

MARMARA ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ



ANONİM KRİPTOPARALARIN KORELASYON TABANLI MAHREMİYET ANALİZİ

MUHAMMET ALİ ÖZTÜRK

YÜKSEK LİSANS TEZİ

Bilgi Güvenliği Mühendisliği

DANIŞMAN
Dr. Öğr. Üyesi Hüseyin YÜCE

EŞ-DANIŞMAN
Dr. İsa SERTKAYA

İSTANBUL, 2020

Yazarlık Beyanı

Ben, MUHAMMET ALİ ÖZTÜRK, başlığı, 'ANONİM KRİPTOPARALARIN KORELASYON TABANLI MAHREMİYET ANALİZİ' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: _____

Tarih: _____

CORELATION BASED PRIVACY ANALYSIS OF PRIVATE CRYPTOCURRENCIES

MUHAMMET ALİ ÖZTÜRK

Abstract

Keywords: Bitcoin, cryptocurrencies, miner pools, Zcash, Dash, Monero, Verge, PIVX

In January 2009, Satoshi Nakamota published "Bitcoin" and this sparked the beginning of a new information tehnologies, named blokchain. Despite blockchain technology has already been mentioned as a concept, today this technology is usually identified with Bitcoin. While blokchain and cryptocurreny is thought as the same thing/technology by the many, in fact these two aren't the same thing. Blockchain is the technology that has a more general scope than crytocurrency, while cryptocurrencies is some kind of blockchain that transactions of blockchain deliver coins which can be used like real currencies in the real world.

Bitcoin still keeps its status as the most succesful, most used and most expensive crptocurrency. For many years, Bitcoin was thought totally secure, anonymous and private thanks to its using of "public-keyed address" that can be said as Bitcoin identifier. Unfortunately, these addresses is kept in fully public Bitcoin's ledger so Bitcoin cannot be anonymous at all. Because for example, if a malicious node learn an address which belongs to his target, it's totally possible to track all previous transactions of addresses of target.

Because of this problem, various methods suggested and developed to increase anonymity. But again, these methods like CoinJoin or Mixin proved to be insufficient against various malicious attacks or academical analysises, so anonymous cryptocurrencies began to emerge as an alternative to Bitcoin. Zcash, Dash, Verge and PIVX anonymous cryptocurrencies are enchanced-forks of Bitcoin while Monero anonymous cryptocurrency is enchanced-fork of Litecoin.

In theory, these crytocurrencies present a fully anonymous and private transaction possibility. But in practice, after conducting various analysis these crytocurrencies appeared to be not that "fully" anonymous at all. In this research, Zcash, Dash and Monero will be tried to analyze. After that it will be emphasized whether these anonymous crypytocurrencies are secure and anonymous then why some of these anonymous crypytocurrencies are not anonymous in practise and what can be done about it.

ANONİM KRİPTOPARALARIN KORELASYON TABANLI MAHREMİYET ANALİZİ

MUHAMMET ALİ ÖZTÜRK

Öz

Anahtar Sözcükler: Bitcoin, kripto paralar, madenci havuzları, Zcash, Dash, Monero, Verge, PIVX Ocak 2009 yılında Satoshi Nakamoto tarafından Bitcoin yayınlandıktan sonra blokzincir adında yeni bir bilişim teknolojisi doğmuştur. Her ne kadar kavram olarak daha önceki yıllarda bahsedilmişse de blokzincir, Bitcoin kriptoparası ile neredeyse özdeşleşmiş bir kavram olarak karşımıza çıkar. Ancak, blokzincir ile kriptoparalar aynı şey olarak düşünülse de blokzincir teknolojisi çok daha genel kapsama sahip bir bilişim teknolojisiyken kriptoparalar değer olarak gerçek dünyada alışveriş yapmaya imkân sunan paralar olan coinlerin iletildiği blokzincirlerdir.

Bitcoin kriptoparası günümüzde halen en yaygın, en değerli ve en pahalı kriptopara olma özelliğini korumaktadır. Uzun yıllar boyunca Bitcoin, bir çeşit Bitcoin kimliği olan açık anahtarlı adresleri kullandığı için anonimliği tamamıyla sağladığı düşünülmüştür. Ancak bu adresler tamamıyla umumi yani herkese açık bir kayıt defterinde tutulduğundan mütevellit Bitcoin aslında hiçbir şekilde anonim değildir. Misal olarak Bitcoin adresi bir şekilde öğrenilen bir kullanıcının yaptığı tüm geçmiş işlemleri ve bu işlemlerin miktarlarını geriye doğru takip etmek mümkündür.

