekil 10 üzerinden gidersek, Bob kendisine gelen bir transferdeki (P_2) parayı harcayabilmek için, harcama anahtarını (b) kullanarak transfer gizli anahtarını (x_2) hesaplar. Kendisine gelmiş olan parayı transfer etmek için, bu (x_2) değerini kullanarak, gerçekleştireceği transferi Şekil 10'daki gibi halka imza ile imzalar.

Şekil 10: Standart Cryptonote transferi: Gelen transfer bölümünmde, iki mix-in kullanır (dolayısıyla üç gelen transfer),bu üç anahtarı içeren halka imza harcanan çıktıya karşılık gelen gerçek gelen adresini gizler.

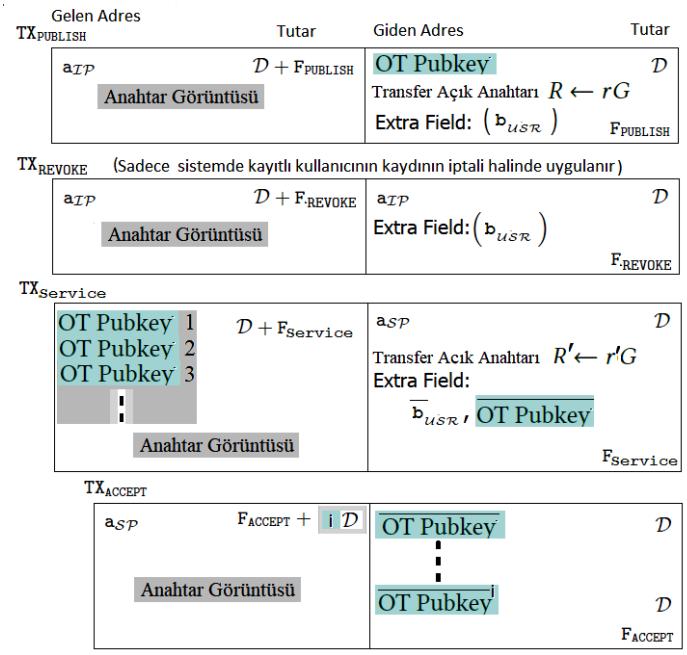


Monero ile ilgili daha detaylı bilgiye (van Saberhagen, 2013) makalesinden ulaşılabilir. Monero para birimi, aşağıdaki iki özelliği sağlayarak Bitcoin'in gizlilik sorunlarını giderir.

- Bağlantısızlık: Herhangi iki işlem için aynı kişiye gönderildiğini ispat etmek imkansız olmalıdır.

- Izlenemezlik: Cryptonote'da Bob sadece belirli bir anahtarla doğrulanabilen değil; bir kümeye dahil olan herhangi bir anahtarla doğrulanabilen bir imza atar. Yani kümeye dahil olanlardan herhangi biri bu imzayı atmış olabilir. Monero'da, Bitcoin'de olduğu gibi Extra veri alanı mevcuttur. Bu nedenle Bölüm 2.5'de özetlenen sistem ile uyumludur.

Şekil 11: Monero tabanlı anonim biyometrik tanımlama sistemi



3.3 Monero tabanlı anonim kimlik yönetimi

Kurulum: $\mathcal{IP}$ sistem parameterelerini Monero transferleri aracılığı ile yayınlar.

Kullanıcı kaydı: $\mathcal{USR}$, $\mathcal{IP}$'ye kimliğini kanıtlar ve Monero adresini $a_{\mathcal{USR}} = (A, B)$ ve biyometrik verisini de içeren kimlik verilerini $(X_1, ..., X_{n-1})$ sunar. $\mathcal{IP}$, kullanıcının Önbilgi bölümünde belirtilen şekilde kimlik güven belgesini içeren $\mathrm{TX}_{\mathrm{PUBLISH}}$ transferini şekil 11 deki gibi yayınlar. Kullanıcı sistemden çıkmak isterse, $\mathcal{IP}$ kullanıcı kaydını $\mathrm{TX}_{\mathrm{REVOKE}}$ transferi ile iptal eder.

