ANONİM KRİPTOPARALARIN KORELASYON TABANLI MAHREMİYET ANALİZİ

Muhammet Ali Öztürk[1,2], İsa Sertkaya[3], Hüseyin Yüce[4]

[1] Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği, İstanbul, Türkiye
[2] TÜBİTAK BİLGEM Bilgi Sistemleri, Kocaeli, Türkiye
[3] MCS Labs & BCLabs, TÜBİTAK BİLGEM UEKAE, Kocaeli, Türkiye
[4] Marmara Üniversitesi, Teknoloji Fakültesi, İstanbul, Türkiye
muhammet.ozturk@tubitak.gov.tr, isa.sertkaya@tubitak.gov.tr,
huseyin@marmara.edu.tr

ÖZET

Bitcoin, açık anahtarlı adresleri kullandığı için anonimliği tamamıyla sağladığı düşünülse de bu adresler herkese açık bir kayıt defterinde tutulduğundan dolayı anonim değildir. Bu nedenle anonim kriptoparlar yayınlanmıştır. Anonim kriptoparaların teoride matematiksel olarak tamamıyla anonim olduğu düşünülse de pratikte anonimliği yeteri kadar sağlayamazlar. Bu makalede Zcash, Dash ve Monero anonim kriptoparalarının pratikte iddia edildikleri kadar anonim olup olmadığını tespit etmek amacıyla korelasyon tabanlı mahremiyet analizleri yapılmıştır. Bu makaleyle beraber ilk defa Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi çalışması yapılmıştır, Zcash için daha önce yapılan bir çalışma bulunmaktadır. Zcash'in korumalı işlemleri %84,4 ve Dash'in ÖzelGönderim ile alakalı işlemleri %49.304 oranında ilişkilendirilebilmiştir. Monero işlemlerinin adres ve miktarları tamamen gizli olduğu için korelasyon tabanlı mahremiyet analizi gerçekleştirilememiştir.

Anahtar Kelimeler— Mahremiyet analizi, anonim kriptopara, zcash, dash, monero

Correlation Based Privacy Analysis of Private Cryptocurrencies

ABSTRACT

Although Bitcoin is considered to provide complete anonymity because it uses public-key addresses, these addresses are not anonymous because they are kept in a public registry. For this reason, anonymous cryptocurrencies have been published. It is stated that anonymous cryptocurrencies are mathematically anonymous in theory, for various reasons they cannot provide enough anonymity in practice. In this article, correlation-based privacy analyzes were conducted to determine whether the anonymous cryptocurrencies of Zcash, Dash and Monero are indeed as anonymous as they claim in practice. With this article, correlation-based privacy analysis was carried out for the first time for Dash and Monero anonymous cryptocurrencies, there is a previous study for Zcash. Zcash's shielded transactions were associated with the rate of 84.4% and Dash's PrivateSend-related transactions at a rate of 49.304%. Correlation-based privacy analysis could not be performed for Monero because the addresses and amounts of Monero transactions are completely confidential.

Keywords— Privacy analysis, anonymous cryptocurrency, zcash, dash, moner

I.GİRİŞ (INTRODUCTION)

Bitcoin açık kaynak kodlu, yazılım tabanlı bir çeşit dijital para birimidir. Kullanmış olduğu kriptografik yöntemlerden dolayı Bitcoin'e kriptopara, kullanılan teknolojiye de blokzincir denir. Bitcoin'i farklı kılan şey blokzincir teknolojisinin sağlamış olduğu anonimlik ve herhangi bir merkeze bağlı olmayan yapısıdır [1].

En temel tabiriyle blokzincir hiçbir merkezi otoriteye ihtiyaç olmaksızın değer olarak atfedilen çeşitli varlıkların bir veriymiş gibi aktarılmasını sağlayan veritabanına verilen isimdir [2],[3]. Blokzincirin altyapısı kendisine adını veren "bloklar (blocks)" ve bu bloklar içerisine eklenen "işlemlerden (transactions)" oluşur. Bu işlemler, ilgili blokzincire ait her türlü verinin kaydedildiği bir çeşit içerik bilgisidir. Bu kayıtlar birleştirilir ve belirli aralıklarla bloklara yazılır. Bu bloklar da sırayla art arda oluşturularak bir zinciri

oluşturur. Blokzincirdeki herbir blok (ilk blok hariç) kendisinden önceki bloğun özet (hash) bilgisini de tutar.

Bitcoin işlem, blok ve adreslerinin tamamının açık (public) veritabanlarına kaydedilmesinden dolayı Bitcoin kriptoparası düşünüldüğü kadar anonim değildir. Bu nedenden ötürü de Zcash, Dash ve Monero gibi anonimlik ve mahremiyete daha fazla önem veren anonim kriptoparalar çıkmıştır.

Anonim kriptoparaların ortak özelliği anonimliğin artırılarak mahremiyetin ihlalinin engellenmesinin sağlanmasıdır. Dolayısıyla bu kriptoparalara anonim kriptoparalar (anonymous cryptocurrencies) adı verilmiştir. Örnek olarak Zcash, anonimliği korumalı havuz ve gizli işlemeler vasıtasıyla sağlamaya çalışır.

Ne var ki, anonim kriptoparalar teoride anonimlik sağladıklarını belirtseler de pratikte bu kriptoparalar çeşitli yöntemlerle analiz edilebilmektedirler. Bu durumda da anonim kriptoparaların sağladıkları anonimlik ve mahremiyet ihlal edilebilmektedir. Anonim kriptoparaların analiz edilebileceğini tespit etmek amacıyla bu makalede Zcash, Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi yapılacaktır.

Yıllar boyunca Bitcoin kriptoparasının anonimliğine odaklanan çeşitli çalışmalar ve araştırmalar yapılmıştır. Bu çalışmaların önemli bir kısmı Bitcoin adresleri, blokları ve işlemlerleri üzerinde yapılan çalışmalardır [4], [5], [6], [7], [8]. Bu çalışmalar Bitcoin adresine sahip madenciler (miners), madenci havuzları (mining pools), normal kullanıcılar (standart users) ve Bitcoin satıcıları/borsacıları (Bitcoin exchanges) gibi çeşitli kullanıcı gruplarına odaklanarak mahremiyet analizi gerçekleştirir. Başka araştırmalar ise Bitcoin kriptoparasının eşler arası ağının (peer-to-peer network) analiz edilerek çeşitli bilgilerin elde edilmesi üzerine odaklanmıştır [9],[10],[11].

Anonim kriptoparalar da Bitcoin gibi çeşitli mahremiyet analizi çalışmalarının konusu olmuşlardır. [12] ve [13] çalışmaları Dash anonim kriptoparasının mahremiyet analizine odaklanır. Monero anonim kriptoparası üzerine odaklanan [14],[15] ve [16] araştırmaları genel itibariyle çeşitli analiz yöntemleriyle anonimliğin ihlaline odaklanırken [17] çalışması tüm bu çalışmalardan farklı olarak "Makine Öğrenme (Machine Learning)" yöntemlerini kullanarak anonimliğin analizine odaklanmıştır. [2], [18], [19], [20], [21], [22], [23] çalışmalarıysa doğrudan Zcash anonim kriptoparasına odaklanır. Alex Birkuyov tarafından hazırlanan [2] çalışması bahsedilen mahremiyet analizlerinden doğrudan korelasyon tabanlı olan tek çalışmadır.

Kriptoparaların sadece blokzincirde bahsedilen özellikleri üzerinden mahremiyet analizi yapılmaz, kriptosistemdeki çeşitli öğeler de analiz edilebilmektedir. [24] ve [25] çalışmaları Bitcoin, Zcash, Dash ve Monero'nun ağ analizlerini yaparken [26] çalışması ise yine Bitcoin, Dash, Monero, ve Zcash için mobil cüzdanları (mobile wallet) üzerine mahremiyet analizi yapar.

Anonim kriptoparalar oldukça farklı araçları kullanarak blokzincirdeki işlem ve adres mahremiyetini sağlamayı amaçlar. Bu nedenle birçok farklı mahremiyet analizi yapılmıştır. Bu makalede Zcash, Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi yapılmıştır. İlk olarak bu anonim kriptoparaların kullanımları gruplandırılmıştır. Daha sonra ilgili anonim kriptoparaların adresleri, işlemleri ve blokları analiz edilerek adreslerin birbirleriyle olan ilişkileri tespit edilmeye; yani anonimleştirilen para transferlerinin anonimliğinin bozulmasına (de-anonymization) çalışılmıştır. Makalede ilk olarak [2] makalesinden yola çıkılarak Zcash anonim kriptoparası için korelasyon tabanlı mahremiyet analizi çalışması yapılmıştır. Analiz sırasında Alex Birkuyov'un kullanmış olduğu algoritmalarda bazı güncellemeler yapılmıştır. Dash ve Monero anonim kriptoparaları içinse daha öncesinden herhangi bir korelasyon tabanlı mahremiyet analizi yapılmamıştır, bu analiz çalışması ilk defa bu makalede yapılmıştır.

Analiz çalışmasının ardından makalede yapılan bu analizin sonuçları paylaşılmıştır. Daha sonra elde edilen bu sonuçların nedenleri hakkında tartışma yapılmıştır. Son olarak anonim kriptoparaların kullanıcı ve geliştiricilerine bu sonuçlardan kaçınmaları için önerilerde bulunulmuştur. Kısaca bu makalede sadece analiz çalışması yapılmamış; anonim kriptoparalarlar ilgilenenler için sonuca götüren nedenler ve önerilerden de bahsedilmiştir.

II. TANIMLAR (DEFINITIONS)

2.1. Blokzincir ve Bitcoin

Blokzincirin çözüm getirdiği en önemli sorunlarda birisi de merkezi güvene dayalı sistemlerdir. Blokzincir teknolojisi, "değer (value)" olarak atfedilen verilerin dağıtık olarak veritabanlarında tutulmasıdır [1]. Bitcoin kriptoparası eşler arası teknolojisini (peer-to-peer technology) kullanarak herhangi merkezi ağ olmadan çalışır [27].

Bitcoin adreslerinin tamamıyla açık adres olması gibi sebeplerden dolayı düşünüldüğü kadar mahremiyet sağlamamaktadır. Jong-Hyouk Lee tarafından hazırlanan araştırmaya göre Bitcoin'in anonim olmamasının kısaca 3 sebebi vardır, [28]:

1. Blokzincirin açık olması (public blockchain)
2. Adreslerin açık anahtarlı olması (public key-based address)
3. Eşler arası veri paylaşımının İnternetten yapılması (peer-to-peer networking over the Internet)

2.2. Anonim Kriptoparalar

Bitcoin'in anonimlik sağlamada yetersiz olmasından dolayı anonim kriptoparalar yayınlanmıştır. Anonim kriptoparaların aşağıdaki özellikleri sağlanmış olması beklenir [28]:

- **Gizlilik:** Yapılan para transferlerindeki gönderen, alan ve gönderilen para miktarı işlemi yapan adres sahipleri haricindeki hiçbir kimse tarafından bilinmemesi için bir şekilde gizlenmesi gerekmektedir.
- **Takip Edilememezlik:** Anonim olarak yapılan para transferlerdeki paraların hiçbir şekilde işlem tarihçesinde (yani defterlerde) izlenilebilir yahut ilişkilendirilebilir olmaması gerekmektedir.
- **Birbiriyle Değiştirilebilirlik:** Tüm dijital paraların birbirlerinden ayırt edilemez olduğu, böylece karşılıklı olarak değiştirilebilir olduğu temin edilmelidir.

Makalede Zcash, Dash ve Monero anonim kriptoparaları üzerine korelasyon tabanlı mahremiyet analizi yapılacağından dolayı aşağıda kısaca bu anonim kriptoparalardan ve anonimliği nasıl sağladıklarından bahsedilecektir.

2.3. Zcash

Zerocash protokolü kullanılarak geliştirilmiş olan Zcash, Bitcoin'den çatallandırılmış (forked) bir kriptoparadır. Bitcoinden farklı olarak zk-SNAKRs kullanılarak matematiksel olarak işlemler ve adresler için anonimlik sağlar. Bitcoin gibi şeffaf işlemlerin (transparent transactions) yanında ayrıca gizli işlemleri (private transactions) de destekler. Gizli işlemlerde transfer edilen para ikinci bir havuz olan korumalı havuza (shielded pool) aktarılır [29], [30].

Zcash kriptoparasının kullanmış olduğu temel para birimine ZEC, en küçük para birimine Zatoshi denir. 1 ZEC 10^8 Zatoshiye eşittir. Varsayılan işlem ücreti (transaction fee) 10^4 Zatoshidir (10^{-4} ZEC). İlk blok ödülü (block mining reward) 12.5 ZEC (10 ZEC madenciye, 2.5 ZEC Zcash geliştiricilerine) kadardır. Zamanla bu ödül Zcash kurucuları tarafından düşürülmüştür. Şu anki blok üretme ödülü 6.25 ZEC kadardır. 1.25 ZEC Zcash kurucularına gider, kalan 5 ZEC'de bloğu oluşturan madenciye gönderilir [2].

Girdi ve çıktının görünür olduğu açık adreslere (transparent-address) t harfi ile başladıkları için kısaca t-adres, gizli ve çıktının gizlendiği gizli adreslere (private-address) de z harfi ile başladıkları için kısaca z-adres de denir. Zcash'te z-adreslerin geçtiği işlemlere EkleBöl işlemleri (JoinSplit transactions) adı verilir, kısaca EB-işlemleri (JS-transactions) de denir. Bir EB-işleminde en fazla 2 farklı z-adresi kullanılabilir. Toplamda 4 farklı EB-işlemi bulunmaktadır [29]:

1. **z'den z'ye işlemler (z-to-z transactions):** Sadece z-adresleri arasında yapılmış olan işlemlerdir. Hem gönderenin hem de alıcının adresleri gizlidir. Ayrıca gönderilen miktar ve alınan miktar tamamen gizlidir. Sadece böyle bir işlemin gerçekleştiğine dair işin ispatı vardır. Zden zye işlemde görülebilen tek veri bu işlemin bedelidir. Zcash'de gizliliğinin sağlandığı EB-işlemidir. Burada yapılan işlemler korumalı havuzdan korumalı havuza yapılan bir işlem olmasından dolayı bu işlemlere korumalı işlemler (shielded transactions) de denilir.
2. **z'den t'ye işlemler (z-to-t transactions):** Girdi olarak sadece z-adres varken çıktı olaraksa bir veya daha fazla t-adresi bulunur. Korumalı havuzdan şeffaf havuza ZEC aktarımı olduğundan dolayı bu işlemlere korumanın kaldırılması işlemleri (deshielding transactions) de denilir. Bu işlemlerde girdi miktarı 0 ZEC'tir. Çıktı değerleri defterde herkese açıktır. Toplam çıktıyla beraber işlem bedelinin toplamı korumalı havuzdan çıkan Zcash'i verir.
3. **t'den z'ye işlemler (t-to-z transactions):** Çıktı olarak sadece z-adres, girdi olaraksa bir yahut daha fazla t-adres bulunur. Şeffaf havuzdan korumalı havuza ZEC aktarımı yapıldığından dolayı bu işlemlere aynı zamanda korumanın oluşturulması işlemleri (shielding transactions) de denilir. z'den t'ye işlemlerin aksine t'den z'ye işlemlerde girdi değerleri defterde herkese açıkken çıktı değeri gizlidir, yani blokzincirde 0 ZEC olarak görülür. Girdilerin toplamından işlem bedeli çıkartıldığı zaman çıkan sonuç korumalı havuza gönderilen Zcash'i verir.
4. **tz'den tz'ye işlemler (tz-to-tz transactions):** Hem işlem girdisinde de hem de işlem çıktısında hem t-adres hem de z-adres bulunur. İşlem bedeliyle beraber çıktıların toplamının toplanır. Elde edilen toplam girdilerin toplamından çıkartılır. Çıkan sonuçta farkın pozitif çıkması durumunda korumanın sağlanması işlemi, farkın negatif çıkması durumunda korumanın kaldırılması işlemi yapılmış denilebilir. Farkın 0 çıkmasıysa bu işlemin bir çeşit korumalı işlem olmasını sağlar.