Bahsedilen bu nedenlerden ötürü zaman içerisinde anonimliği geliştirici CoinJoin yahut Mixin gibi çeşitli yöntemler ortaya atılmıştır. Ancak bu yöntemlerin de yetersiz olduğu çeşitli kötü niyetli saldırılar yahut akademik analizler sonucunda anlaşılınca artık Bitcoin'e alternatif olarak anonim kriptoparalar yayınlanmaya başlamıştır. Anonim kriptoparalardan Zcash, Dash, Verge ve PIVX anonim kriptoparaları Bitcoin'den çatallanmış (Bitcoin's fork) yani Bitcoin kodu kullanılarak geliştirmiş kriptoparalardır. Monero anonim kriptoparası ise Bitcoin değil Litecoin'den çatallaştırılmıştır.

Teoride tamamıyla anonim olduğu belirtilen bu kriptoparalar pratikte istenilen anonimlik ve mahremiyeti yakalamadığı yapılan çeşitli analiz çalışmalarıyla ortaya konulmuştur. Bu araştırmada Zcash, Dash ve Monero kriptoparaları analiz edilmeye çalışılacaktır. Daha sonra bu kriptoparaların neden anonimliği ne derece sağlayıp sağlamadığı detaylı bir şekilde açıklanıp olası mahremiyet ihlallerine karşı neler yapılabileceğinden bahsedilecektir.

Teşekkür

İçindekiler

Yazarlık Beyanı **ii**

Abstract **iii**

Öz **iv**

Teşekkür **v**

Şekil Listesi **viii**

Tablo Listesi **ix**

Kısaltmalar **x**

1 Giriş **1**
1.1 Yapılmış Çalışmalar . . . 2
1.2 Katkımız . . . 4
1.3 Tezin Yapısı . . . 4

2 Giriş ve Tanımlar **6**
2.1 Blokzincir Teknolojisi . . . 7
2.1.1 Blokzincir Tipleri . . . 10
2.1.2 Kriptoparalarda Konsensüs . . . 10
2.1.3 Bloklar . . . 12
2.1.4 İşlemler . . . 13
2.1.5 Madencilik . . . 15
2.1.6 Zaman Damgası Sunucusu . . . 15
2.1.7 İşin İspatı (Proof-of-Work) . . . 16
2.1.8 Ağ . . . 17
2.1.9 Gizlilik . . . 18
2.2 Bitcoin Nedir? . . . 19
2.3 Bitcoinde Gizlilik . . . 23
2.3.1 Mixin Protokolü ve CoinJoin . . . 27
2.3.2 Karıştırma Ağları (Mix Nets) . . . 27
2.3.3 Tor (The Onion Router) . . . 28
2.4 Anonim Kriptoparalar . . . 29
2.4.1 Zcash . . . 30
2.4.2 Dash . . . 33
2.4.2.1 AnaUç (MasterNode) . . . 34

2.4.2.2 ÖzelGönderim (PrivateSend) . . . 34
2.4.2.3 HızlıGönderim . . . 36
2.4.3 Monero . . . 36
2.4.3.1 Halka İmzalar (Ring Signatures) . . . 37
2.4.3.2 Açık Adresler . . . 38

3 Uygulama ve Analiz 40
3.1 Zcash Analizi . . . 41
3.1.1 Madencilerin Analizi . . . 45
3.1.1.1 TMadencilerin Analizi . . . 49
3.1.1.2 ZMadencilerin Analizi . . . 50
3.1.2 Gidiş-Geliş İşlemleri . . . 52
3.1.2.1 Temel Karşılaştırma . . . 53
3.1.2.2 Alt-küme Toplamlarının Karşılaştırılması . . . 55
3.1.2.3 Parmak İzi Değerleri Karşılaştırması . . . 56
3.2 Dash Analizi . . . 56
3.2.1 Madencilerin Analizi . . . 59
3.2.2 Gidiş-Geliş İşlemleri . . . 60
3.2.2.1 Temel Karşılaştırma . . . 61
3.2.2.2 Alt-küme Toplamlarının Karşılaştırılması . . . 61
3.2.2.3 Parmak İzi Değerleri Karşılaştırması . . . 64

4 Sonuçlar ve Tartışma 65
4.0.1 Zcash Analizi Sonuçları . . . 65
4.0.2 Dash Analizi Sonuçları . . . 67
4.1 Diğer Analiz Sonuçları . . . 68
4.1.1 Monero Analizi . . . 70
4.2 Tartışma . . . 73
4.3 Öneriler . . . 76