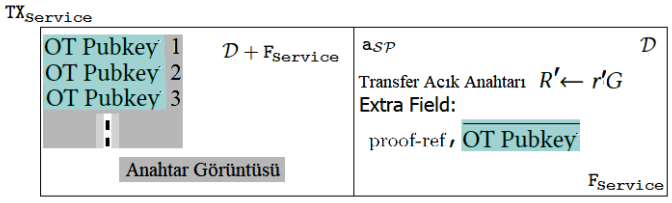
Kimlik tanımlama: Zerocoin ve Zerocash'in aksine, sadece iki ilave transfer işlemi ile tamamlanır: $\mathrm{TX}_{\mathrm{Service}}$ ve $\mathcal{SP}$ nin onay kararını içeren $\mathrm{TX}_{\mathrm{Accept}}$.

1- *Servis talebi* ($\mathrm{TX}_{\mathrm{Service}}$): Kullanıcı Şekil 12'deki $\mathrm{TX}_{\mathrm{Service}}$ transferini güncel biyometrik verisi ile hazırlanmış kimlik güven belgesini transferin extra bölümüne ekleyerek servis sağlayıcı $\mathcal{SP}$ ye gönderilecek şekilde hazırlar. Aynı ekstra bölümüne transfer açık anahtarı R' ile hazırlanmış yeni bir hedef anahtarını ($\overline{P} = \overline{\mathrm{OT\ Pubkey}}$) da ekler.

2- *Servis sağlayıcının kararı* $\mathcal{SP}$ ($\mathrm{TX}_{\mathrm{Accept}}$): Kullanıcının Önbilgi bölümünde yer alan güncel biyometrik verisi ile hazırlanmış kimlik güven belgesinine ait sıfır bilgi ispatlarının ayrı bir kanaldan servis sağlayıcıya ulaştırılması sonucunda doğrulanması halinde $\mathcal{SP}$ kabul kararını verir ve ilgili $\mathrm{TX}_{\mathrm{Accept}}$ transferini kabul edilen diğer kullanıcıların $\mathrm{TX}_{\mathrm{Service}}$ transferilerinin extra bölümünde girdikleri hedef anahtarlarına şekil 11 deki gibi gönderir.

Yine, biyometrik eşleşme/tanıma uygulması yerine kimlik yönetimi uygulaması baz alındığında, kimlik güven belgesi h'ın şifreli biyometrik şablonun b aksine sabit bir değer olması nedeniyle şekil 11 de yer alan $\mathrm{TX}_{\mathrm{Service}}$ transferindeki extra field bölümü şekil 3 de olduğu gibi doğrudan kimlik güven belgesi gösterimine ilişkin ispata ait link bilgisini (proof-ref) içerir.İlgili transfer akışı şekil 12'de sunulmuştur.

Şekil 12: Monero tabanlı anonim kimlik yönetim sistemi



4. Güvenlik Analizi

Esasen tasarlanan biyometrik tanımlama ve kimlik yönetim sistemleri, anonim kripto paralar üzerinden çalıştığından, güvenlikleri doğrudan ilgili kripto paranın sağladığı güvenlik nosyonlarına (Miers et al., 2013; Sasson et al., 2014; van Saberhagen, 2013) bağlıdır. Ayrıca, blokzincir üzerinde tutulan biyometrik veri/kimlik güven belgesi, homomorfik şifreleme sistemi ve sıfır bilgi ispatı birlikte kullanılarak (Sarier, 2018; Brands, 2000; Augot et al., 2017b; Sarier, 2021), herhangi bir aşamada herhangi bir deşifre yapılmadan (Processing in the encrypted domain) işlem görmektedir. Bu konuda detaylı güvenlik analizleri, gerek biyometrik tanımlama (Sarier, 2018) gerekse kimlik yönetim sistemleri (Sarier, 2021; Augot et al., 2017b) üzerinden tamamlanmış olduğundan, okuyucu detaylar için ilgili yayınlardan faydalanabilir.