2.4. Dash

18 Ocak 2014 tarihinde Bitcoin kriptoparasındaki anonim eksikliğini farkeden Evan Duffield tarafından geliştirilmiştir [31], [32], [33].

Dash, aslında Bitcoin tabanlı yazılım olan Litecoin kriptoparası çatallanmasıdır. Bitcoin'e nazaran daha anonimleştirme odaklı coin transferi yapısı sunar. Bitcoin'e göre 2 farklı yenilik getirmiştir [34]:

2.4.1. AnaUç

Kriptoparalarda veri akışının sürekliliğini sağlamak ve eşleri ilgili ağda gerçekleşen çeşitli olaylarda güncel tutmak için P2P ağında çalışan ve tam düğüm (full node) adı verilen sunuculardır. AnaUçlar kriptosistemdeki ÖzelGönderim ve HızlıGönderim denilen iki tane çok önemli işlemden sorumludur. Bir

kullanıcının AnaUç olabilmesi için 1000 Dash'e sahip olması gerekir. Yaptıkları bu yatırıma karşılık AnaUçlar herbir üretilen bloklardan sağlanan blok ödülün yaklaşık %45'ini alır. Diğer %45'i bloğu üreten madenciye giderken kalan ödülün %10 kadarı Zcash'te olduğu gibi Dash kurucularına gider.

2.4.2. ÖzelGönderim

Bitcoin'de önerilen CoinJoin yapısının üzerine kurulmuştur. CoinJoin'de kısaca elindeki parayı anonimleştirmek isteyen bir kullanıcı yine elindeki parayı anonimleştirmek isteyen başka bir kullanıcıyla beraber Dash karıştırma işlemine girer. Burada Dash transferi rastgele başka farklı adreslere gönderilerek girdi ile çıktı arasında hiçbir ilişki bulundurulmaz. ÖzelGönderim en az 3 kullanıcının karıştırma işlemine katılması şartını koşar. Bunun yanında karıştırma işleminin toplamda 2 ile 16 sefer (round) arasında yapılmasını şart koşar. Ağda dağıtık olan AnaUçlar vasıtasıyla ÖzelGönderim işlemi gerçekleştirilir. Yapılan karıştırmalar sayesinde Dash, anonimlik şartlarından birisi olan "birbiriyle değiştirilebilirliği" sağladığını belirtir. ÖzelGönderim sadece 10 Dash'ın katlarını (en fazla 10^3 Dash ve en az 10^{-3} Dash) kullanır.

2.5. Monero

18 Nisan 2014'te yayınlanan Monero anonimlik, mahramiyet ve işlem gizliliğine odaklanan bir anonim kriptoparadır [35], [36]. Monero "gizlenmiş bir açık defterdir" (obfuscated public ledger); yani herkes işlem gönderebilir ve alabilir ancak hiçbir kimse bu işlemlerdeki adresleri ve gönderilen miktarları göremez. Diğer kriptoparalar gibi yeni madeni paralar çıkarmak ve madencileri "ağı korumak ve işlemleri doğrulamak" için teşvik etmek amacıyla işin ispatı mekanizmasını kullanır.

Para birimi XMR'dir. Blok ödülü ilk blokta 17.592169267200 XMR olarak belirlenmişken her blokla düşen bu ödül 3 Temmuz 2020 23:13:28 UTC tarihli 2134425. bloğun ödülü 1.579420370752 XMR kadardır. XMR 10^{-12} ye kadar bölünebilir, yani teknik olarak en küçük yapılabilen Monero işlemi 0.000000000001 XMR olacaktır. Anonimliği sağlamak için halka imzalar yapısından faydalanır.

Kriptografide halka imza, her birinde anahtar olan bir kullanıcı grubundaki üyelerden herhangi biri tarafından imzalanabilen bir çeşit dijital imzadır. Yani halka imza ile imzalanan bir mesaj dışarıdan bir grup kullanıcı tarafından imzalanmış gibi görünür. Ancak aslında bu mesaj, anahtara sahip olan o gruptaki sadece bir kişi tarafından imzalanmıştır. Halka imzaları işlem çıktılarının geriye doğru takip edilememesini sağlar [37].

2.6. Uygulama ve Analiz

Bu çalışmada Alex Birkuyov'un hazırlamış olduğu [2] makalesindeki yapılan çalışmalar temel alınarak Zcash, Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi yapılmıştır. Bu analizler neticesinde analiz edilebilen ilgili anonim kriptoparaların ne derecede işlem ilişkilendirilmesi yapılabildiği hesaplanmıştır. Anonim kriptoparaların analizi için Bitcoin ile Bitcoin kodundan türetilme kriptoparalar için hazırlanmış olan ve Github veri deposuna (repository) yüklenmiş olan Blocksci[1] açık kaynak kodlu uygulaması kullanılacaktır. Zcash içinse Blocksci uygulamasının Zcash için hazırlanmış olan çatallanması[2] kullanılacaktır.

III. ZCASH ANALİZİ (ANALYSIS OF ZCASH)

Zcash için analize 784834. bloğun üretildiği tarih olan 04 Nisan 2020 Cumartesi 12:03:06 tarihinde başlanmıştır. Bunun anlamı Zcash anonim kriptoparası için yapılan korelasyon tabanlı mahremiyet analizi 04 Nisan 2020 tarihinden önce üretilmiş olan tüm 784834 bloğu kapsar. 784834. bloktan sonra üretilmiş ve üretilecek olan tüm bloklarla beraber Zcash için yapılacak tüm yeni güncellemeler yapılmış olan mahremiyet analizi çalışması kapsamınının dışındadır.

Mahremiyet analizi çalışmasında ilk olarak Zcash kullanıcılarının korumalı XMR aktarımı sağlayan EB-işlemlerini ne derece kullandığı Şekil 1'deki grafikte gösterildiği gibi tespit edilmiştir. Şekil 1'de gösterilmekte olan grafikte Zcash anonim kriptoparasının çıktığı tarih olan 2016 Ekim tarihinden analiz çalışmasının yapıldığı 2020 Nisan tarihine kadar Zcash kullanıcıların tercih ettikleri işlem tipleri yıl ve ay bazında toplamları gruplanarak gösterilmiştir. Şekil 1'deki x ekseninde olan *Blok Üretme Tarihi* ilgili işlem tipinin toplandığı yıl ve ayı belirtir. Grafikteki y ekseninde de işlem tipinin tercih edilme sayısını verir. Grafik incelendiği zaman kullanıcıların büyük çoğunlukla doğrudan şeffaf işlemleri tercih ettikleri görülecektir. Zcash'in ilk çıktığı aylarda, yani 2016 Ekim, Kasım ve Aralık aylarında kullanıcıların EB-işlemlerini tercihi %25-%30 oranındaydı. Zcash işlemlerinin anonimliğinin sağlanması açısından önemli bir değer olan bu oranın zaman içerisinde artması beklenirken %10-%15 oranına kadar düştüğü gözlemlenmiştir. Mart 2020 ayı için bu oran %15,91'dir. Şekil 1'deki grafikte Zcash kullanıcıları EB-işlemlerini gerektiği düzeyde tercih etmedikleri açıkça görülmektedir.

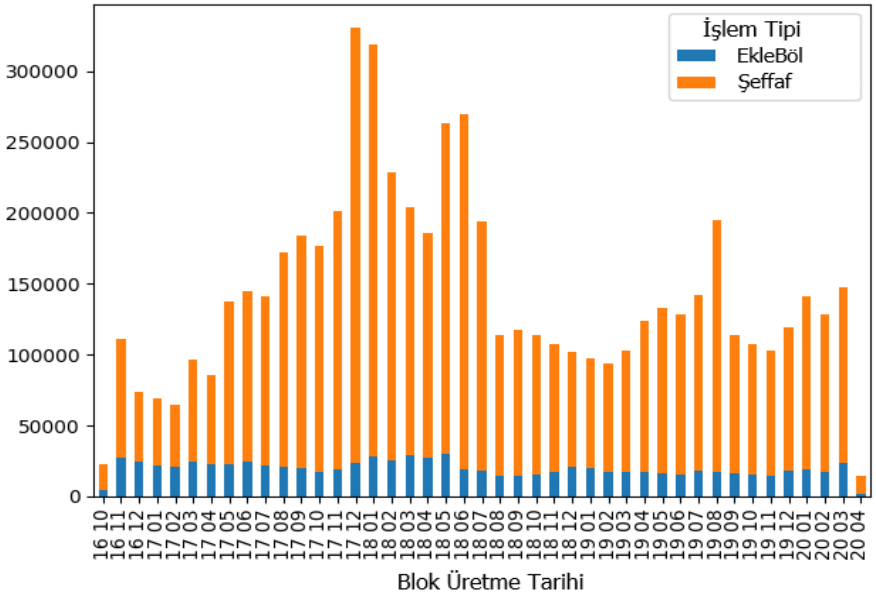
Analiz çalışması kapsamında daha yine aynı tarihler için Zcash kullanıcıların EB-işlem tiplerini tercih etme oranlarına bakılmıştır. Şekil 2'de yıl ve aylara göre tercih edilen EB-işlemi tipi grafiği gösterilmektedir.

[1] Princeton University - Center for Information Technology Policy tarafından hazırlanan Blocksci açık kaynaklı uygulama koduna https://github.com/citp/BlockSci bağlantı adresine tıklayarak ulaşabilirsiniz.

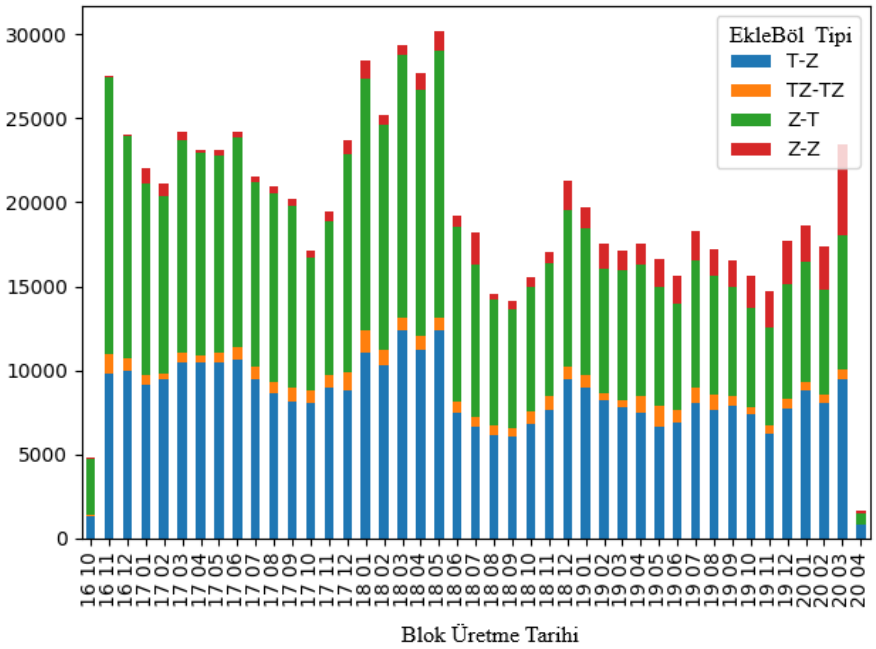
[2] CryptoLux Research Group at SnT, University of Luxembourg tarafından hazırlanmış olan Blocksci uygulamasının Zcash için hazırlanmış forkuna https://github.com/cryptolu/BlockSci bağlantı adresine tıklayarak ulaşabilirsiniz.

Şekil 2'deki x ekseninde bulunan *Blok Üretme Tarihi* Şekil 1'deki x ekseni ile aynı değeri taşır. Grafikteki y eskeni ise kullanıcıların ilgili yıl ve ayda tercih ettikleri toplam EB-işlemi tipini verir. Burada üzerinde en fazla durulması gereken EB-işlemi tipi zden zye yapılan korumalı işlemlerdir. 2016'nın son aylarına tekabül eden Zcash'in çıktığı ilk zamanlarda korumalı EB-işlemlerinin tüm EB-işlemlerine oranı %1-%3 oranındayken zaman içerisinde bu oranın önemli bir istakrarlı artış sergilediği aşikârdır. Bu oran Mart 2020'de %23,17 oranına kadar çıkmıştır. EB-işlemleri arasında üçüncü şahıslara neredesye hiçbir şekilde yapılan işlemin miktarı ve adresleri hakkında bilgi vermeyen tek EB-işlemi tipi bu korumalı işlemlerdir. Korumalı işlemlerin kullanım oranının artması Zcash kriptoparasının daha zor korelasyon tabanlı mahremiyet analizi yapılabilmesini sağlar. Bu grafik EB-işlemlerini kullanan Zcash kullanıcılarının zaman içerisinde Zcash anonim kriptoparasını kullanma konusunda iyi yönde bilinçlendikleri bilgisini verir. Çünkü ne kadar gizli adres kullanılarak yapılsalar da zden tye, tden zye ve tzden tzye yapılan işlemler sonuçta korumalı havuza giren ve korumalı havuzdan çıkan Zcash miktarları (yani işlemlerin ZEC yahut Zatoshi değerleri) hakkında bilgi verirler.

Analiz işlemi için bir sonraki adında blokzincirdeki tüm işlemler için "çıktı adresi değeri" gruplanmıştır. Çıktı adresi değerleri gruplaması için en çok kullanılan 10,000 adres çıktısı incelenmiştir. Şekil 3'te en çok kullanılan 10,000 işlem adreslerine ait çıktıların ZEC değerleri verilmiştir. Bu grafikte verilen sonuç "10,000 farklı işlem çıktısı" değeri değil "10,000 farklı çıktı adresi" değeridir. Şekil 3'teki grafikte x eksenindeki *OutputValue* çıktı adreslerinin Zatoshi cinsinden değerini verir. Grafikteki y eksenindeki *tops* ise bu değerlerin toplam kullanılma sayısını verir. Şekil 3'teki grafik incelendiği zaman grafikteki değerlerin ilginç bir şekilde 10^6 Zatoshi yani 0,01 ZEC'te yoğunlaştığı ve 10^7 Zatoshi yani 0,1 ZEC'e doğru toplam kullanılma sayısı azalan şekilde değiştiği gözlemlenmektedir. 10^6 Zatoshi değeri neredeyse 1,000,000 kez adres çıktısı olarak kullanılmıştır. Bu sonuç Zcash anonim kriptoparasında özellikle 0.01 ZEC / 10^6 Zatoshi ve 0.1 ZEC / 10^7 Zatoshi arasındaki değerlerin azımsanamayacak bir ölçüde en çok kullanılan adres çıktısı değerleri olduğunu gösterir.