5 Netice 79

A Ek-A 81

B Ek-B 83

Kaynaklar 85

Özgeçmiş 92

Şekil Listesi

2.1 Çeşitli Güven Sistemlerine Dayalı Sistemler 8
2.2 Merkle Ağacı [1] 8
2.3 Merkle Ağacı [24] 9
2.4 Konsensüs Tipleri [14] 11
2.5 Bitcoin'deki İşlemlerin Yapısı [55] 14
2.6 Zaman Damgası Alınan Bloklar, [55] 16
2.7 Geleneksel Bankadaki Gizlilik - Blokzincirdeki Gizlilik [55] 18
2.8 Yıllara Göre BTCUSD (Bitcoin Amerikan Doları) Grafiği [17] 20
2.9 Yıllara Göre Bitcoin İşlemleri Grafiği 21
2.10 Son 1 Yıldaki Tüm Madencilerin ve Maden Havuzlarının Blok Ödülü Pastasındaki Payları [12] 22
2.11 Son 1 Yıldaki En Büyük 10 Maden Havuzu Tablosu [12] 22
2.12 Son 1 Yıldaki En Büyük 10 Maden Havuzu Tablosu 24
2.13 Son 1 Yıldaki En Büyük 10 Maden Havuzu Tablosu 24
2.14 Coinjoin Şeması [53] 27
2.15 Mixnet Mekanizması Şeması [61] 28
2.16 Bitcoin ve Anonim Kriptoparaların Kısa Tarihçesi [47] 29
2.17 *dfd89aa42cbe00d6862be21a7cde582fc5606f23f5297adca3c7d4a6f54f3410* koduna sahip 2134748. nolu bloktaki işlem 37

3.1 Yıl ve Aylara Göre İşlem Tipi (Transaction Type) Grafiği 41
3.2 Yıl ve Aylara Göre EkleBöl İşlemleri Tipi (JoinSplit Transactions Type) Grafiği 42
3.3 En Çok Kullanılan 10,000 İşlem Çıktısı 43
3.4 En Çok Kullanılan 10,000 Adres Çıktısı 44
3.5 En Çok Kullanılan 1,000,000 Adres Çıktısı 44
3.6 Aktif Zcash Madenci Havuzları https://www.poolwatch.io/coin/zcash bağlantı adresini kullanarak ulaşabilirsiniz. 1 Temmuz 2020 1:37 tarihinde erişilmiştir. 46
3.7 En Çok Kullanılan 1,000,000 Adres Çıktısı 58
3.8 En Çok Kullanılan 1,000,000 Adres Çıktısı 58

Tablo Listesi

3.1 Son 25,000 Blok İçin Madenci Havuzları ve Madencilerinin Ürettikleri Blok Sayıları ve Kazandıkları Toplam Blok Ödüllerinin Tablosu 47
3.2 Algoritma 29 Sonucunda Bulunan MUhtemel TMadenciler Tablosu 50
3.3 Algoritma 2 Analizi Sonucunda Bulunan Muhtemel ZMadenciler 52
3.4 Tiplere Göre Dash İşlemleri Sayıları 59
3.5 Son 25,000 Blok İçin Tiplere Göre Dash İşlemleri Sayıları 59
3.6 Dash Muhtemel TMadenciler 60
3.7 Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu 62
3.8 Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu 63

Kısaltmalar

BTC	**Bitc**oin
XBT	**X**[1]**Bit**oin
mBTC	**m**ini**Bitc**oin
UTXO	**U**nspent**T**ransaction**O**utput
ZEC	**ZC**ash
T-adres	**T**ransparent-adres (Açık adres)
Z-adres	**Z**cash-adres (Gizli adres)
EB-işlemleri	**E**kle **B**öl-işlemleri
GDİ	**G**idiş **D**önüş **İ**şlemleri
ÖGG-işlemleri	**Ö**zel **G**önderime **G**iren-işlemler
ÖGÇ-işlemleri	**Ö**zel **G**önderimden **Ç**ıkan-işlemler
TK	**T**emel **K**arşılaştırma
AKTK	**A**lt **K**üme **T**oplamları **K**arşılaştırma

[1] **X** hiçbir ülkeye bağlı olmayan uluslararası camiada kabul görmüş para birimi demektir.