5. Karşılaştırma

Öncelikle her üç sistem de sadece kimlik tanımlama amaçlı olarak uygulandığından, para üstü yoktur. Transfer edilen tutarlar sabit ve sembolik bir değere D eşit olduğundan, miktar yönünden takip yoluyla güvenlik açığı yoktur. Zerocoin RSA tabanlı sıfır bilgi protokolüne dayanır ve bu ispat 45 kB dan daha büyük yer tutar, ve tüm ağda yayımlanması ve tüm peerler (node) tarafından bu ispatların doğrulanması ve kalıcı olarak kütükte saklanması gerekir. Dolayısıyla Bitcoin'den çok daha fazla ağı yorar. Zerocoin'i Bitcoin'e çevirmek çift ayrık-logaritma bilgi ispatına dayanır ve 128-bit güvenlik'te 450 ms doğrulama süresi gerekir (Miers et al., 2013). Daha güncel bir çalışmada bu veriler yeniden hesaplanmış ve Spend (harcama) işlemi için 26kB ve 320ms doğrulama süresine ulaşılmıştır (Paul et al., 2019). Bitcoin'de ise aynı veriler ortalama 1kB ve 1ms olarak ölçülmüştür (Miers et al., 2013; MONERO.HOW, 2021a). Monero'nun Zerocoin'e göre daha az işlem gerektirdiği (van Saberhagen, 2013)'da gösterilmiştir. Monero transferi ortalama 2kB yer tutar, yani standard bir Bitcoin transferinden daha büyüktür. Ancak, blok bekleme süresi 1 dk, doğrulama süresi ise 2 dk'dır, bu veriler Bitcoin'in 1/5'ine eşittir (MONERO.HOW, 2021a). Monero daha verimli bir kriptoparadır ancak Zerocoin gibi sıfır bilgi protokolü içermediğinden mixin (halkadaki imza) sayısına bağlı olarak takip edilme olasılığı daha yüksektir (Kumar et al., 2017; Wijaya et al., 2018).

Ayrıca, standart bir Bitcoin transfer ücreti (fee) 360 satoshi, yani byte başına 0.0000036 Bitcoin(BTC)'dir (Augot et al., 2017a). Ortalama 267 byte büyüklüğündeki bir $\mathrm{TX}_{\mathrm{PUBLISH}}$ transferi (Augot et al., 2017a) için .0009612BTC ≈ 3.23USD masraf ödenir (8/2/2019'da, 1BTC ≈ 3360USD). Oysaki, Bitcoin'de 2020/2021 aralığında gerçekleşen değer artışı nedeniyle transfer ücreti ≈ 74.36USD'a kadar yükselmiştir (MONERO.HOW, 2021b). Yine, standart bir Bitcoin transfer ücreti (fee), Mart 2021 itibari ile transfer başına ortalama 22.13Dolar'dır (YCHARTS, 2021). Ayrıca, (MONERO.HOW, 2021b) Bitcoin ve Monero transfer ücretlerini aşağıdaki tabloda özetlendiği şekilde karşılaştırmalı olarak sunmuştur.

Tablo 1.Transfer ücret karşılaştırması (MONERO.HOW, 2021b)

	Transfer ücreti	Transfer ücreti (USD)
Monero (median)	0.000015XMR	0.0035
Bitcoin (median)	0.000291BTC	17.7614

Monero ve Zerocash karşılaştırması çeşitli yönlerden (Bit-Degree, 2021)'da ele alınmıştır. Her iki anonim kripto paranın farklı yönlerden (hız, ölçeklenme, kullanılabilirlik, transfer ücreti) birbirine üstünlük sağladığı gerçeği ışığında, Monero, hız, kullanım kolaylığı ve ölçeklenme problemlerini Zerocash'e göre daha iyi çözmekte iken, transfer ücreti Zerocash'de daha düşüktür. Ancak her iki anonim para birimi de Bitcoin'den daha hızlıdır.