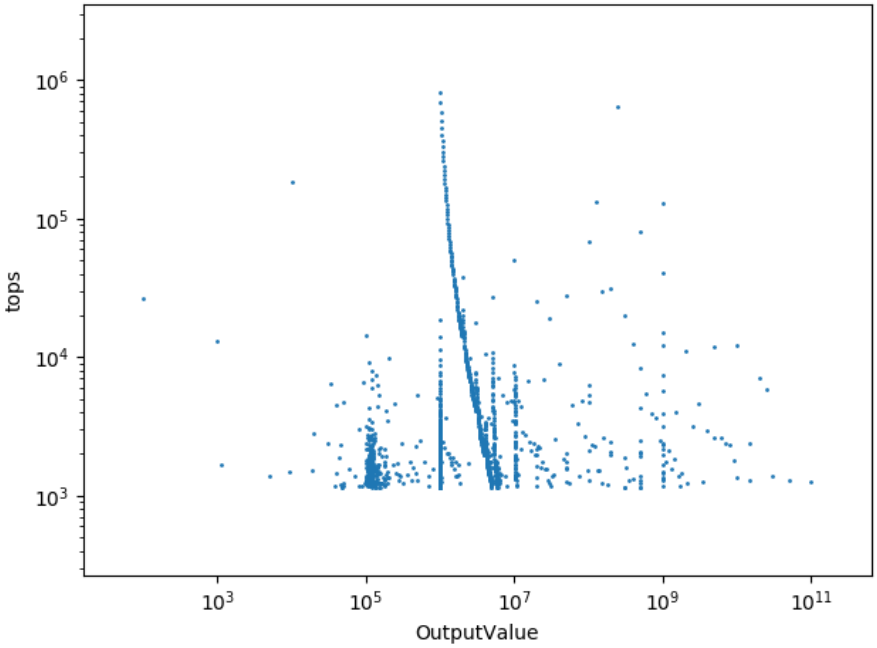


Şekil 1. Yıl ve Aylara Göre İşlem Tipi (Transaction Type) Grafiği

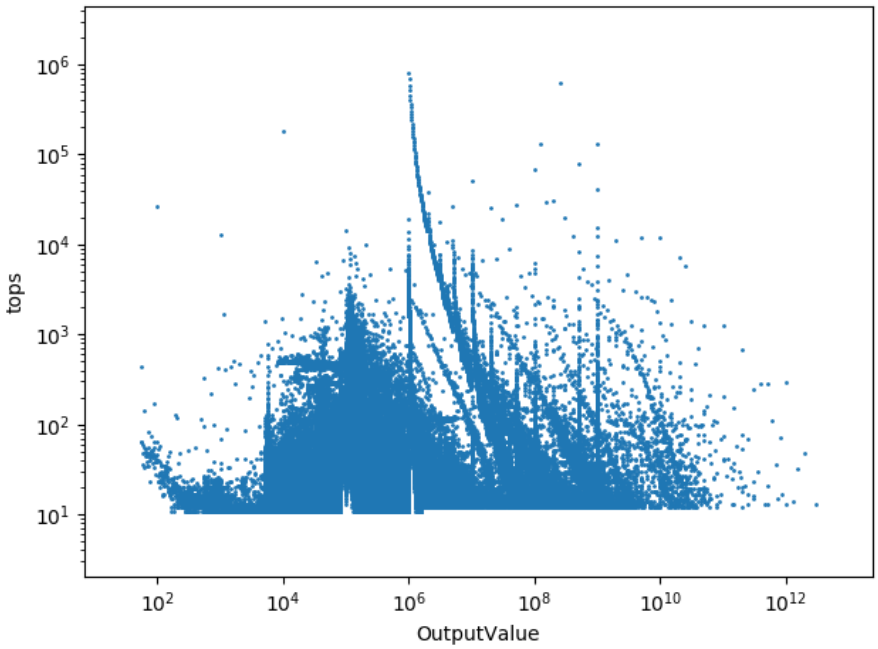


Şekil 2. Yıl ve Aylara Göre EkleBöl İşlemleri Tipi (JoinSplit Transactions Type) Grafiği

.



Şekil 3. En Çok Kullanılan 10,000 Adres Çıktısı



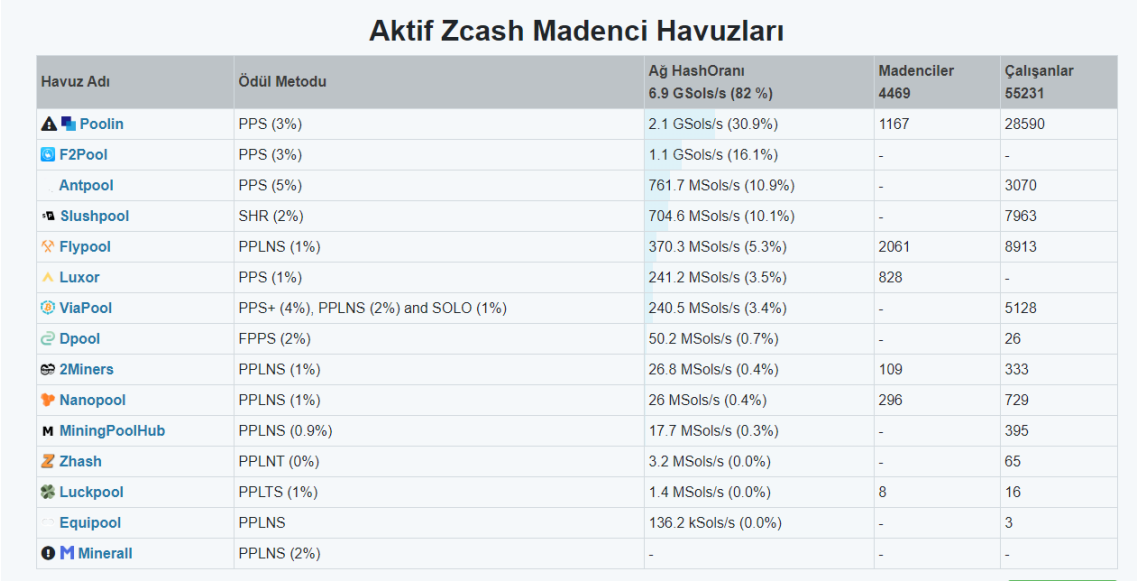
Şekil 4. En Çok Kullanılan 1,000,000 Adres Çıktısı

Analiz çalışmasında bir sonra grafikte en çok kullanılan 1,000,000 çıktı adresi değeri incelenmek istendiğinde Şekil 4'teki grafik sonuç olarak çıkmıştır. Grafikteki *OutputValue* ve *tops* eksenleri Şekil 3'teki eksenlerin aynısıdır. Şekil 3'te olduğu gibi Şekil 4'te de 0.01 ZEC/10^6 Zatoshi ve 0.1 ZEC/10^7 Zatoshi arasındaki değerlerin azımsanamayacak bir ölçüde en çok kullanılan adres çıktısı değerleri olduğu açıkça gözlemlenmektedir. Madenci havuzlarının bünyesinde bulundurdukları madencilere genellikle en az 0.01 ZEC/10^6 Zatoshi katılım payı verdikleri bilinmektedir. Madenci havuzları madencilerin yapmış oldukları işlemci gücü destek payına göre 0.01 ZEC'in üstüne Zatoshi seviyesinde ekleme yaparlar. Misal olarak bir madenciye 0.01022 ZEC ödeme yapılırken daha fazla işlemci gücü tedarik eden başka bir madenciye 0.01322 ZEC ödeme yapılabilir. Bu bilgiler ışığında Şekil 3 ve Şekil 4'teki grafiklerde gözlemlenen yoğunlaşmanının madenci havuzlarının yaptıkları madenci ödemelerinden kaynaklandığını sonucuna varılabilir. Aynı zamanda elde edilen bu sonuç madenci ve blok ödülü üretme kaynaklı işlemlerin Zcash kriptoparasındaki işlemlerin önemli bir bölümüne tekabül ettiği anlamına da gelir. Ancak bazı madenci havuzları madencilerine blok üretme ödülünden düşen paylarını zden zye korumalı işlemler aracılığıyla gönderdiğinden kesin olarak bu konuda bir şey söylenemez.

3.1. Madenci Havuzları ve Madencilerin Analizi

Şekil 5'te Aktif Zcash madenci havuzları gösterilmektedir. Şekil 5'teki madenci havuzları ağ özetleme oranının (network hashrate) %82'sini kapsarken Poolin isimli madenci havuzu ağ özetleme oranının %30,9 kadarını kapsadığı görülmektedir. Bu durum "merkezisizleştirilmiş" olarak bir merkezi otorite olmaksızın işlem yapan blokzincirler için oldukça tehlikeli bir durumdur. Gerçekten de Nisan 2020'de yapılan madenciler analizinde en fazla blok üretme ödülü alan madencinin Poolin madenci havuzu olduğu ve F2Pool ve Antpool ile bu üç madenci havuzunun madenci ödülü pastasından en fazla payı aldıkları gözlemlenmiştir.

Hem zamanla Zcash kriptoparası için ciddi değişiklikler manasına gelen Overwinter gibi güncellemeler nedeniyle, hem de madenci havuzlarınının madencilerinin sürekli madenci havuzu değiştirmesi ve yeni madenci havuzlarının maden üretme yarışına dâhil olması sebebiyle aşağıda detaylı olarak açıklanacak işlem analizleri tüm 784834 blok için baştan sona olacak şekilde yapılmamıştır. Ayrıca belki de milyonlarca işlemle beraber bu işlemlerde ZEC gönderip alan on milyonlarca adresi sürekli olarak korelasyon tabanlı mahremiyet analizi işlemine girdirmek analizin performansı açısından etkili sonuçlar almayı zorlaştırır. Bu gibi nedenlerden dolayı analizlerin tamamı belirli bir blok aralığında yapılmasının daha doğru olacağı kanaatine varılmıştır. Bunun için de son 10,000, 25,000 ve 50,000 blok kısaca temel analizlere sokularak hız ve performans ile elde edilen sonuçların etkileri ve yüzdeleri bakımından karşılaştırılmışlardır. Karşılaştırma sonucunda korelasyon tabanlı mahremiyet analizinin son 25,000 blok aralığı için yapılmasında karar kılınmıştır.



Aktif Zcash Madenci Havuzları

Havuz Adı	Ödül Metodu	Ağ HashOranı 6.9 GSols/s (82 %)	Madenciler 4469	Çalışanlar 55231
Poolin	PPS (3%)	2.1 GSols/s (30.9%)	1167	28590
F2Pool	PPS (3%)	1.1 GSols/s (16.1%)	-	-
Antpool	PPS (5%)	761.7 MSols/s (10.9%)	-	3070
Slushpool	SHR (2%)	704.6 MSols/s (10.1%)	-	7963
Flypool	PPLNS (1%)	370.3 MSols/s (5.3%)	2061	8913
Luxor	PPS (1%)	241.2 MSols/s (3.5%)	828	-
ViaPool	PPS+ (4%), PPLNS (2%) and SOLO (1%)	240.5 MSols/s (3.4%)	-	5128
Dpool	FPPS (2%)	50.2 MSols/s (0.7%)	-	26
2Miners	PPLNS (1%)	26.8 MSols/s (0.4%)	109	333
Nanopool	PPLNS (1%)	26 MSols/s (0.4%)	296	729
MiningPoolHub	PPLNS (0.9%)	17.7 MSols/s (0.3%)	-	395
Zhash	PPLNT (0%)	3.2 MSols/s (0.0%)	-	65
Luckpool	PPLTS (1%)	1.4 MSols/s (0.0%)	8	16
Equipool	PPLNS	136.2 kSols/s (0.0%)	-	3
Minerall	PPLNS (2%)	-	-	-

Şekil 5. Aktif Zcash Madenci Havuzları (*https://www.poolwatch.io/coin/zcash bağlantı adresini kullanarak ulaşabilirsiniz. 1 Temmuz 2020 01:37 tarihinde erişilmiştir.*)

Tablo 1, tüm Zcash madenci ve madenci havuzlarının toplamda üretmiş oldukları blok sayısıyla beraber elde ettikleri blok ödüllerini Zatoshi cinsinden verir. Bazı t-adresleri için t-Havuz, bazıları için de t-Madenci olarak bahsedilmiştir. Bunun tek nedeni t-Havuz olarak bahsedilen t-adresleri çeşitli Zcash gezginleri (Zcash explorer) kullanılarak tespit edilebilirken t-Madenci olarak bahsedilen t-adresleri bu gezginlerde tespit edilemeyen diğer madencilerdir. Bunlara havuz denmeyişinin tek sebebi de bu adreslerin madenci havuzuna mı yoksa doğrudan bir madenciye mi ait olduğu tespit edilemediğinden dolayıdır. Bunun yanında listede bazı t-adreslerinin yanına (1) ve (2) sayılarının olduğu görülmektedir; bu rakamlar işaret ettikleri üç t-adresinin aynı maden üretme ödülü işleminde aynı ödülü paylaştıklarını belirtmek için konulmuşlardır. Bu kullanıcıların neden bu şekilde bir kullanıma gittikleriyle alakalı herhangi bir bilgiye ulaşılamamıştır. Ayrıca ödülü paylaşan bu t-adresler yüzünden en alttaki TOPLAM'da üretilen 25,000 blok olması gerekirken 25,395 blok üretilmiş gibi görünmektedir. (1) ve (2) olarak belirtilen adresler blok sayısının çoklanmasına ve TOPLAM'ın 25,000'den çok olmasına sebep olmuştur.

Madenciler edindikleri maden ödülünü ilk olarak korumalı havuzdan aktarır. Bu ödülü korumalı havuza aktardıktan sonra harcarlar. Bu nedenle elde edilen tüm ödüller bir şekilde korumalı havuza aktarılır, yani bu ödülleri en azından bir kere EB-işlemi kullanılarak harcanırlar/aktarılırlar. Madenci havuzları da ilk olarak ödülü korumalı havuza gönderir. Daha sonra madencilere ödeme için pay ederler. Yukarıdaki madenci havuzları incelendiği zaman üç farklı şekilde bünyelerindeki madencilere blok ödülünden pay verdikleri görülmüştür:

Tablo 1. Son 25,000 Blok İçin Madenci Havuzları ve Madencilerinin Ürettikleri Blok Sayıları ve Kazandıkları Toplam Blok Ödüllerinin Tablosu

Muhtemel Madenci Havuzu	Üretilen Blok Sayısı	Elde Edilen Ödül (Zatsohi)
t-Havuz$_1$	6689	3,344,969,017,139
t-Havuz$_2$	4064	2,032,320,097,793
t-Havuz$_3$	3473	1,736,716,892,093
t-Havuz$_4$	3116	1,558,218,911,897
t-Havuz$_5$	1984	992,096,545,245
t-Havuz$_6$	1844	903,249,641,532
t-Havuz$_7$	1671	835,613,483,844

t-Havuz$_8$	1005	502,575,066,265
t-Madenci$_{1.1}$ (1)	192	94,800,000,000
t-Madenci$_{1.2}$ (1)	192	1,200,000,000
t-Madenci$_{1.3}$ (1)	192	0
t-Madenci$_2$	123	61,504,294,873
t-Havuz$_9$	119	59,505,023,033
t-Havuz$_{10}$	114	57,002,644,529
t-Madenci$_3$	110	55,003,940,580
t-Madenci$_4$	108	54,001,092,756
t-Madenci$_5$	59	29,503,685,602
t-Madenci$_6$	54	27,000,610,772
t-Madenci$_7$	48	24,010,592,681
t-Havuz$_{11}$	48	24,001,376,828
t-Madenci$_8$	40	20,002,890,351
t-Havuz$_{12}$	40	20,001,576,991
t-Madenci$_9$	28	14,000,407,478
t-Madenci$_{10}$	26	13,000,740,130
t-Madenci$_{11}$	16	8,000,755,908
t-Madenci$_{12.1}$ (2)	11	5,502,394,915
t-Madenci$_{12.2}$ (2)	11	0
t-Madenci$_{13}$	10	5,000,690,720
t-Madenci$_{12.3}$ (2)	6	3,000,067,198
t-Madenci$_{14}$	2	1,000,003,838
TOPLAM	**25395**	**12,482,802,444,991**

1. İlk yöntemde madenci havuzları korumalı havuzdan ZEC'leri bir t-adrese aktarır daha sonra madencilerine ödeme yaparlar. Yani zden tye bir EB-işlemi gerçekleştikten sonra ödeme tamamen şeffaf işlemler olan tden tye işlemlerle gerçekleştirilir. Bu şekilde ödeme yapan madenci havuzlarına TMadenciler denilir.
2. İkinci yöntemde madenci havuzları korumalı havuzdan doğrudan pay etme işlemi yaparlar. Bu yöntemin en çarpıcı özelliği zden tye yapılan işlemde adres ve miktarı görünmeyen bir girdiden sayısı yüzleri bu t-adreslere ödeme yapılmasıdır. Bu şekilde bir ZEC gönderimini madenci havuzları dışında hemen hemen hiçbir kimsenin yaptığı gözlemlenememiştir. Bu şekilde payı dağıtan madenci havuzlarına ZMadenciler denilir.
3. Üçüncü ve son yöntemde madenci havuzları pay dağıtımını tamamen korumalı zden zye işlemler vasıtasıyla yaparlar. Korumalı işlemleri analiz etmek mümkün olmadığı için de bu madenci havuzları korelasyon tabanlı mahremiyet analizi kapsamında incelenemişlerdir. Bu durum her ne kadar makalede elde edilecek sonuç açısından üzücü olsa da anonimliği birinci önceliği olan Zcash kriptoparası için oldukça mühim ve sevindirici bir durumdur.