Bölüm 1

Giriş

Tarih boyunca altından veyahut gümüşten yapılmış olan ve İngilizce "coin" adı verilen madeni paralar her türlü alış verişin belkemiği olmuştur. Yıllar geçtikçe altın ve gümüşten yapılma madeni paraların yerini daha kolay üretilmesi ve taşınabilmesi gibi çeşitli faydaları sayesinde kağıt paralar almıştır. 20. yüzyılın sonlarında dünya İnternetin yaygınlaşmasıyla yeni bir döneme girmiş ve herşeyin merkezinde olan ticaret, dolayısıyla "para" bu yaygınlaşmadan etkilenmiştir. Binlerce yıl gerek takasla gerekse kağıt paralarla yapılan her türlü alış veriş artık İnternet üzerinden yapılabilir hale gelmiştir. Ayrıca yine kredi kartlarının yaygınlaşmasıyla hiçbir şekilde fiziksel bir paraya ihtiyaç olmadan ticari işlemler yapılabilir olmuştur. Nihayet 2009 yılına gelindiğindeyse Satoshi Nakamoto olarak bilinen bir kişinin (yahut bir grubun) Bitcoin adını verdiği açık kaynak kodlu bir yazılımı yayınlamasıyla "paranın" dünyasında yeni bir döneme girilmiştir, [55].

Bitcoin, daha önce de bahsettiğimiz gibi açık kaynak kodlu yazılım tabanlı bir çeşit elektronik para birimidir. Kullanmış olduğu kriptografik yöntemler nedeniyle Bitcoin ve sonrasında çıkan tüm para birimlerine genel olarak kriptopara (cryptocurrency), bu kriptopraların kullanmış oldukları teknolojiye de blokzincir (blockchain) adı verilir. Bitcoin ve kriptoparaları bu kadar farklı kılan şey kullanmış oldukları teknoloji olan blokzincirinin sağlamış olduğu anonimlik (anonimty) ve herhangi bir merkeze bağlı olmayan dağıtık (distributed) yapısıdır.

En temel tabiriyle blokzincir hiçbir merkezi otoriteye ihtiyaç olmaksızın değer olarak atfedilen çeşitli varlıkların bir veriymiş gibi aktarılmasını sağlayan veritabanıdır. Her ne kadar ilk çıktığı zamanlarda sadece Bitcoin gibi kriptopara alanında kullanılsa da blokzincirin daha başka birçok farklı alanda da kullanılabileceği görülmüştür. Bu tezde sadece kriptoparalar üzerine odaklanılacaktır.

Blokzincirin altyapısı kendisine adını veren bloklar (blocks) ve işlemlerdden [1] (transactions) oluşur. Bu işlemler ilgili blokzincire ait her türlü verinin kaydedildiği içerik bilgisidir. Bitcoin gibi kriptoparalar için bu bilgiler coin transferinde aktarılan Bitcoin miktarı, coini gönderenin ve coinin gönderildiği yerin adresleri (input ve output adresleri) ve coin transferinin zamanı gibi verilerdir. Bu işlemler birleştirilir ve belirli aralıklarla bloklara yazılır. Bu bloklar da sırayla art arda oluşturularak bir zinciri oluşturur. Blokzincirdeki herbir blok (ilk blok hariç) kendisinden önceki bloğu özet bilgisini de tutar, [18], [55].

Para transferleri için kullanılan Bitcoin adreslerinin doğrudan gerçek bir kişi, grup yahut kurumla ilişkilendirilebilecek bir bilgi içermemesi sayesinde bu adresleri kullananlar için anonimlik ve mahremiyet sağlar. Ne var ki Bitcoin işlemlerinin, bloklarının ve hatta adreslerinin tamamının açık veritabanlarına kaydedilmesi nedeniyle Bitcoin kriptoparasının düşünüldüğünden daha az anonimlik ve mahremiyet sağladığı gözlemlenmiştir. Kimi zaman adres sahiplerinin adres bilgilerini isteyerek yahut bilmeden paylaşması, kimi zaman da yapılan işlemlerin IP adresinlerinin anlaşılması gibi sebepler nedeniyle ilgili adresin kime ait olabileceği ve buna benzer çeşitli kişisel bilgiler ele geçirilebilmektedir. Bu da bulunan adere ait tüm işlemlerin açık bir şekilde herkes tarafından görülebilmesine neden olur. Sonuç olarak bu durum işlem ve adres gizliliğine daha fazla önem veren Zcash ve Dash gibi çeşitli yeni "anonim kriptoparaların" bulunmasına neden olmuştur.