Ayrıca, Zerocash (Zcash) anonim kriptoparası için ortalama transfer ücreti Mart 2021 itibari ile 0.026267USD olarak belirlenmiştir (coindesk, 2021). Yine, Zerocoin (Zcoin) anonim kriptoparası için Mart 2021 itibari ile minimum transfer ücreti 0.0000019 (0.0000113USD) 'dir (CoinLore, 2021). Burada unutulmaması gereken, Zerocoin ve Zerocash'de Mint işlemi ve Spend işlemi dışında diğer işlemler Basecoin olan Bitcoin üzerinde gerçekleşir. Yine Mint işlemi Bitcoin'den Zerocoin/Zeocash'e geçiş, Spend işlemi ise tam ters yöne geçiş sağlamaktadır. Bu nedenle herbir servis talebi için gerekli

toplam kullanıcı maliyeti hesaplandığında Zerocoin ve Zerocash tabanlı sistemlerde Basecoin olan Bitcoin transfer ücreti de dikkate alınmalıdır.

Tablo 2. Kimlik Yönetiminde herbir servis talebine ait Transfer ücreti

	Transfer ücreti	Transfer ücreti (USD)
Monero (XMR)	0.000015XMR	0.0035
Zerocash (ZEC)	0.00029BTC+ZEC	17.76+0.02626
Zerocoin (Zcoin)	0.00029BTC+Zcoin	17.76+0.000011

6. Sonuç

Karşılaştırma bölümünde analiz edilen her üç anonim para birimi açısından, toplam maliyet, güven belgesinin her bir gösterimi için gerekli toplam transfer adedi, Bitcoin fork'u olması nedeniyle Zerocoin ve Zerocash transferlerine ilaveten Bitcoin transferi nedeniyle oluşan ilave maliyet, kullanım kolaylığı, hız ve ölçeklenme yönleri hep birlikte ele alındığında, Monero'nın Bitcoin forku olmaması ve daha az transfer adedi gerektirmesi nedeniyle Zerocoin ve Zerocash'e göre kullanıcı açısından daha verimli, hızlı, kullanılabilir ve ucuz bir kimlik yönetim sistemi sağladığı açıktır. Gelecek çalışmalarda, Monero'nun, RingCT (Noether, 2015; Yuen et al., 2020) entegrasyonu ile iyileştirilen anonimlik özellikleri de dikkate alınarak, Zerocash'e göre belirgin güvenlik zaafiyetlerinin ortadan kalkması ile kimlik yönetim sistemlerinde kullanılması gerek teorik gerekse pratik uygulama yönleriyle ele alınabilir.

7. Teşekkür

Yazar, başta EJOSAT dergi editörleri ve EJOSAT dergi sekreteri olmak üzere, tüm hakemlere değerli yorumları ve katkıları için teşekkürlerini sunar.

Kaynakça

Augot, D., Chabanne, H., Chenevier, T., George, W., and Lambert, L. (2017a). A user-centric system for verified identities on the bitcoin blockchain. In CBT'17, volume 10436 of LNCS, pages 390–407. Springer.

Augot, D., Chabanne, H., Clémot, O., and George, W. (2017b). Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain. In PST'17, pages 25–2509. IEEE.

Augot, D., Chabanne, H., and George, W. (2019). Practical solutions to save bitcoins applied to an identity system proposal. In ICISSP'19, pages 511–518. SciTePress.

BCTR (Retrieved on March, 2021). Blockchain tabanlı biyometrik doğrulama sistemi. https://bctr.org/blockchaintabanli-biyometrik-dogrulama-sistemi-4624/.

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., and Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7:164908–164940.

BitDegree (Retrieved on March, 2021). Zcash vs monero – the complete guide. https://www.bitdegree.org/crypto/tutorials/zcash-vs-monero.

Blanton, M. and Hudelson, W. M. P. (2009). Biometricbased non-transferable anonymous credentials. In ICICS'09, volume 5927 of LNCS, pages 165–180. Springer.

Brands, S. A. (2000). Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press.