3.1.1. TMadencilerin analizi

Alex Birkuyov tarafından hazırlanan [2] makalesinde bahsedilen yöntemlerden yola çıkarak TMadencilerin analizi yapılmıştır. Makalede bahsedilmiş olan ilgili analiz algoritması yüzeysel olduğundan dolayı bu algoritmadan yola çıkılarak yeni bir TMadenci bulma algoritması yazılmıştır. Bu algoritma Ek-A'da Algoritma I: TMadencilerinBulunması başlığıyla gösterilmiştir.

Algoritma 1'de yapılan analiz çalışmasından sonra bulunan *korumaliHavuzdanCoinAlanGruplanmisListesi* ile daha önce tespit edilmiş olan madenci havuzları listesi karşılaştırılır. Karşılaştırma, blok üretme ödüllerini korumalı havuza koyan madenci havuzlarının yaptıkları tden zye işlemleri çıktı toplamlarıyla *korumaliHavuzdanCoinAlanGruplanmisListesi*'ndeki muhtemel TMadencilerin yaptıkları zden tye işlemlerinin toplamı karşılaştırılır. Bu karşılaştırma sonucunda bulunan veriler aşağıdaki Tablo 2 de detaylı olarak gösterilmiştir. Ödül Adresi olarak belirtilen adresler blok ödülünü alan adreslerdir. Ödeme adresleri olarak belirtilen adresler ise ödülü alan madenci havuzunun bünyesinde bulundurdukları madencilere ödeme yaptıkları adreslerdir.

Bir madenci havuzu için birden fazla ödeme adresi olabilir. Analiz sırasında bazı adreslerin çarpraz bir şekilde birbirlerine ödeme yaptıkları gözlemlenmiştir. Bu da analiz sırasında hangi adreslerin gerçekten ödeme yapılan adres olduğu, hangi adreslerin ödeme yapılan adres olduğunu anlamayı zorlaştırmıştır. Bu nedenle bir önceki tabloda bulunan bazı madenci havuzlarının TMadenci kategorisine girdikleri tespit edildiği halde Tablo 2'deki listede yer alamamışlardır.

Aşağıdaki Tablo 2'de Ödül Adresi'nin sağındaki Blok Sayısı alanı o adresin toplamda kaç blokta tden zye EB-işlemi yaptığını verir. O alanın sağında bulunan Zatoshi Değeri alanı da o bloklarda gönderilen toplam Zatoshi cinsinden değerlerini verir. Bazı madenci havuzları blok ödüllerini biriktirip göndermeyi tercih ederken bazı madenci havuzları aldığı ödülleri doğrudan göndermeyi tercih etmişlerdir. Ödeme Adresi alanının sağındakı Blok Sayısı alanı muhtemel TMadenci adresinin yaptığı zden tye EB-işlemlerinin toplam sayısını, o alanın sağında bulunan Zatoshi Değeri alanı da bu işlemlerin toplam gönderilen Zatoshi cinsinden değerini verir.

Tablo 2. Algoritma 1 Kullanılarak Bulunan Muhtemel TMadenciler Tablosu

Ödül Adresi	**Blok Sayısı**	**Zatoshi Değeri**	**Ödeme Adresi**	**Blok Sayısı**	**Zatoshi Değeri**
t-Madenci$_{12.1}$ (2)	11	5,502,394,915	MuhtemelTMadenci$_1$	11	5,502,174,915
t-Havuz$_6$	1864	991,096,475,562	MuhtemelTMadenci$_2$	1848	991,559,348,012
t-Madenci$_2$	10	64,504,511,838	MuhtemelTMadenci$_3$	9	64,500,000,000
t-Havuz$_2$	46	2,049,331,846,484	MuhtemelTMadenci$_4$	22	2,049,331,406,484
TOPLAM	1931	1,061,103,382,315	**TOPLAM**	1890	1,061,561,522,927

Son 25,000 blok içerisinde toplamda 17,656 EB-işlemi yapılmıştır. TMadenci analizi ile yukarıdaki tabloya göre toplamda 3,821 EB-işleminin birbirleriyle ilişkisi ortaya çıkmaktadır. Bunun anlamı bütün EB-işlemlerinin %21,6'sının korumalı havuza girmelerine rağmen hangi adresten gelip hangi adrese gittiği izlenebilmekte; ayrıca hangi madenci adresinin hangi madenci havuzu bünyesinde bulunduğu tespit edilebilmektedir. TMadencilerin analizi ile son 25,000 blok için tüm EB-işlemlerinin %21,6'sının anonimliği ve mahremiyeti analiz edebilmiştir. Son 10,000 ve 50,000 blok analizi yapıldığında da yine benzer oranlar elde edilmiştir.

3.1.2. ZMadencilerin analizi

TMadenci olarak adlandırılmış olan madenci havuzları bünyesindeki madencilere ödül paylaşımını korumalı havuzdan ZEC'i çektikten sonra şeffaf işlemler vasıtasıyla yaparlar. ZMadencilerse araya fazladan bir şeffaf işlem koymaksızın ödemeleri doğrudan korumalı havuzdan madencilerine olacak şekilde yaparlar. Yani ödemeler zden tye EB-işlemleri vasıtasıyla gerçekleştirilir. ZMadencileri bulmak için kullanılmış olan algoritma Ek-B'de Algoritma II: ZMadencilerinBulunması başlığıyla gösterilmiştir. TMadenciler algoritmasında olduğu gibi ZMadenciler kullanılan algoritmada da [2] makalesinde bulunan ilgili algoritma temel alınmış ve üzerinde bazı güncellemeler yapılmıştır.

Algoritma sonucunda Muhtemel ZMadenciler bulunduktan sonra TMadencilerde yapıldığı gibi ilk olarak Tablo 1'deki madenci havuzları tablosunda tespit edilen madenci havuzlarının blok üretme ödülleri toplamıyla muhtemel ZMadencilerin gruplanmış haldeki zden tye işlemlerinin girdi değerleri toplanarak karşılaştırılır ve eşleşen kayıtlar listelenir. Yapılan karşılaştırmanın sonucu aşağıdaki Tablo 3'teki gibidir. Tablo 3'teki listede Tablo 2'deki gibi bir Ödeme Adresi alanı bulunmamasının tek nedeni ZMadencilerin ödemeyi aracı bir t-adresi olmadan doğrudan yapmalarıdır. Gruplandırılabilecek bir t-adresi olmadan, z-adresleri de gruplandırılamayacağından dolayı tespit edilen işlemler gruplandırılmıştır, bu nedenle bir Ödeme İşlemi Grubu oluşturulmuştur. Bu grup 30 ve daha fazla aynı adrese (madencilerin adresleri) sahip olan işlemlerin oluşturduğu gruptur. ZMadenciler için algoritma sonucunda ikiden fazla "işlem grubu" bulunmuştur. Ancak karşılaştırma sonucunda herhangi bir Tablo 1'deki t-adresin değeriyle eşleşme olmadığından aşağıdaki listede diğer işlem grupları

gösterilememiştir. Bunun yanında bir diğer madenci havuzu tespit etme yöntemi olan "madenci adresinden yola çıkarak madenci havuzlarını bulma yöntemi" kullanılmaya çalışılmış; ancak bu madenci havuzları yine de tespit edilememiştir. Bu durumun nedeni madenci havuzları kendi sitelerinde artık madenci adreslerini gizlemeyi tercih etmektedirler.

Tablo 3. Algoritma 2 Kullanılarak Bulunan Muhtemel ZMadenciler

Ödül Adresi	Blok Sayısı	Zatoshi Değeri	Ödeme İşlemi	Blok Sayısı	Zatoshi Değeri
t-Havuz$_{10}$	100	57,002,644,529	İşlemGrubu$_1$	98	56,955,178,696
t-Havuz$_9$	111	59,004,988,098	İşlemGrubu$_2$	109	58,828,420,000
TOPLAM	211	116,007,632,627	**TOPLAM**	207	115,783,598,696

ZMadencileri bulma algoritması sonuçlara göre toplamda 418 korumalı işlem muhtemel ZMadenci kategorisinde birbirleriyle ilişkilendirilmiştir; bu da son 25,000 bloktaki korumalı işlemlerin %02,4'ünün birbirleriyle bir ilişkisi olduğu anlamına gelir. Böylece TMadenci havuzu analizi sonuçları ile ZMadenci analizi sonuçları birleştirildiği takdirde şimdiye kadar son 25,000 bloktaki tüm korumalı işlemlerin %24'ü için korelasyon tabanlı mahremiyet analizi yapılabilmiş demektir.

TMadencilerle veya ZMadencilerle ilişkilendirilememiş toplamda 24 madenci daha bulunmaktadır. Bu madencilerden bir kısmı muhtemelen madenci havuzu değil ciddi miktarda işlemci gücü toplamış madenci adresleridir. Ayrıca bahsedilen madencilerin TMadenci ve ZMadenci algoritmalarında tespit edilememesinin en önemli nedeni yukarıda da bahsedildiği gibi bazı madenci havuzlarınının bünyesinde bulundurdukları madencilere blok ödülünden payı zden zye korumalı işlemler vasıtasıyla gerçekleştirmesidir. Kalan madencilerin 2,158 EB-işlemi daha bulunmaktadır ki, bu da tüm EB-işlemlerinin %12,2'sidir. Her ne kadar bu işlemler takip edilememiş olsa da toplamda tüm EB-işlemlerinin %36,2'sinin madenciler ve madenci havuzları ile bir şekilde ilişkili olduğu söylenebilir.

3.2. Gidiş-Geliş İşlemleri

Zcash kriptoparasını kullanan ve yaptıkları ZEC aktarımlarına mahremiyet kazandırmak isteyen Zcash kullanıcıları bunu EB-işlemleri vasıtasıyla gerçekleştirirler. Her ne kadar bir nebze anonimlik ve mahremiyet kazandırsa da bazı Zcash kullanıcıları kısa süre içerisinde tden zye, sonra da zden tye ZEC aktarımı gerçekleştirirler. Yapılan bu işlemler sonucunda da ZEC aktarımlarında tden zye işlemin değeriyle zden tye işlemin değeri aynı yahut yakın olduğu için bu iki adres arasında ilişki kurulabilmektedir. Bu ilişki sonucunda korumalı havuza giren ve korumalı havuzdan çıkan iki farklı EB-işlemi arasında doğrudan bir ilişki elde edilmiş olur. Bu şekilde analiz edilerek bulunan EB-işlemlerine gidiş-geliş işlemleri (round-trip transaction-RTT / kısaca GGİ) denir [2], [19].

Gidiş-geliş işlemleri 3 farklı yöntemle analiz edilmektedir, [2]. Bu yöntemlerin hepsinde bir ya da daha fazla tden zye işlemin girdi değeriyle bir ya da daha fazla zden tye işlemin çıktı değerleri karşılaştırılır. İlk yöntemde kısaca birer tden zye ve zden tye işlemin değerleri birbirine eşit mi değil mi diye bakılır. Bu iki değer birbirine eşitse arada bir ilişki vardır denilebilir. İkinci yöntemde bir tden zye işlem iki farklı z'ten t'ye işlemin toplamına eşit mi değil mi diye kontrol edilir. Eşitlik bulunursa yine bu işlemler arasında bir ilişki olduğu söylenebilir. Üçüncü ve sonunca yöntemde de yine bir tden zye ve zden tye işlemin değerlerinin son 4 rakamı karşılaştırılır. Son 4 rakamında benzerlik olan değerler, değerlerin kendisi birbirine yakınsa aralarında bir ilişki vardır denilir.

3.2.1. Temel karşılaştırma

Temel karşılaştırma yönteminde korumalı havuza Z aktarımı yapan bir tden zye işlem (bundan sonra t-z işlemi olarak bahsedilecektir) ile korumalı havuzdan çıkan zden tye işlem (bundan sonra z-t işlemi olarak bahsedilecektir) karşılaştırılacaktır. Karşılaştırmada basitçe korumalı havuza giren ZEC değeri ile korumalı havuzdan çıkan ZEC değeri karşılaştırılır ve birbirlerine eşit olmaları halinde bu iki işlem arasında bir ilişki olduğu varsayılır. Bu karşılaştırmadaki tek koşul t-z işleminin z-t işleminden önce gerçekleşmiş olmasıdır (yani ZEC ilk önce korumalı havuza girmiş, daha sonra korumalu havuzdan çıkmıştır).

Yapılan karşılaştırmada ilk olarak birbirine eşit değerler karşılaştırılmıştır. Daha sonra t-z işlemiyle korumalı havuza ZEC girdirdikten sonra zden zye işlem (bundan sonra z-z işlemi denilecektir) yapıp daha sonra bu ZEC'leri havuzdan z-t işlemiyle çıkartan Zcash kullanıcılarının işlemlerinin de analizi yapılmıştır. Zcash kullanıcıları burada doğrudan bir t-z işlemi yapıp hemen ardından z-t işlemi yapmak yerine bu iki işlem arasında korumalı bir (yahut daha fazla) z-z işlemi yaparak karıştırma yaparlar. Korumalı z-z işlemlerinde daha önce de bahsedildiği gibi sadece işlem bedelleri görülmektedir. Bunun için karşılaştırmaya ayrıca işlem bedelleri de dâhil edilmiştir.

Bahsedilen ilk temek karşılaştırmada karşılaştırma denklemi "t-z girdi değeri = z-t çıktı değeri" şeklindedir. İkinci karşılaştırmadaki denklem arada yapılmış olması muhtemel olan z-z korumalı işlemleri de dâhil etmek amacıyla "t-z değeri = z-t değeri + işlem

bedeli * (yapılan muhtemel z-z işlemi sayısı veya değiştirlen işlem bedeli – kullanıcılar ayrıca işlem bedellerini de değiştirebilirler)" şeklinde değiştirilmiştir. İşlem bedellerinde ilk olarak sadece varsayılan işlem bedeli olan 10^5 Zatoshi değerindeki işlemler dâhil edilmiştir. Ancak işlem bedelleri ZEC aktaran kişiler tarafından değiştirilebileceğinden yahut ZEC aktarımı yapan kişilerin birden fazla karşılaştırma işlemi (z-z işlemi) yapabileceklerinden işlem bedelleri $2*10^5$, $3*10^5$, $4*10^5$, $5*10^5$ ve $6*10^5$ olarak belirlenmiştir. En fazla işlem bedelinin $2*10^5$ olarak seçildiği yapılan karşılaştırmalarda tespit edilmiştir. Yukarıda yapılan temel gidiş-geliş işlemleri karşılaştırmalarında toplamda 1,516 farklı t-z ve z-t işlemi arasında ilişki tespit edilmiştir; bu da toplam EB-işlemlerinin işlemlerin %08,6'sına tekabül eder.

3.2.2. Alt-küme toplamlarının karşılaştırılması

Korumalı havuzda z-z işlemi yaparak "*ZEC karıştırması yapmak*" z-z işlemlerini hiç kullanmamaya nazaran daha fazla anonimlik sağlamaktadır. Ancak sonuçta doğrudan korumalı havuza giren değerle aynı yahut yakın bir değeri korumalı havuzdan çıkararak şeffaf havuzda Zcash işlemlerine devam etmek de bir önceki kısımda yapılan analiz çalışmasında da gözlemlendiği gibi yine düşünüldüğü kadar anonimlik sağlamamaktadır. Bu durumda Zcash kullanıcıları korumalı havuzdan çıkarken ellerinde bulundurdukları ZEC'leri iki yahut daha fazla parçaya bölüp bu parçaları farklı t-adreslere göndererek anonimlik ve işlem gizliliğinin artırmayı amaçlarlar. Ne var ki, ZEClerini iki parçaya bölerek korumalı havuzdan çıkartan kullanıcıların işlemlerini analiz etmenin de yöntemi bulunmaktadır.