Zcash, Dash ve Monero gibi kriptoparaların ortak özelliği kendi bünyelerindeki kullanıcılara çeşitli şekillerde anonimlik ve gizlilik sağlamalarıdır. Zcash kriptoparası açık olarak yapılan işlemlerin (public transactions) yanında ayrıca gizli işlemleri (private/shielded transactions) kullanarak işlemin miktar ve adresini gizlerken, Dash kriptoparası da işlem miktarlarını matematiksel algoritmalar ve işin ispatı (proof of work) vasıtasıyla gizler. Dash ve PIVX kriptoparaları işlemleri Masternode'ların yardımıyla karıştırarak anonimlik sağlarken Verge kriptoparasıysa Tor ve I2P kullanarak yapılan işlemlerin IP adreslerini gizler. Kullanılan bu çeşitli yöntemler vasıtasıyla bu anonim kriptoparalar kullanıcıları için çeşitli şekillerde gizlilik ve mahremiyet sağlarlar. Ne var ki analiz edilebilen çeşitli kullanıcı alışkanlıkları, kullanılan algoritmalar ve yöntemlerdeki çeşitli hata ve açıklar veyahut kriptoparaları hedef alan çeşitli saldırılar sonucunda kullanıcıların bilgileri üçüncü şahıslar tarafından ele geçerilmesi mümkün olmaktadır.

1.1 Yapılmış Çalışmalar

Bitcoin kriptoparasının [55] makalesiyle beraber Satoshi Nakamoto mahlaslı bir kişi tarafından 2009 yılında yayınlanmasından sonra anonimlik ve gizliliği ne derece sağlayabildiğini anlayabilmek adına farklı çalışmalar yapılmıştır. Bitcoin üzerine yapılan bu çalışmaların önemli bir kısmı Bitcoin adreslerinin, bloklarının ve işlemlerinin üzerinde

yapılan çalışmalardır, [36], [54], [58], [29], [57]. Bu çalışmalar Bitcoin adresine sahip madenciler (miners), Bitcoin satıcıları (borsacıları / exchanges), normal kullanıcılar ve anonimi amaçlayan iyi yahut kötü niyetli kişi, grup yahut oluşumlar gibi çeşitli kullanıcı gruplarını hedefler. Hedefledikleri bu kullanıcı gruplarının coin transferleri sırasındaki davranışlarını, bu transferleri gerçekleştirmek için yapılan işlemleri ve bu işlemlerin toplantıdığı blokları analiz ederek hangi adresin kime ait olduğunu bulmaya çalışırlar. Bu işleme kısaca Bitcoinin anonimliğinin açık hale getirilmesi veya kısaca **anonimsizleştirme (de-anonoymization)** adı verilir. Bir diğer araştırma yöntemi ise Bitcoin kriptoparasının uçtan uca ağının (peer-to-peer network) analiz edilerek çeşitli bilgilerin elde edilmesi üzerine odaklanır, [59], [49], [38]. Bunun yanında Bitcoin adreslerinin IP adreslerinin ToR gibi çeşitli aracılarla gizlenmesini sağlayan anonimleştirme yöntemleri üzerine de analiz çalışmaları yapılmıştır, [38], [27], [52].

Bitcoin üzerine yapılan bu çalışmalar neticesinde iddia edildiği kadar anonimlik sağlamadığı anlaşılmıştır. Bu nedenle daha sonraki yıllarda Dash, Monero, Verge, PIVX, Beam ve Zcash gibi daha çok kullanıcıların anonimliğine odaklanan çeşitli yeni anonim kriptoparalar ortaya çıkmıştır. Her ne kadar gerçekten de Bitcoin kriptoparasından daha fazla anonimlik sağlasalar da bu kriptoparalar üzerine de çeşitli çalışmalar yapılmıştır. Yapılan bu araştırmaların neticesinde de anonimlik ve gizlilik üzerine odaklanan bu anonim kriptoparalarda da gizlilik ve mahremiyet ihlallerinin yapılabileceği gözlemlenmiştir. Örnek olarak doğrudan Dash anonim kriptoparasına odaklanan [48] ve [30] çalışmaları, Monero anonim kriptoparası üzerine odaklanan [44], [51] ve [50] çalışmaları bulunmaktadır. ToR'u kullanarak IP adres gizlemesi yaptığından dolayı Verge anonim kriptoparası için [38] araştırmasını örnek olarak göstermek mümkündür. Ayrıca diğer kriptoparalardan farklı olarak zk-SNARK adı verilen bir sır vermeyen kanıt (zero-knowledge-proof) ve Zerocash üzerine kurulmuş Zcash anonim kriptoparası üzerine yine anonimsizleştirmeyi amaçlayan birçok çeşitli araştırmalar yapılmıştır, [28], [43], [46], [40], [42], [31], [37].