BZLab (Retrieved on March, 2021). Blokzincir. http://blockchain.bilgem.tubitak.gov.tr/.

coindesk (Retrieved on March, 2021). Zcash zec average transaction fee (24h).https://www.coindesk.com/price/zcash.

CoinLore (Retrieved on March, 2021). Coinlore koinler/zcoin blockchain stats. https://www.coinlore.com/tr/coin/zcoin.

CryptID (Retrived on May, 2018). source code available at https://github:com/cryptidid/cryptid. http://cryptid:xyz/.

Dodis, Y., Reyzin, L., and Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In EUROCRYPT'04, volume 3027 of LNCS, pages 523–540. Springer.

Kumar, A., Fischer, C., Tople, S., and Saxena, P. (2017). A traceability analysis of monero's blockchain. In ESORICS'17, volume 10493 of LNCS, pages 153–173. Springer.

Lesavre, L., Varin, P., Mell, P., Davidson, M., and Shook, J. (Accessed on: August, 2019). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. https://doi.org/10.6028/NIST.CSWP.07092019-draft.

Liu, Y., Sun, G., and Schuckers, S. (2019). Enabling secure and privacy preserving identity management via smart contract. In CNS'19, pages 1–8.

Miers, I., Garman, C., Green, M., and Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. In SP'13, pages 397–411. IEEE.

MONERO.HOW (Retrieved on March, 2021a). How long do monero transactions take? https://www.monero.how/howlong-do-monero-transactions-take.

MONERO.HOW (Retrieved on March, 2021b). How much are monero transaction fees? https://www.monero.how/monero-transaction-fees.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Noether, S. (2015). Ring signature confidential transactions for monero. Cryptology ePrint Archive, Report 2015/1098.

Othman, A. and Callahan, J. (2018). The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity. In IJCNN'18, pages 1–7.

Paul, J., Xu, Q., Fei, S., Veeravalli, B., and Aung, K. (2019). Practically realisable anonymisation of bitcoin transactions with improved efficiency of the zerocoin protocol. In FICC'18, pages 108–130. Springer.

Ruffing, T., Thyagarajan, S. A. K., Ronge, V., and Schröder, D. (2018). Burning zerocoins for fun and for profit – A cryptographic denial-of-spending attack on the zerocoin protocol. In CVCBT'18, pages 116–119. IEEE.

Sarier, N. D. (2018). Privacy preserving biometric identification on the bitcoin blockchain. In CSS'18, volume 11161 of LNCS, pages 254–269. Springer.

Sarier, N. D. (2021). Comments on biometric-based non-transferable credentials and their application in blockchain based identity management. Computers & Security, 105:102243.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy, pages 459–474.

Toutara, F. and Spathoulas, G. (2020). A distributed biometric authentication scheme based on blockchain. In 2020 IEEE International Conference on Blockchain, pages 470–475. IEEE.

van Saberhagen, N. (2013). Cryptonote v 2.0. Available at https://cryptonote.org/whitepaper.pdf.

Wijaya, D. A., Liu, J. K., Steinfeld, R., Liu, D., and Yuen, T. H. (2018). Anonymity reduction attacks to monero. In Inscrypt'18, volume 11449 of LNCS, pages 86–100. Springer.

YCHARTS (Retrieved on March, 2021). Bitcoin average transaction fee. Available at https://ycharts.com/indicators/bitcoin_average_transaction_fee.

Yuen, T. H., Sun, S., Liu, J. K., Au, M. H., Esgin, M. F., Zhang, Q., and Gu, D. (2020). RingCT 3.0 for blockchain confidential transaction: Shorter size and stronger security. In FC'20, volume 12059 of LNCS, pages 464–483. Springer.

Zhou, X., Hafedh, Y., Wang, Y., and Jesus, V. (2018). A simple auditable fingerprint authentication scheme using smart contracts. In SmartBlock'18, volume 11373 of LNCS, pages 86–92. Springer.

Zhu, X. and Badr, Y. (2018). Identity management systems for the internet of things: A survey towards blockchain solutions. Sensors, 18(12):4215.