Alt-küme Toplamlarının Karşılaştırılması durumunda iki farklı z-t işlemi çıktı değerleri toplamıyla bu değerlerin işlemlerinden önce gerçekleşmiş olan herhangi bir t-z işleminin girdi değeri birbirleriyle karşılaştırılır. Burada kullanıcı korumalı havuza t-z işlemi ile ZEC aktarmıştır, bu ZEC'i iki farklı z-adrese bölerek bu adresler aracılığıyla iki farklı z-t işlemi gerçekleştirmiştir.

Karşılaştırma sonrası bu iki değer eşleştiği takdirde bu değerler arasında bir ilişki olması muhtemeldir. Karşılaştırma işlemine başlamadan önce bir önceki yöntemde yapıldığı gibi Z-madenciler ve T-madenciler karşılaştırılacak işlemlerden çıkartılmıştır. Ayrıca buna ek olarak bir önceki karşılaştırmada tespit edilen işlemler de karşılaştırılacaklar listesinden çıkartılır. Aynı şekilde girdi ve çıktı değerlerinden yine üç defadan fazla karşılaştırmaya giren değerleri olan işlemler de listeden çıkartılır. Kalan çıktı değerlerinin hepsi toplanır, toplanan değerlerden yine üç defadan fazla çıkan değerler bulunacak karşılaştırma sonuçlarının çoklanmasını engellemek adına çıkartılır. Son olarak bir önceki yöntemin ikinci karşılaştırmasında yapıldığı gibi muhtemel z-z ara-işlemlerinin işlem bedeli değerleri z-t işlemlerinin çıktılarının toplamıyla ayrıca toplanır ve t-z işlemlerinin girdi değerleriyle karşılaştırılır.

Yapılan alt-küme toplamları karşılaştırması sonucunda 1,613 farklı girdi ve çıktı işleminin eşleştiği tespit edilmiştir. Bu da tüm EB-işlemlerinin işlemlerin %09,1'ine tekabül eder.

3.2.3. Parmak izi değerleri karşılaştırması

Zcash kullanıcıları t-z işlemi yahut z-t işlemi kullanarak ZEC aktarımı yaparken bazen gönderilecek değerdeki EB-işlemlerinin varsayılan işlem ödülü değeri olan 10.000 Zatoshi'den daha az olan kısmını görmezden gelme hatasına düşerler. "Parmak izi değeri" adı verilen bu değer kullanılarak iki farklı işlemin girdi ve çıktı değerleri arasında bir ilişki kurmak mümkün olmaktadır. Daha önceki karşılaştırma denklemlerinde olduğu gibi bu karşılaştırma denkleminde de T-Madencilerin işlemleri, Z-Madencilerin işlemleri ve daha önceki her iki yöntemdeki karşılaştırmalarda tespit edilen işlemler karşılaştırılacaklar listesinden çıkartılır. Ayrıca parmak izi değeri üç kereden daha fazla kez listeye giren değerlere ait işlemler de parmaz izi değerleri karşılaştırması analizindeki karşılaştırılacaklar listesinden çıkartılır. Bu karşılaştırmada t-z işlemi girdi değeriyle z-t işlemi çıktı değeri son 4 rakamı eşit olan tüm işlemler bulunur. Burada dikkat edilmesi gereken en önemk-li nokta girdi değerinin çıktı değerinden büyük olması; ancak çok büyük olmamasıdır. Bu nedenle karşılaştırılarak bulunan işlemlerin değerleri (Girdi_Değeri / Çıktı_Değeri) -1<0.01 olacak şekilde bir denkleme sokulur. Bu denklem sonucunda 593 farklı t-z ve z-t işlemi bulunur. Bu da tüm EB-işlemlerinin %03,4'üne tekabül eder.

3.3. Zcash Analizi Sonuçları

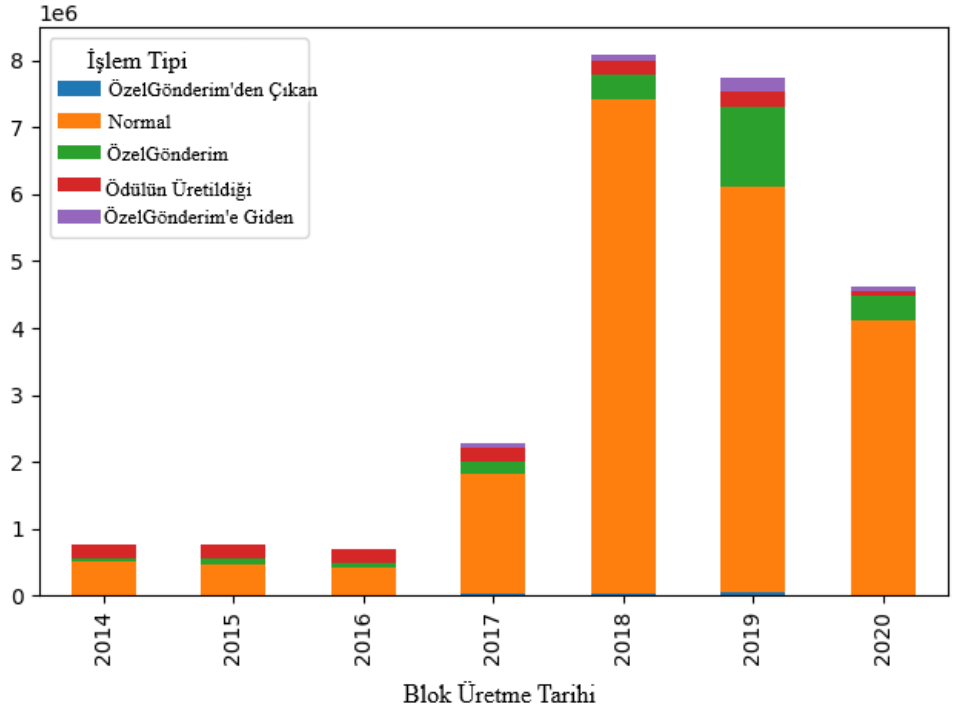
Yukarıda detaylı bir şekilde anlatılan korelasyon tabanlı mahremiyet analizi işlemlerinin sonucunda son 25,000 bloktaki toplam 7,961 EB-işleminde tam olarak bir ilişki tespit edilebilmiştir ki, bu da tüm EB-işlemlerinin %45,1'idir. Bu ilişkiler haricinde 2,158 ödülü alan madenci havuzu yahut madencinin yapmış olduğu t-z işlemi, 325 Zcash sahiplerinin yapmış olduğu t-z işlemi, 783 TMadenci şartlarına uyan z-t işlemi ve 23 ZMadenci şartlarına uyan z-t işlemi tespit edilmiştir. Bu adresler ve işlemler tek taraflı analiz edilebilen ancak kime ait olduğu "kesinlikle" belli olan ve toplam EB-işlemlerinin %18,6'lık kısma tekabül eden adres ve işlemlerdir. Toplamda bu şekilde olan 3,289 işlem tespit edilmiştir.

Zcash kriptoparası için son 25,000 bloktaki EB-işlemlerinin tam olarak 4,302 tanesi, yani %24,6'sı z-z işlemidir. Bu işlemleri mevcut yöntemlerle analiz etmek mümkün değildir. Bu nedenle analiz edilebilme ihtimali olan EB-işlemlerinden z-z işlemleri çıkartıldığı takdirde kalan tüm EB-işlemlerinin %84,4'ü için bir şekilde ilişkilendirilme yapılmıştır. Sonuç olarak Zcash anonim kriptoparası pratikte istenilen seviyede anonim değildir.

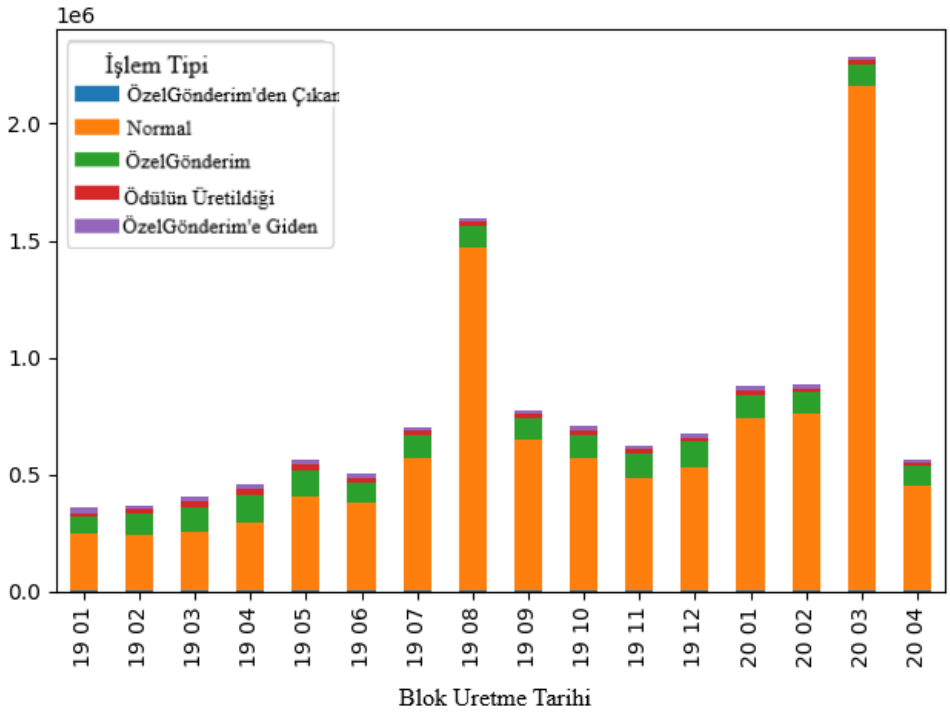
IV. DASH ANALİZİ (ANALYSIS OF DASH)

Dash analizi 26 Nisan 2020 16:23:44 tarihinde başlatılmıştır. Bu tarihte üretilen en son blok 1297693. bloktur. Zcash analizinde olduğu gibi 1297693. bloktan sonra üretilmiş bloklar ve bloklara ait işlemler analize dâhil edilmeyecektir. Korelasyon tabanlı mahremiyet analizinde yapılacak olan madenci havuzu analizleriyle gidiş-geliş işlemleri analizi yine aynı şekilde Zcash anonim kriptoparasında yapıldığı gibi son 25,000 blok temel alınarak yapılacaktır.

Zcash'teki işlemler EB-işlemleri ve şeffaf işlemler olarak ikiye ayrılırken tüm işlemleri şeffaf olan Dash'in işlemleri, ÖzelGönderim kullanılarak anonimlik sağlayan karıştırma işlemleri (mixing transactions) ve normal işlemler olmak üzere ikiye ayrılır. Doğrudan bu karıştırma işlemlerini analiz etmek, karıştırmada kullanılan adreslerin sadece o işleme özel (tek kullanımlık) olmaları nedeniyle gruplandırılamayacaklarından dolayı mümkün değildir. ÖzelGönderim işlemleri bu nedenle bir nevi Zcash'teki zden zye korumalı işlemlerine benzer. Zcash için yapılan analiz korumalı havuza giren tden zye ve korumalı havuzdan çıkan zden tye işlemler kullanılarak mümkün olmaktadır. Bu nedenle Dash'in analiz edilebilmesi için ÖzelGönderim dışındaki normal işlemleri analiz edilebilecek şekilde gruplandırmak gerekmektedir.



Şekil 6. Yıllara Göre Kullanıcılar Tarafından Dash İşlem Tiplerinin Tercih Edilme Oranları



Şekil 7. 2019 ve 2020 Yılları İçin Aylara Göre Kullanıcılar Tarafından Dash İşlem Tiplerinin Tercih Edilme Oranları

Dash anonim kriptoparası için korelasyon tabanlı mahremiyet analizi gerçekleştirebilmek adına tüm işlem tipleri aşağıdaki gibi 5 parçaya bölünmüştür:

1. **Normal İşlemler:** Bitcoin'deki işlemlerin aynısıdır. Zcash anonim kriptoparasında bu işlemler şeffaf işlemler olarak geçer. Dash'te bulunan bu normal işlemler mahremiyet analizine dâhil edilmeyecektir.
2. **Ödül İşlemleri:** Bloğu oluşturan madenciyle beraber AnaUç'a blok ödülünün verildiği işlemdir. Bitcoin ve Zcash gibi tüm kriptoparalarda bu işlemler bulunur. Girdi adresi daima boştur ve işlem ücreti sıfırdır. Girdi değeri üretilen blok ödülüyle blok içerisinde geçen işlemlerin işlem bedeli değerlerinin toplamıdır. Normal işlemlerde olduğu gibi analize dâhil edilmez.
3. **ÖzelGönderim İşlemleri:** Dash anonim kriptoparası için "anonimliğin" gerçekleştirildiği işlemlerdir. 2.4 Dash bölümünde detaytlı bir şekilde anlatılmışlardır. Yapılan korelasyon tabanlı mahremiyet analizi açısından incelendiği zaman Zcash'teki zden zye korumalı işlemlere benzerler. Girdi sayısı ile çıktı sayısı ve girdi değeri toplamı ile çıktı değeri toplamı daima aynıdır, işlem ücreti sıfırdır. Korelasyon tabanlı mahremiye analizini gerçekleştirmek adres gruplaması yapılamadığından mümkün değildir, bu nedenle mahremiyet analizine dâhil edilmezler.
4. **ÖzelGönderim'e Giden İşlemler:** Elindeki Dash'i anonimleştirmek isteyen kullanıcı, bu Dash'leri yukarıdaki 3. maddede anlatılan ÖzelGönderim işlemlerine dâhil eder. Dash gezginleri incelendiği zaman ÖzelGönderim işlemlerinden hemen önceki işlemde ilgili Dash değerinin parçalanıp farklı adrese bölündüğü gözlemlenecektir. Dash'lerin ÖzelGönderim öncesi parçalandığı işlemlere ÖzelGönderim'e Giden İşlemler adı verilir. İşlem ücreti sıfırdan büyüktür. Bu işlemleri tespit etmek çıktı adreslerinin değerlerine bakılır. Eğer 2 ya da daha fazla 1.00001 sayısına bölünen çıktı adresi değeri varsa bu işlem ÖzelGönderim'e Giden İşlemdir. Zcash anonim kriptoparasındaki tden zye işlemlere benzerler. Dash anonim kriptoparası için mahremiyet analizine dâhil edilmiş olan ilk işlem tipidir.
5. **ÖzelGönderim'den Çıkan İşlemler:** ÖzelGönderim'e Giden İşlemlerin aksine ÖzelGönderim kullanılarak anonimleşmesi sağlanan Dash'lerin sahipleri tarafından harcanmak vs. gibi sebeplerle kullanıcının cüzdanlarına geri ödendiği işlemlerdir. Yani anonimleştirilen Dash'lerin tekrardan bir adrese kümelendirildiği işlemlerdir. İşlem ücreti sıfırdan büyüktür. Bu işlemleri tespit etmek için bu sefer girdi adreslerinin girdi değerlerine bakılır. Eğer 2 ya da daha fazla 1.00001 sayısına bölünen girdi adresi değeri varsa bu işlem ÖzelGönderim'den Çıkan İşlemdir. Zcash anonim kriptoparasındaki zden tye işlemlere benzerler. Dash anonim kriptoparası için mahremiyet analizine dâhil edilmiş olan bir diğer işlem tipidir.