Yukarıda bahsedilen araştırmaların haricinde ayrıca bazı araştırmalar Bitcoin ile beraber Dash ve Monero gibi kriptoparaları da analiz ederek bir birden fazla kriptoparayı aynı anda analiz ettiği bir araştırma ortaya koymuşlardır. [39] çalışması Bitcoin ve benzeri kriptoparaların ananomliği analizi üzerinden yola çıkarak Mixcoin adında anonim bir kriptopara ortaya çıkarmayı amaçlar. [33] ve [32] çalışmaları farklı kriptoparaların ağ (network) anonimsizleştirme analizi yaparken [35] çalışması ise Bitcoin, Dash, Monero, and Zcash kriptoparalarının mobil cüzdanları (mobile wallet) üzerine anonimsizleştirme analizi yapar. [47] araştırması da kriptoparaların anonimsizleştirme analizinden ziyade Bitcoin kriptoparası ile beraber belli bir değere sahip daha onlarca kriptopara varken neden anonimlik ve mahremiyete daha fazla önem veren kriptoparalara ihtiyaç duyulduğundan bahseder. Bunun yanında ayrıca kullanıcıların Zcash anonim kriptoparasındaki korumalı

işlemlerde olduğu gibi mahremiyet üzerine odaklı özellikleri neden istenilen ölçüde tercih etmediklerini hakkında bir yorum ortaya koyar.

1.2 Katkımız

Yapılacak olan bu tez çalışmasında Bitcoin kriptoparasına alternatif olarak çıkan ve anonimliliği amaçlayan gizli kriptoparaların anonimliği üzerine "korelasyon tabanlı mahremiyet analizi" yani kısaca anonimsizleştirme analizi üzerine odaklı bir araştırma çalışması yapılacaktır. Yapılacak bu analiz çalışması Alex Birkuyov tarafından hazırlanmış olan araştırma makalesindeki analiz çalışması temel alınarak yapılacaktır, [28]. İlk olarak anonim kriptoparanın blokzincirindeki tüm bloklar incelenecek, daha sonra spesifik olarak madencilerin analizi ve son olarak gidiş-dönüş işlemleri (kısaca GDİ) analiz edilecektir.

Yapılacak olan tez çalışmasında Bitcoin gibi tamamıyla açık işlemler yapan kriptoparalarının analizinden ziyade Zcash gibi anonimliğe odaklanan kriptoparalarda yapılan işlemlerin analizine odaklanılacaktır. Burada evvela Zcash kriptoparasının blokzincirine dahil olan bloklar, işlemler ve bu işlemleri gerçekleştiren adresler analiz edilecektir. Daha sonra sırasıyla yine işlemlerin ve kullanıcı adreslerinin anonimliğine odaklandıklarını söyleyen Dash ve Monere kriptoparalarının analizleri gerçekleştirilip işlemler ve adresler arasındaki ilişkiler ortaya çıkartılmaya çalışılacaktır. Zcash kriptoparası haricindeki diğer kriptoraların için bu tezde yapılacak analize benzer bir analiz çalışmasına daha önce rastlanmamıştır. Kısım 1.1'de Dash ve Monero için çeşitli anonimsizleştirme çalışmalarından bahsedilmiştir. Verge'nin kullandığı Tor mekanizmasını hedef alan çaışmalarda da yine Kısım 1.1'de değinilmiştir. Ne var ki, yapılacak olan tez içerisindeki analiz çalışması bu bahsedilen çalışmalardan farklı bir çalışma olacaktır.

Son olarak, yapılan analiz çalışmasıyla beraber her bir anonim kriptoranın ne derece anonim olup olmadığı ve bu anonim kriptoparaların kullandıkları algoritmalarla beraber anonimliği sağladığı söylenen korumalı işlemler gibi mekanizmaların ne derece bu anonimliği sağladığı tespit edilmeye çalışılacaktır. Aynı zamanda bunun yanında bu anonim kriptoparaları kullanan kullanıcı gruplarının ilgili özellikleri ne derece kullandıklarını tespit edilmeye çalışlacak ve bu tespitlerin akabinde elde edilen verilen yorumlanacaktır.

1.3 Tezin Yapısı

Yapılacak olan tez çalışmasının genel yapısı aşağıdaki gibidir:

Bölüm 2'de Blokzincir ve Bitcoin hakkında bilgi verilecektir. Blokzincirde konsensus gibi terimler ne demektir, blok ve işlem nedir, madencilik ve işin ispatı ne anlama gelir

gibi konular alt-başlıklarda ele anılacaktır. Daha sonra kısaca Bitcoin'den bahsedilecek ve Bitcoin'de anonimlik ve gizlilik üzerinde durulacaktır. Sonrasında neden Bitcoin'e alternatif olarak anonim kriptoparaların yayınlandığından bahsedilecek ve sonra da Zcash, Dash ve Monero anonim kriptoparalarıyla beraber bunların çalışma mantıklarıyla ve anonimlik ile kullanıcı mahremiyetini nasıl sağladıklarından bahsedilecektir.