Yukarıda gösterilmekte olan Şekil 6 ve Şekil 7'de Dash işlem tiplerinin iki farklı zaman aralığı için grafikleri verilmiştir. Şekil 6'da Dash'in ilk çıktığı 2014 yılından analiz için belirlenen en son blok olan 1260895 nolu bloğa kadar olan, yani 26 Nisan 2020 tarihine kadar üretilmiş olan tüm bloklarının işlem tiplerine göre toplam kullanılma sayılarının grafiği verilmiştir. Şekil 7'de ise 2019 ile 2020 yılları içinde 01 Ocak 2019 tarihinde üretilen ilk bloktan yine 1260895. bloğa kadar aylara ve yıllara göre tüm bloklarının işlem tiplerine göre toplam kullanılma sayılarının grafiği verilmiştir. Her iki grafikte de sol üstte görünen *1e6* ifadesi y eksenindeki değerlerin 1,000,000'ın katları olduğunu belirtir. Mesela Şekil 6'da 2017 yılı için x ekseninde bulunan Normal İşlem verisinin y eksenindeki değeri ortala 2'dir. Bunun anlamı 2017 yılında Dash kullanıcıları yaklaşık 2,000,000 civarında Normal İşlem gerçekleştirmişler demektir.

Şekil 6'daki grafik incelendiği zaman Dash kullanımının 2017 yılında bir anda ciddi bir şekilde arttığı açıkça görülmektedir. Grafikte tüm yıllar için ÖzelGönderim işlemlerini kullanıcılar tarafından çok fazla tercih edilmediği aşikârdır. Aynı durum Şekil 7'de bulunan grafikte de görünmektedir. Bu iki grafik incelendiği zaman anlaşılacağı üzere Dash kullanıcıları büyük çoğunlukla normal işlemleri yapmayı tercih etmektedir. Tablo 4'te Şekil 6'da gösterilmekte olan ilk bloktan 1260895. bloğa kadar yapılan tüm işlemlerin işlem tipine göre toplam kullanılma/tercih edilme sayıları verilmiştir. ÖzelGönderim işlemleri, ÖzelGönderim'e Giden işlemler ve ÖzelGönderim'den Gelen işlemler; yani ÖzelGönderim ile alakalı işlemlerin "toplamının" tüm işlemlerin toplamına oranı Tablo 4'te görüldüğü gibi %11.79 olmaktadır.

Tablo 4. 129769. Bloğa Kadar Tiplere Göre Dash İşlemleri Sayıları ve Yüzdeleri

Dash Blokzinciri İşlem Tipi	**Toplam İşlem Sayısı**	**Toplam İşlem Sayısı Yüzdesi**
ÖzelGönderim'e Giden	493,818	1.976501384
ÖzelGönderim'den Gelen	147,193	0.589138444
ÖzelGönderim	2,305,085	9.226078621
Normal	20,732,384	82.98115028
Blok Ödülü	1,305,970	5.227131276
TOPLAM	24,984,450	100.00

Dash anonim kriptoparası için daha efektif bir korelasyon tabanlı mahremiye analizi yapabilmek adına Zcash anonim kriptoparasında da yapıldığı gibi ilgili analiz çalışması son 25,000 blok için yapılmıştır. Tablo 5'te son 25,000 blok için kullanıcıların tercih ettikleri toplam işlem tipi sayıları ve yüzdeleri verilmiştir. Son 25,000 blokta ÖzelGönderim ile alakalı işlemler toplamda 179,995 işlemdir (ÖzelGönderim işlemleri, ÖzelGönderim'e Giden işlemler ve ÖzelGönderim'den Gelen işlemler). ÖzelGönderim ile alakalı işlemler toplamının tüm işlemler toplamına oranı %6,81 oranına gerilemiştir.

Korelasyon tabanlı mahremiyet analizi çalışması Dash anonim kriptoparası için ise sadece ÖzelGönderim'e Giden işlemler ve ÖzelGönderim'den Gelen işlemler için yapılacaktır. Bu iki işlem tipinin toplam sayısıysa tüm işlemler sayısının %1.13'üne tekabül eden 29,894 tane işlemdir. Yani korelasyon tabanlı mahremiyet analizi tüm işlemlerin sadece %1,13'ü için yapılacaktır. %5,68 oranında olan ÖzelGönderim işlemleri için korelasyon tabanlı mahremiyet analizi yapılamamaktadır. Kalan %93,19 oranındaki Normal işlemler ve Blok Ödülü işlemlerini analiz etmeye gerek bulunmamaktadır.

Tablo 5. Son 25,000 Blok İçin Tiplere Göre Dash İşlemleri Sayıları ve Yüzdeleri

Dash Blokzinciri İşlem Tipi	**Toplam İşlem Sayısı**	**Toplam İşlem Sayısı Yüzdesi**
ÖzelGönderim'e Giden	23,558	0.890872471
ÖzelGönderim'den Gelen	6,336	0.239603021
ÖzelGönderim	150,101	5.676239443
Normal	2,436,524	92.13991667
Blok Ödülü	27,855	1.053368396
TOPLAM	2,644,374	100.00

4.1. Madencilerin Analizi

Zcash'den farklı olarak Dash kriptoparasında blok ödülleri madencilerle beraber aynı zamanda AnaUçlara da gönderilir. Ancak hangi adresin AnaUça, hangi adresin madenciye ait olup olmadığını bilmek doğrudan mümkün değildir. Bu nedenle madenci havuzlarının mahremiyet analizine madenci havuzlarına ait adreslerle beraber mecburen AnaUçlara ait olan adresler de eklenmişitr. Madenci havuzlarını ve yaptıkları anonim işlemlerini tespit etmek için Zcash'te olduğu gibi yine bünyesinde bulundurdukları madencilere yaptıkları ödemeler gruplandırılarak analiz işlemi yapılmıştır. Madenci havuzu, Dashleri "normal işlemleri" kullanarak ödeme yapıyorsa TMadenci, "ÖzelGönderim'den çıkan işlemleri" kullanıyorsa ZMadenci olacaktır.

İlk olarak tüm Ödül İşlemlerine çıktı olan tüm adresler AnaUç olup olmadığını bakılmaksızın madenci olarak varsayılmıştır. Daha sonra bu adreslerden yine aynı 25,000 bloğu içerisinde ÖzelGönderim'e Giden İşlemler listesinde girdi adresi olarak tespit edilen adresler listelenir. Ödülü alan olası madenci havuzlarının tespitinden sonra sıra ödülü madencilere dağıtan TMadencilerle ZMadencileri tespit etmeye gelir. Bu işlem Zcash için uygulanan algoritmaya benzer bir algoritmayla gerçekleştirilir. İlk olarak yapılan TMadencilerin bulunması analizi sonrası elde edilen sonuçlar aşağıdaki tablodaki gibidir:

Tablo 6. Dash İçin Muhtemel TMadenciler

Havuz Adresleri	Dash Değeri	İşlem Sayısı	TMadenci Adresleri	Dash Değeri	İşlem Sayısı
$HavuzGrubu_1$	852,530,786	6	$MuhtemelTMadenci_1$	852,476,979	1
$HavuzGrubu_2$	10,899,071	6	$MuhtemelTMadenci_2$	10,840,118	1

Yukarıdaki gösterilen Tablo 6'da TMadenci olarak tespit edilen kayıtlar gösterilmektedir. ZMadenci olaraksa hiçbir kayıt bulunamamamıştır. Ödül adresini ÖzelGönderim'e gönderen toplamda 12 işlem ve ÖzelGönderim'den ödülleri alarak madencilere paylaştıran toplam 2 işlem tespit edilmiştir. Toplamda bulunan 14 işlem son 25,000 bloktaki analiz edilecek olan ÖzelGönderim'e Giden işlemlerle ÖzelGönderim'den Çıkan işlelerim toplamının %0.468321402 kadarına denk düşmektedir. Oldukça düşük bir değer tespit edilmesinden dolayı madenci analizi işlemleri Dash için maalesef gözardı edilecek, mahremiyet analizi sonuçlarına dâhil edilmeyeceklerdir.

4.2. Gidiş-Geliş İşlemleri

Gidiş-Geliş işlemleri Dash kriptoparası için "t" zamanında gerçekleşmiş bir ÖzelGönderim'e Giden İşlemle (bundan sonra "ÖGG işlemi" denilecektir) "$t+t_1$" zamanında (yani daha sonraki herhangi bir zamanda) gerçekleşmiş bir ÖzelGönderim'den Çıkan İşlemin (aynı şekilde bundan sonra "ÖGÇ işlemi" denilecektir) karşılaştırılmasıdır. Yani aslında Zcash'te yapılmış olan gidiş-geliş işlemleri analizine benzer bir yöntem uygulanır. Zcash'de yapılan girdi ve çıktı değerleri karşılaştırmasına Dash için de ÖGG işleminin çıktı toplamı ve ÖGÇ işleminin girdi toplamı değerleri karşılaştırılır.

4.2.1. Temel Karşılaştırma

Gidiş-geliş işlemleri karşılaştırmasında ilk olarak temel karşılaştırma yapılır. Yine Zcash analiznde olduğu gibi"t" zamanında ÖzelGönderim'e giden "ÖGG" işlemiyle "$t+t_1$" zamanında ÖzelGönderim'den çıkan başka bir "ÖGÇ" işlemi karşılaştırılır. ÖGG işleminin 10'un katsayılarına ayrılmış çıktı adresleri değerleri toplamıyla ÖGÇ işleminin 10'un katsayılarına ayrılmış girdi adresleri değerleri toplamı karşılaştırılır ve birebir eşleşen kayıtlar listelenir.

Karşılaştırma işlemi sonrasında toplamda 8795 farklı işlemin listeye girdiği gözlemlenmiştir. Liste incelendiği zaman bazı Dash miktarı adres sayısı ikililerin onlarca defa listeye girdiği görülmektedir. Örnek vermek gerekirse 24002972. numaralı indekse sahip işlem toplamda 64 farklı başka işlemle ilişkilendirilmiştir. Bu durumda 100 kez yahut daha az listeye giren 4427 işlem, 25 kez yahut daha az listeye giren 1400 işlem ve 7 kez yahut daha az listeye giren 510 işlem tespit edilmiştir. Birebir eşleşen girdi adres toplamı ve çıktı adres toplamı olan işlemlerin sayısı ise 76'dır.

4.2.2. Alt-küme toplamlarının karşılaştırılması

Diğer bir gidiş-geliş işlemleri karşılaştırması olan "Alt-küme Toplamlarının Karşılaştırılması" Dash anonim kriptoparası Zcash'te yapılana benzer bir mantık uygulanarak gerçekleştirilir. İlk olarak "t" zamanında gerçekleştirilmiş bir ÖGG işleminin 10'un katsayısı olan çıktı adresleri değerleri toplamıyla "$t+t_1$" ve "$t+t_2$ ($t+t_1$ ile $t+t_2$ zamanları aynı yahut farklı zamanlar olabilir) zamanlarında gerçekleştirilmiş 2 farklı ÖGÇ işlemlerinin 10'un katsayısı olan girdi adreslerinin değerlerinin toplamı karşılaştırılır. Karşılaştırma sonucunda birebir eş olan işlemler kümesi listeye eklenir.

Karşılaştırma sonucunda toplamda 10417 farklı işlemin listeye girdiği gözlemlenmiştir. İlk gidiş-geliş işlemleri karşılaştırılması listesinde olduğu gibi bu listede de aynı Dash miktarına sahip bazı işlemlerin onlarca defa listeye girdikleri gözlemlenmiştir. Bu sefer $ÖGÇ_1$ girdi değeri, $ÖGÇ_2$ girdi değeri ve bu iki değerlerin toplamıyla $ÖGÇ_1$ işlem indeksi ve $ÖGÇ_2$ işlem indeksleri temel alınarak tüm liste gruplandırılır.

Gruplandırma sonucunda hala aynı işlemlerin onlarca hatta daha fazla kez karşılaştırma sonucu listesine girdiği görülmüştür. Listedeki toplam görünme sayıları (count) gruplandığı zaman 100 kez yahut daha az listeye giren 10392 işlem, 25 kez yahut daha az listeye giren 10183 işlem ve 7 kez yahut daha az listeye giren 9954 işlem tespit edilmiştir. Birebir eşleşen girdi adres toplamı ve çıktı adres toplamı olan işlemlerin sayısı ise 7832'dir. Her iki listenden çıkan sonuçlar Tablo 7'de aşağıdaki gibi verilmiştir:

Tablo 7. Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu

Karşılaştırmada Adres Görülme Sayısı	Temel Karşılaştırma	Temel Karşılaştırma Yüzdesi	Alt Küme Toplamları Karşılaştırması	Alt Küme Toplamları Karşılaştırması Yüzdesi	Karşılaştırma Toplamı	Karşılaştırma Toplamı Yüzdesi
Sadece 1 Defa	76	%0.254	7,832	%26.199	7,833	%26.202
7 ve Daha Az	510	%1.706	9,954	%33.298	9,971	%33.354
25 ve Daha Az	1,400	%4.683	10,183	%34.064	10,387	%34.746
100 ve Daha Az	4,427	%14.808	10,392	%34.763	11,698	%39.131
Hepsi	8,795	%29.421	10,417	%34.846	14,739	%49.304

Tablo 7'de ilk olarak her iki listede sadece bir kez karşılaştırmada görünen işlemlerin sayısı gösterilmiştir. Daha sonra sırayla 7 kez ve daha az görünen, 25 kez ve daha az görünen, 100 kez ve daha az görünen işlemlerin sayısı gösterilmiş; en sonda da listede bulunan tespit edilmiş tüm işlemlerin sayısı verilmiştir. Her bir sayının yanındaki "Yüzde" olarak belirtilen alan ÖGG ve ÖGÇ işlemlerin toplamı olan 29894 sayısına göre ilgili karşılaştırma sayısının yüzdesini verir.

Korelasyon tabanlı mahremiyet analizinden olan alt-küme toplamları karşılaştırması sonucunda birebir karşılaştırılabilme ihtimali olan %26.202 oranında işlem bulunmuştur. Bu karşılaştırmalardaki önemli olan nokta şudur; gruplandırma sırasında listede görünme sayısı arttıkça iki işlem arasında tutarlı bir ilişkilendirme yapıp işlemin takip edilebilmesi azalmaktadır. Bunun yanında yapılan ilişkilendirmenin geçerliliği (yani gerçekten de iki işlem arasında ilişki olup olmadığının tespit edilmesi) ÖzelGönderim'den çıkan işlemde olan tüm karıştırmalardaki adreslerden geriye giderek anlaşılabilir. Mesela X_1 işlemi ÖGG işlem ve X_2 ÖGÇ işlemi olsun. Listede bu iki işlem arasında ilişki olması ihtimalinin belirtilmesi durumunda X_2 işlemine girdi olan $X_{1.A}$, $X_{1.B}$, $X_{1.C}$ şeklindeki tüm adreslere bakılır. Daha sonra bunların çıktısı olduğu ÖzelGönderim işlemlerinde bulunan tüm işlemlerin $X_{1.A.1}$, $X_{1.A.2}$, $X_{1.A.3}$, $X_{1.b.1}$ $X_{1.b.2}$, $X_{1.b.3}$, $X_{1.c.1}$, $X_{1.c.2}$ ve $X_{1.c.3}$ şeklindeki girdi adreslerine gidilir. Her bir geriye gidilen seferin bir önceki muhtemel ilişki yolu sayısıyla mevcut ÖzelGönderim işleminin girdi adresi sayısı çarpılır. Yukarıdaki durumda ilk ÖzelGönderim işleminde 3 ilişki ihtimali varken ikincisinde 9, üçüncüsünde 27 ve dördüncüsünde 81 ilişki ihtimali olacaktır, bu durum her bir ÖzelGönderim işlemi tam olarak 3 adresle yapıldığı varsayılarak hesaplanmıştır. Yapılan sefer sayısı arttıkça ilişkilendirmeyi doğrulamanın zorluğu da yine ciddi bir şekilde artacaktır. Buna karşılaştırma sonuç listelerindeki işlemin görünme sayılarının artmasını da eklersek özellikle 7 defadan daha fazla listeye giren işlemlerin doğrulanmasını ne derece zorlaştığı daha iyi anlaşılacaktır. Yine de bu durum bütün ÖzelGönderim işlemlerinde girdi-çıktı ikililerinin tamamını teker teker deneyerek ÖGG işlemleriyle ile ÖGÇ işlemleri arasındaki ilişkiyi körlemesine bir yöntem ile bulmaktan daha kolay ve hızlı olacaktır. Bu durum şu şekilde düşünülebilir; Kaba Kuvvet (Brute Force) kullanarak bir şifreleme algoritmasını kırabilmek için m*n*t değer zaman kadar sürdüğü varsayılsın. Bu süreyi n birim zaman kadar azaltarak m*t kadar süreye düşürmek algoritmanın çok daha kolay kırılmasına olanak sağlayacaktır ki, şifreleme algoritmasını kırmak tam olarak bu durumu ifade eder. Yapılan analiz çalışması sayesinde bir Dash işleminin mesela x*y sayıda Dash işlemiyle olabilecek olası ilişki sayısı ihtimali mahremiyet analizi sayesinde x Dash işlemine düşürülmüştür.

Daha sonra, gidiş-geliş işlemleri mahremiyet analizi çalışmasına ek olarak Zcash anonim kriptoparasından farklı olarak Dash anonim kriptoparası için ÖGG işlemlerinin çıktı adresleri sayısıyla ÖGÇ işlemlerin girdi adresleri sayısı karşılaştırmaya eklenmiştir. Çünkü kullanıcılar, ÖzelGönderim'e girdikleri Dash miktarının tamamını olduğu gibi cüzdanlarındaki bir adreste toplayıp harcayabilmek istedikleri takdirde parçalanan tüm Dash'lerin bulunduğu adresleri girdi olarak yeni bir ÖGÇ işlemine dâhil etmeleri gerekir. Bu durumda ÖGG işleminin toplam çıktı sayısı ile ÖGÇ işleminin toplam girdi sayısı aynı olacaktır. Bu nedenle toplam Dash değerlerinin eşit olmasının yanında toplam girdi-çıktı adres sayılarının eşit olması koşulu da analiz karşılaştırılmasına eklenmiştir. Adres sayılarının eş olması koşulunun karşılaştırma analizine eklenmesiyle çıkan sonuçlar Tablo 8'de aşağıdaki gibi verilmiştir.

Tablo 8. Adres Sayıları Dâhil Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu

Karşılaştırmada Adres Görülme Sayısı	Temel Karşılaştırma	Temel Karşılaştırma Yüzdesi	Alt Küme Toplamları Karşılaştırması	Alt Küme Toplamları Karşılaştırması Yüzdesi	Karşılaştırma Toplamı	Karşılaştırma Toplamı Yüzdesi
Sadece 1 Defa	41	%0.137	3,187	%10.661	3,201	%10.708
7 ve Daha Az	289	%0.967	6,160	%20.606	6,188	%20.700
25 ve Daha Az	843	%2.820	6,992	%23.389	7,216	%24.139
100 ve Daha Az	2,743	%9.176	7,280	%24.353	8,417	%28.156
Hepsi	4,861	%16.261	7,607	%25.447	10,688	%35.753

Yapılan yeni gidiş-geliş işlemleri mahremiyet analizleri neticesinde hem temel karşılaştırma için hemn de alt-küme toplamları karşılaştırması için elde edilen toplam işlem sayısı yüzdesinin önemli ölçüde azaldığı gözlemlenmektedir. Örnek olarak sadece 1 defa eşleşen toplam işlem sayısı 7,883'en 3,201'e düşmüştür. Yine toplamda 14,739 işlem değil 10,688 işlem tespit edilmiştir. Her ne kadar toplam bulunan sonuç açısından bir azalma olduğu düşünülse de bu muhtemel ilişkilerin gerçekten var olup olmadığı tespit etmek isteyen için bu durum kolaylık sağlayacaktır.

4.2.3. Parmak izi değerleri karşılaştırması

ÖzelGönderim'e girebilecek en küçük değer 0.001 Dash olduğundan ve bu değer de varsayılan işlem ücretinden büyük olduğundan parmak izi gidiş-geliş işlemleri analizi Dash için yapılmayacaktır.

4.3. Dash Analizi Sonuçları

Gidiş-geliş işlemleri mahremiyet analiz çalışmasında ilk aşamada sadece işlemlerin toplam girdi ve çıktı değerleri karşılaştırması yapılmış ve bu karşılaştırma sonucunda tüm ÖzelGönderim'e giden ve ÖzelGönderim'den gelen işlemlerin %49,304'ü için ilişkilendirilme yapılmıştır. İlgili mahremiyet analizine işlemlerde bulunan girdi ve çıktı adreslerinin toplam sayılarının eşit olması koşulu da eklendiğinde bu oranın %35,753'e düştüğü gözlemlenmiştir. Yapılan ilişkilendirmeler "ÖGG Xt_1 ve ÖGÇ Xt_2 işlemlerinin adres sayıları ve işlem değerleri birbirine eşittir; bu nedenle aralarında bir ilişki olması muhtemeldir." varsayımı temel alınarak yapılmıştır. Ne var ki, ilişkinin doğrulaması tez konusu kapsamında olmadığı için detaylıca açıklanmamış ve ilişkiyi doğrulayan herhangi bir çalışma yapılmamıştır. Dash kriptoparası tamamıyla umumi yani herkese açık bir kriptopara olduğundan, ilişkilendirmenin doğru olmasını kontrol etmek amacıyla ÖGÇ Xt_2 işleminden tüm ÖzelGönderim adresleri kullanılarak geriye doğru gitmek yeterli olacaktır.

Dash anonim kriptoparası için madenci havuzları kullanılarak bir analiz yapılmamıştır. Bu nedenle mahremiyet analizi sonuçları sadece gidiş-geliş işlemlrinde bulunan sonuçlardır.

V. MONERO ANALİZİ (ANALYSIS OF MONERO)

2.5 Monero alt-kısmında kısaca anlatıldığı gibi Monero oldukça popüler bir anonim kriptoparadır ve Bitcoin'den sonra en önemli ilk 10 kriptoparadan birisi olduğu bazı kaynaklar tarafından belirtilir[3]. Ne var ki, korelasyon tabanlı mahremiyet analizi çalışması kapsamında bir analiz çalışması yapılamamıştır. Bunun temel nedeni şudur; yapılan tez çalışması farklı zamanlarda, yani farklı bloklarda gerçekleştirilmiş olan işlemlerin toplam işlem değerlerinin birbirleriyle karşılaştırılarak arada bir ilişki bulunması üzerine odaklanır. Mesela Zcash için t_1 zamanında yapılmış bir t-z işleminin toplam girdi değeriyle $t_1 + t_i$ zamanında (yani daha sonra) yapılmış bir z-t işleminin çıktı değerleri toplamı karşılaştırılır. İki değerin birbirine eş olması durumunda arada bir ilişki vardır denilebilir. Monero'daki ödül işlemleri hariç tüm işlemlerin girdi ve çıktı değerlerinin herkese açık olan kayıt defterlerinde özetlenerek yahut tamamıyla gizlendiği için bu değerleri herhangi bir şekilde gruplandırarak veya gruplandırmadan doğrudan karşılaştırmak mümkün olmamaktadır. Sonuç olarak Monero anonim kriptoparası için korelasyon tabanlı mahremiyet analizi yapılamamıştır.

VI. TARTIŞMA VE ÖNERİLER (DISCUSSION AND SUGGESTION)

6.1. Tartışma

Bitcoin kriptoparası her ne kadar ilk çıktığında anonim olduğu düşünülse de açık anahtarlı adres kullandığı için hiçbir şekilde anonim olmadığı zaman içerisinde anlaşılmıştır. Çünkü bu açık anahtarlı adres kullanılarak Bitcoin defterinde tüm işlem geçmişini rahatlıkla görüntülenebilmekter. Bu nedenle Bitcoin için daha fazla anonimlik sağlaması adına çeşitli yöntemler

[3] https://www.investopedia.com web sayfasında bu iddia detaylı olarak belirtilmiştir.

önerilmiştir. Bu yöntemlerin de arzu edilen anonimliği sağlamadığı anlaşılınca korelasyon tabanlı mahremiyet analizi çalışmasının temel konusu olan anonim kriptoparalar yayınlanmıştır.

Bahsedilen bu anonim kriptoparalar teoride çeşitli kriptografik yöntemler yahut Zerocash gibi protokollerle çeşitli şekillerde güçlü bir anonimleştirme sağlarlar. Ne var ki, kriptosistemde bulunan ve blokzincir teknolojisi bünyesindeki elemanları haricindeki cüzdanlar yahut eşler arası ağ gibi elemanları analiz edildiğinde [24] ve [26] makalelerinde belirtilen örneklerinde olduğu gibi anonimliği bozma yapılabilmektedir. Bunun yanında anonim kriptoparalarla işlem yapan çeşitli kullanıcı adresleri analiz edildiğinde de yine anonimliği bozma yapılabildiği gözlemlenmiştir. Bu anoninmliği bozma yöntemine "korelasyon tabanlı mahremiyet analizi" adı verilir.

Zcash ve Dash gibi anonim kriptoparaların anonimsizleştirilebilmesinin temel sebeplerini aşağıdaki gibi listelemek mümkündür:

- Bilgi güvenliğinde en zayıf halkanın "insan" olduğu her zaman vurgulanmıştır. Kriptoparalarda da bu durum maalesef farklı değildir. Zcash ve Dash analizi sırasında normal kullanıcıların anonim işlemleri yaparken yeterince bilinçli davranmadıkları gözlemlenmiştir. Örnek vermek gerekirse kullanıcının t_1 zamanında yapmış olduğu X_1 işlemini işlem gizliliğini sağlamak adına anonimliğin sağlandığı EkleBöl yahut ÖzelGönderim yöntemi kullandıktan sadece saatler sonra, $t_1 + t_i$ zamanında X_2 işlemini yaparak aynı değerle ilgili anonimliği sağlayan yöntemden çıkıp kendisine ödeme yapması bu iki işlem arasında bir ilişki kurulmasına neden olmaktadır.
- Kriptoparalarda farklı kullanıcı grupları bulunmaktadır. Bu kullanıcı gruplarından madenciler kriptoparalar için en önemli görevlerden birisi olan blokzincire yeni blokların eklenmesi görevini belli bir blok ödülü karşılığında icra ederler. Bundan dolayı madenci havuzları ve madenciler için hususi olarak yapılan anonimsezliştirme yöntemleri geliştirilmiştir. Gerçekten de madenci havuzlar Zcash kriptoparasında olduğu gibi sürekli olarak benzer şekilde madencilere ödeme yaparlar. Korumalı havuzları kullandıkları halde bu madenci havuzlarını analiz etmek mümkün olmaktadır. Sonuç olarak madenci havuzlarının yaptığı işlemler daha kolay analiz edilerek anonimsizleştirilebilir olur.
- Zcash kriptoparası için işlemlerin kolay takip edilebilir olmasının en temel sebeplerinden birisi z-z korumalı işlemlerin sayısının olması gereken seviyelerde olmamasıdır. Sadece korumalı işlemin yapılması da takip edilememezliğin, dolayısıyla anonimliğin ve mahremiyetin sağlanması için yeterli olmaz. Korumalı havuza girdirilen değerlerin korumalı havuzun dışarısına çıkartıldığında hiçbir şekilde birleştirilemeyecek şekilde parçalanarak çıkartılması alternatif olarak önerilir.
- Dash kriptoparası düşünüldüğü zaman ÖzelGönderim işlemleri 10'un katsayılarına bölündüğünde kullanıcılar aynı şekilde bu bölünmüş değerleri tek bir adres üzerinde muhtemelen "harcaması daha kolay olacağı" gibi sebeplerden dolayı toplamaktadırlar. Bu da yine işlem anonimliğinin ve mahremiyetinin ihlal edilmesine neden olmaktadır.

6.2. Öneriler

Anonim kriptoparaların en önemli özelliği isimlerinden de anlaşılacağı gibi kullancılar için anonimlik ve mahremiyet sağlamalarıdır. Korelasyon tabanlı mahremiyet analizi sonucundan anlaşılacağı gibi bu anonim kriptoparaları teoride anonimliği sağladıklarını belirtirlerken pratikte istenildiği ölçüde anonimliği yakalayamamaktadırlar. Kriptoparalarda mahremiyet ve anonimliğini artırabilmek adına sadece Zcash ve Dash değil tüm anonim kriptoparalara geliştiricileri ve kullanıcılarına öneriler aşağıda verilmiştir:

- Anonim kriptopara geliştiricileri kullanıcıları "anonim özelliklerinin nasıl kullanılması" gerektiğiyle alakalı bilgilendirme yapmaları önerilir. Örneğin en iyi pratikler (best practices) şeklinde bir web sayfası oluşturulup kullanıcılar için en doğru bir şekilde nasıl EkleBöl işlemi yahut ÖzelGönderim işlemi yapabilecekleri basitçe bilgilendirilebilir.
- Kullanıcılar beklendiği gibi kendileri için en kolay ve en ucuz olan yöntemi seçeceklerdir. Hem anonim hem de normal işlem seçeneği sunan kriptoparalar, anonim işlem yapmaları için kullanıcıları zorlayamacaklarından kullanıcıları teşvik amaçlı çeşitli alternatif yöntemlere gidebilirler.
- Zcash kriptoparası için, kullanıcılar korumalı bir işlem yaptıkları zaman korumalı işleme girerken kullandıkları işlem miktarını korumalı işlemden çıkarken kullanmamaları önerilir. Bunun yerine kullanıcılar sadece ihtiyacı olan miktarı korumalı havuzdan çıkarmaları daha doğru olacaktır.
- Yine Zcash kullanıcılarının EB-işlemlerinin tamamıyla anonimlik sağlamadığını bilmeleri gerekir. Korumalı havuza ZEC aktardıkları zaman bu korumalı havuzda ZEC'i farklı z-adreslere parçalamaları ve farklı z-adresleri üzerinden işlem yapmaları daha fazla anonimlik ve takip edilememezlik sağlayacaktır.
- Zcash kullanıcıları son olarak işlem yaparken Zatoshi cinsinden 10.000'in (varsayılan işlem bedeli) katsayısı olacak yuvarlak değerler üzerinden işlem yapmaktan kaçınmalıdırlar. Böylece kötü niyetli kişiler göz ardı edilen ve

analiz çalışmasında parmak izi değeri de denilen değerleri kullanarak işlem geçmişini takip edemeyeceklerdir.

- Zcash madenci havuzları bünyesinde bulundurdukları madencilere ödemeli hep aynı adres üzerinden yapmaktan kaçınmalıdırlar. Yapılan analizde bazı madenci havuzlarının en azından 6-7 farklı adres kullandıkları tespit edilmiştir ki bu da iyiye işarettir. Ayrıca madenci havuzlarının TMadenci yahut ZMadenci kategorilerine girmekten kaçınmaları için madencilerine ödemeleri doğrudan z-z korumalı işlemler üzerinden yapmaları tavsiye edilir. Misal vermek gerekirse SlushPool, Bitfly ve Luxor Mining isimli madenci havuzları doğrudan z-adrese sahip madencilere ödeme yapmaya imkân sunduklarını belirtilir[4].
- Dash kullanıcıları, Zcash kullanıcıları örneğinde olduğu gibi ÖzelGönderim işlemleri yaptıkları miktarın birebir aynısını, karıştırma seferleri sonunda farklı bir ikinci adrese olduğu gibi toplamamaları önerilir. Çünkü bu şekilde yapıldığında karıştırma sırasında 10'un katsayısına bölünen bir değer tekrardan bölünmediğinden karıştırma sonrası işlem miktarı aynı olduğu gibi toplam girdi adresi sayısı da birebir aynı olur. Dolayısıyla Dash kullanıcılarının ÖzelGönderim öncesi işlemleriyle ÖzelGönderim sonrası işlemleri birbirinin aynısı veya benzeri olmaması gerekir.
- Yine Dash kullanıcılarının ÖzelGönderim sonrası işlemlerinde başka bir adrese ödeme yapacakları zaman ÖzelGönderim'e girdikleri tüm adresleri kullanmak yerine ihtiyacı olan miktarı kullanmaları tavsiye edilir. Bunun yanında, ÖzelGönderim'de kullanılan miktarın tamamına ihtiyaç olması durumunda anonimliği artırmak adına ÖzelGönderim sonrası işlemler farklı şekillerde parçalandıktan sonra o parçaların ödeme yapılacak adrese farklı işlemlerde ödenmesi daha sağlıklı olacaktır.
- Monero ve Verge için doğrudan analiz çalışması yapılmadığı için bu kriptoparalarda doğrudan bir tedbir açıklaması yapılmayacaktır. Ancak anonim yahut anonim değil tüm kriptopara kullanıcılarının şahsi adreslerini gerekmeyen hiçbir yerde açıklamamaları tavsiye edilir. Ayrıca kriptopara geliştiricilerinin bu durumu ihlal eden (veya kendilerinden dijital para satın alan kullanıcıların adreslerini uygulama açıklığı nedeniyle sızdıran) Online marketler yahut forumları izlemeleri; gerekirse bu yerlere geçici veya kalıcı engelleme koymaları önerilir.
- Son olarak Zcash ve Dash geliştiricilerinin, kullanıcı gruplarının genel olarak yapmış olduğu hataları gruplandırmaları önerilir. Böylece her yapılan yanlışı engellemek imkânsız olsa da kullanıcıların en çok yaptığı yanlışlar için düzeltmeler, güncellemeler yahut alternatif yöntemler geliştirmek mümkün olacaktır.