Bölüm 3'de Zcash ve Dash gibi anonim kriptoparaları analiz edilecektir. İlk olarak Zcash için madenci havuzları ve gidiş-geliş işlemleri analiz edilecek; daha sonra aynı şekilde Dash için madenci havuzları ve gidiş-geliş işlemleri analiz edilecektir. Dash, Zcash'ten çok farklı bir kriptopara olduğundan dolayı analize bazı eklemeler yapılacaktır. İlgili kısımlarda bu konudan detaylı bir şekilde bahsedilecektir.

Bölüm 4'de ilk olarak bir önceki analiz bölümünde yapılan çalışmaların sonuçları olan Zcash analizi sonuçları ve Dash analizi sonuçları tartışılacaktır. Daha sonra kriptoparalar için yapılan diğer analiz çalışmalarından ve bunların nasıl yapıldığından kısaca bahsedilecektir. Burada Monero anonim kriptoparalası, Zcash ve Dash gibi neden analiz edilemedi anlatıldıktan sonra bu kriptopalar için yapılmış benzer analiz çalışmalarından bahsedilecektir. Daha sonra yapılan ve bahsedilen tüm bu analiz çalışmaları sonrası anonimliğin ve mahremiyetin ihlalilene sebep olan nedenler üzerine "tartışma" yapılacaktır. Son olarak bu bölümde kriptopara geliştiricilerinin ve kullanıcılarının anonimliği daha iyi seviyelere çıkarmak adına alabilecekleri çeşitli "öneriler" madde madde anlatılacaktır.

Bölüm 5'te ise genel olarak blokzincir ve Bitcoin'den, yapılan işlemlerden, alonan neticelerden, bunların nedenlerinden ve önerilerden özet mahiyetinde bahsedilecektir. Tez çalışması bu bölümle beraber sonlandırılacaktır.

Bölüm 2

Giriş ve Tanımlar

Binlerce yıl boyunca ticaret insanlık tarihinin belkemiğindeki temel yaşam ihtiyaçlarından birisi olmuştur. Ticaret sayesinde insanlar kendi temin edemedikleri ihtiyaçlara belli bir ücret karşılığında ulaşabilmişlerdir. Yaklaşık günümüzden 2500 sene kadar önce, yani MÖ 6. yüzyılda Lidyalıların altın ve gümüşleri eriterek sikke adını verdikleri parayı kullanmaya başlamadasından önce ticaret genellikle takas yoluyla yapıldığı tarih kaynaklarında belirtilmektedir. Zaman içerisinde Lidyalıların keşfettiği madeni para ile ticaret çeşitli medeniyetler tarafından zamanla kabul görmüştür, [23].

Günümüzde ticaret çoğunlukla "kağıt para" olarak basılan para birimleri üzerinden yapılmaktadır. Kağıt para "deri para" şeklinde ilk olarak MÖ 118 yılında Çin'de, kağıt para olarak da MS 806 yılında yine Çin'de bulunmuştur. Batıda 17. yüzyılın sonlarında ilk defa kullanılmaya başlamış ve tüm dünyaya buradan yayılmıştır, [60]. Kağıt paranın önemi üretilmesinin, saklanmasının ve taşınmasının kolay olmasıdır. Kendi başına hiçbir değeri olmayan bir çeşit kağıt parçası olan kağıt para, onu üreten **merkezi otorite** sayesinde önemli bir değer kazanmaktadır. Her ne kadar günümüzde halen büyük çoğunlukla kağıt para kullanılmasına karşın 20. yüzyılın sonlarında kredi kartlarının bulunması ve 21. yüzyılda da internetin yaygınlaşmasıyla yepyeni bir döneme girilmiştir. Bu sayede tamamıyla sanal olarak veritabanları gibi sistemlerde tutulan ve yine merkezi otorite tarafından denetlenen veriler vasıtasıyla çeşitli ticari işlemlerin yapılması mümkün olmaktadır.