VII. SONUÇ (RESULT)

2008 yılının Ekim ayında Satoshi Nakamoto, yayınlamış olduğu [1] makalesinde anlattığı blokzincir teknolojisiyle beraber Ocak 2009'da tüm İnternet kullanıcılarının hizmetine sunduğu Bitcoin kriptoparası bilişim teknolojilerinde yeni bir çağı beraberinde getirmiştir. Dağıtık yapısı ve güven odaklı olmayan mekanizması sayesinde blokzincir farklı birçok kişi, grup ve kuruluş tarafından ilgi odağı olmuştur. Geçen 11 yılda blokzincir teknolojisinin önemini artarak korumuştur.

Bitcoin, ilk çıktığı yıllarda her ne kadar tümüyle anonim olduğu düşünülse de yapılan çalışmalarla hiçbir şekilde anonim olmadığı anlaşılmıştır, [4], [5], [6], [7], [8]. Bu durumda çeşitli geliştiriciler farklı zamanlarda Bitcoin'e alternatif "anonim kriptoparalar" da denilen ve anonimliğe odaklanan kriptoparalar geliştirmişlerdir. Bu kriptoparalar teoride gerçekten de ciddi anlamda anonimlik ve mahremiyet sağlar. Zcash ve Monero kriptografik yöntemler kullanarak istenilen anonimliği sağlarken Dash ve PIVX AnaUçlar ve CoinJoin tabanlı karıştırma mekanizmaları kullanarak yapar. PIVX ayrıca Zcash'in kullanmış olduğu Zerocash protokolünü de kullanır. Verge ise ToR altyapısını kullanarak IP adreslerini gizlemeye odaklanır. Ancak Zcash ve Dash anonim kriptoparalarının yapılan korelasyon tabanlı mahremiyet analizi sonucunda pratikte, yani günlük kullanımlarda düşünüldüğü kadar anonimlik sağlamadığını yapılan analizler neticesinde anlaşılmıştır.

Zcash ve Dash için bu tez içerisinde işlem miktarı (ve Dash için ayrıca toplam adres sayısı) bakımından mahremiyet analizi çalışması yapılmıştır. Analiz çalışması sonucunda Zcash için%84,4 oranında ve Dash için %49,3 oranında (toplam adres sayısı parametresi mahremiyet analizine eklendiğinde bu oran %35,75'e düşmüştür) anonim işleminin birbirleriyle ilişkisi olma ihtimalinin bulunduğu sonucuna varılmıştır. İlgili kriptoparaların anonimlik seviyesinin artırılması için hem kullanıcılarına hem de geliştiricilerine çeşitli görevler düşmektedir. Mahremiyet analizi sonrasında tüm kullanıcı grupları ve anonim kriptopara geliştiricileri için çeşitli önerilerden bahsedilmiştir.

Sonuç olarak şu söylenebilir, anonim kriptoparalar her geçen gün gelişen ve değişen bilişim teknolojilerinin önemli bir parçası olmuşlardır. Özellikle hiçbir şekilde güven odaklı olmayan kriptoparalar gibi bilgi güvenliğinin ve mahremiyetin olduğu "para" odaklı sistemlerde gizlilik ve mahremiyetin ihlalinin ciddi

[4] zcashcommunity.com

seviyelerde yaşanması beklenen bir durumdur. Burada önemli olan nokta kriptopara geliştiricilerinin güvenlik ihlallerinin anlaşılmasının ardından hızlı bir şekilde müdahele edip yapılan yanlışlardan ve ihlallerden ders çıkartabilmesidir. Anonim kritpoparalarda korelasyon tabanlı mahremiyet analizi çalışması sonucunda Zcash ve Dash anonim kriptoparaları için anonimliğin analiz edilebileceği ve işlem geçmişinin tespit edilebileceği gösterilmiş; bunun yanında analiz yapılmasını engellemek yahut çıkan sonuçları daha kabul edilebilir hale getirebilmek için çeşitli önerilerden bahsedilmiştir.

KAYNAKLAR (REFERENCES)

[1] Satoshi, N., Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/, 1–9, 2008

[2] Birkuyov A., Daniel, F., Deanonymization of Hidden Transactions in Zcash, University of Luxembourg, 1-15, 2018

[3] TÜBİTAK BİLGEM UEKAE, Blokzincir, Blokzincir Araştırma Laboratuvarı, https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html, Erişim: 2020-03-27

[4] Birkuyov A., Dmitry K., Ivan P., Deanonymisation of Clients in Bitcoin P2P Network, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14), 15-29, 2014

[5] Sarah M., Marjori P., Grant J., Kirill L., Damon M., Geoffrey M. V., Stefann, S., A fistful of bitcoins: Characterizing payments among men with no names, Proceedings of the 2013 conference on Internet measurement conference ACM, University of California and San Diego George Mason University New York USA, 127-140, 2013

[6] Dorit, R., Adi S., Quantitative Analysis of the Full Bitcoin Transaction Graph, International Conference on Financial Cryptography and Data Security, The Weizmann Institute of Science Department of Computer Science and Applied Mathematics Israel, 6-24, 2013

[7] Androulaki1 E., Karame G. O., Roeschlin1 M., Scherer1 T., Capkun1 S., Evaluating User Privacy in Bitcoin, International Conference on Financial Cryptography and Data Security, ETH Zurich 8092 Zuerich Switzerland ve NEC Laboratories Europe 69115 Heidelberg Germany, 34-51, 2013

[8] Reid F., Harrigan M., An Analysis of Anonymity in the Bitcoin System 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, IEEE, Clique Research Cluster Complex & Adaptive Systems Laboratory UniversityCollege Dublin Ireland, 1318-1326, 2011

[9] Spagnuolo M., Maggi F., Zanero S., BitIodine: Extracting Intelligence from the Bitcoin Network, International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, 457-468. 2014

[10] KoshyEmail P., Koshy D., McDaniel P., An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, International Conference on Financial Cryptography and DataSecurity FC 2014: Financial Cryptography and Data Security, Springer Berlin Heidelberg, 469-485, 2014.

[11] Birkuyov A., Ivan, P.: Bitcoin over tor isn't a good idea, IEEE, Symposiumon Security and Privacy SP 2015. 122-134. IEEE, University of Luxembourg, Esch-sur-Alzette, Luxemburg, 2015

[12] Harry K., Steven G., Alishah C., Malte M., Arvind N., Blocksci: Design andapplications of a blockchain analysis platform, 29th {USENIX} Security Symposium ({USENIX} Security 20), Princeton University, 2721 – 2738, 2020

[13] Atlas, K., An analysis of darkcoin's blockchain privacy via darksend, 1–25, 2014

[14] Abraham H., Bernhard H., An empirical analysis of monero cross-chain traceability, International Conference on Financial Cryptography and Data Security FC 2019: Financial Cryptography and Data Security, Austrian Institute of Technologyand Vienna University of Technology, 150 – 157, 2019

[15] Möser M., Soska K., Heilman E., Lee K., Heffan H., Srivastava S., Hogan K., Hennessey J., Miller A., Narayanan A., Christin N., An empirical analysis of traceability in the monero blockchain, Proceedings on Privacy EnhancingTechnologies, Vol 2018, Iss 3, 143-163, 2018

[16] Amrit K., Clement F., TolePrateek S., A traceability analysis of monero's blockchain, 22nd European Symposiumon Research in Computer Security Proceedings 2017, National University of Singapore, 153-173, 2017

[17] Borggren N., Yoon Kim H., Yao L., Koplik G., Simulated blockchains for machinelearning traceability and transaction values in the monero network, Geometric Data Analytics Inc. Durham NC, 1–10, 2020

[18] Kappos G., Yousaf H., Maller M., Meiklejohn S., An empirical analysis ofanonymity in zcash, 27th USENIX Security Symposium (USENIX Security'18), Cornell University - University College London, 1 – 15, 2018

[19] Quesnelle J., On the linkability of zcash transactions, 27th USENIX SecuritySymposium (USENIX Security '18), Cornell University Esch-sur-Alzette Luxemburg, 1 – 5, 2017

[20] Erik D., Elias R., Florian T., Map-z: Exposing the zcash network in times of transition, IEEE, 44th Conference on Local Computer Networks (LCN), Cornell University Distributed Security Infrastructures Technical University of Berlin, 84 – 92, 2019

[21] Kappos G., Piotrowska A. M., Extending the anonymity of zcash, Cornell University - University College London United Kingdom, 1 – 2, 2019

[22] Alex B., Daniel F. Privacy and linkability of mining in zcash, IEEE, Conference on Communications and Network Security (CNS), University of Luxembourg Esch-sur-Alzette Luxemburg, 118 – 123, 2019
[23] Alex B., Daniel F., Giuseppe V., Privacy aspects and subliminal channelsin zcash, CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, University of Luxembourg Esch-sur-Alzette Luxemburg, 1813–1830 2019
[24] Alex B., Sergei T., Deanonymization and linkability of cryptocurrency transactionsbased on network analysis, IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, , 172 – 184, 2019
[25] Alex B., Sergei T., Transaction clustering using network traffic analysis for bitcoinand derived blockchains, INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019, University of Luxembourg Esch-sur-Alzette Luxemburg, 204 – 209, 2019,
[26] Alex B., Sergei T., Security and privacy of mobile wallet users in bitcoin, dash,monero, and zcash. Elsevier University of Luxembourg Esch-sur-Alzette Luxemburg, 1 – 11, 2019
[27] Bitcoin, Bitcoin'e başlarken, bitcoin.org, https://bitcoin.org/tr/, Erişim: 2020-03-27
[28] Jong-Hyouk L., Rise of anonymous cryptocurrencies: Brief introduction, IEEEConsumer Electronics Magazine IEEE Consumer Electron. Mag. Consumer Elec-tronics Magazine, IEEE, SangmyungUniv. - Cheonan South Korea, 20 – 25, 2019
[29] Daira H., Sean B., Taylor H., Nathan W., Zcash protocol specification, Zcash Protocol Specification, Zcash, 1–151, 2020
[30] Zcash documentation, Zcash Basics, Zcash, https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html, Erişim: 2020-03-28
[31] Dash, Dash documentation, dash.org, https://docs.dash.org/en/stable/, Erişim: 2020-07-01,
[32] Dash, What is dash cryptocurrency? The most comprehensive guide ever!, dash.org, https://blockgeeks.com/guides/what-is-dash/, Erişim: 2020-05-05
[33] Dash, Dash cryptocurrency: Complete dash coin guide, dash.org, https://www.bitdegree.org/tutorials/dash-cryptocurrency/, Erişim: 2020-05-05
[34] Dash, Dash features, dash.org, https://docs.dash.org/en/stable/introduction/features.html, Erişim: 2020-07-01
[35] Wikipedia, Monero. wikipedia.org, https://en.wikipedia.org/wiki/Monero, Erişim: 2020-07-04
[36] Monero, Monero technical specs, Monero Documentation, https://monerodocs.org/technical-specs/, Erişim: 2020-07-04,
[37] Monero, Ring signature, web.getmonero.org, https://web.getmonero.org/resources/moneropedia/ringsignatures.html, Erişim: 2020-07-04

EK-A: Algoritma 1 - TMadencilerin Bulunması
(APPENDIX-A: Algorithm 1 - FindingTMiners)

```
TMadencileriBul(blokZincir)
{
    blokListesi[] = blokZincir[-25000]
    //blokzincirdeki son 25,000 blok çekilir
    işlemListesi[] = blockListesi.işlemler
    muhtemelTMadenciListesi[] = Ø
    korumaliHavuzdanCoinAlanListesi[] = Ø
    korumaliHavuzdanCoinAlanGruplanmisListesi = Ø
    for (işlem in işlemListesi)
    {
     if (işlem.ciktiSayisi > 30 and işlem.KorumalıİşlemMi == false)
    {
            muhtemelTMadenciListesi = işlem.girdiAdresi
    }
        else if (işlem.KorumaliİşlemMi == true)
        {
            korumaliHavuzdanCoinAlanListesi = işlem.ciktiAdresi
        }
    }
    muhtemelTMadenciListesi = muhtemelTMadenciListesi $in$
    muhtemelTMadenciListesi.adres = korumaliHavuzdanCoinAlanListesi.adres
    korumaliHavuzdanCoinAlanListesi = korumaliHavuzdanCoinAlanListesi $in$
    korumaliHavuzdanCoinAlanListesi.adres = muhtemelTMadenciListesi.adres
    odemeYapilanMadenciListesi = blokListesi.islem.ciktiAdresi $in$
    blokListesi.islem = muhtemelTMadenciListesi.islem
    for (muhtemelTMadenci in muhtemelTMadenciListesi)
    {
        TMadencileriGrupla(muhtemelTMadenciListesi, muhtemelTMadenci,
        odemeYapilanMadenciListesi,
        korumaliHavuzdanCoinAlanGruplanmisListesi)
            }
    return korumaliHavuzdanCoinAlanGruplanmisListesi
    }

    TMadencileriGrupla (muhtemelTMadenciListesi,
    muhtemelTMadenci,
    odemeYapilanMadenciListesi,
    korumaliHavuzdanCoinAlanGruplanmisListesi)
```

```
{
    mevcutHavuzunMadenciAdresleri =
    odemeYapilanMadenciListesi in
    odemeYapilanMadenciListesi.islem =
    muhtemelTMadenci.islem
    for (girdi in muhtemelTMadenciListesi)
    {
        girdiIslemMiners =
    odemeYapilanMadenciListesi in
    odemeYapilanMadenciListesi.islem =
    girdi.islem
        if(exists(girdiIslemMiners in
    mevcutHavuzunMadenciAdresleri))
        {
            korumaliHavuzdanCoinAlanGruplan
        misListesi =
        korumaliHavuzdanCoinAlanListesi in
        korumaliHavuzdanCoinAlanListesi.adres
        = girdi.adres
            }
    }
}
```

EK-B: Algoritma 2 - ZMadencilerin Bulunmasi
(APPENDIX-2: Algorithm 2 – Finding ZMiners)

```
ZMadencileriBul(blokZincir)
{
    blokListesi[] = blokZincir[-25000]
    //blokzincirdeki son 25,000 blok çekilir
    muhtemelZMadenciler[] = Ø
    for (blok in blokZincir)
    {
     if (işlem.ciktiSayisi > 30 and
işlem.KorumalıİşlemMi == false)
    {
            muhtemelZMadenciler = blok.islem
        }
    }
    odemeYapilanMadenciListesi =
blokListesi.islem.ciktiAdresi $in$
blokListesi.islem = muhtemelZMadenciler.islem
```