Ne var ki, bütün bu ticari işlemlerin en büyük sıkıntısı yapılan tüm işlemlerin merkezi bir otorite tarafından denetlenip kontrol ediyor olmasıdır. Özellikle İnternet üzerinden yapılan tüm işlemler o işlemin yapıldığı bankanın veri kaydetme merkezlerinde (genellikle büyük veritabanı sunucularında) tutulmaktadır. Burada kullanıcı işlem yapmasını sağlayan merkezi otoriteye **tamamıyla güvenmek** zorundadır. Bu da alıcı ile satıcı arasında bir şekilde mahremiyet isteyen kullanıcıların yaptığı tüm işlemlerle beareber çeşitli kişisel

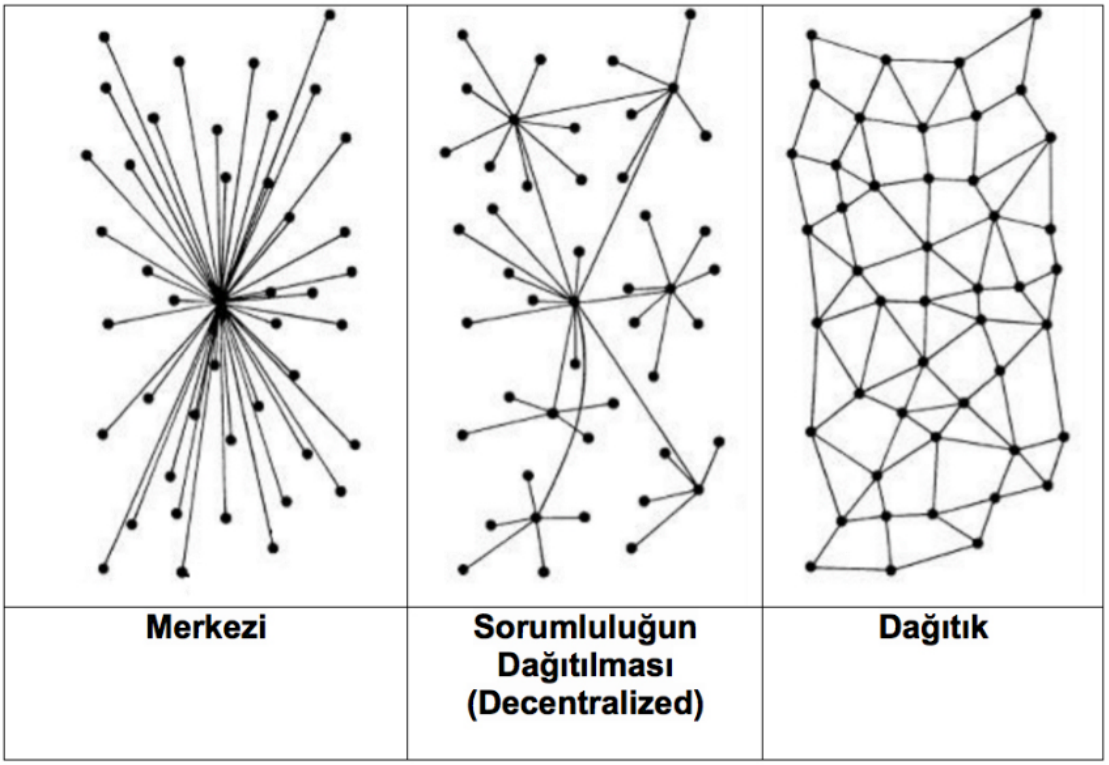
bilgilerinin de üçüncü kişiler (third parties) tarafından kaydedilmesi anlamına gelir. Türkiye'de her ne kadar bankalar gibi kurumsal otoriteler KVKK (Kişisel Verileri Koruma Kanunu) kapsamında kişilerin kişisel bilgilerinin güvenliğini temin etseler de son yıllarda Apple gibi en çok güvenilen kurumlarda bile yaşanılan bilgi sızması gibi çeşitli ihlaller bunun tamamıyla asla mümkün olmadığını ispat etmektedir. Özellikle İnternet ortamında her geçen gün yaygınlaşan bu işlemler hiçbir merkezi otoriteye dayanmayan ve güven odaklı olmayan tamamıyla yeni bir ticari işlemin, dolayısıyla merkezi otorite olan devletlerin yönettiği para birimlerinden bağımsız yeni bir para biriminin ortaya çıkmasını sağlamıştır. Ekim 2008'de Satoshi Nakamoto lakablı bir kişi Bitcoin kriptoparasıyla beraber blokzincir teknolojisini anlatan bir makale yayınlamıştır, [55]. Ocak 2009'da da Bitcoin ağını başlatmıştır.

2.1 Blokzincir Teknolojisi

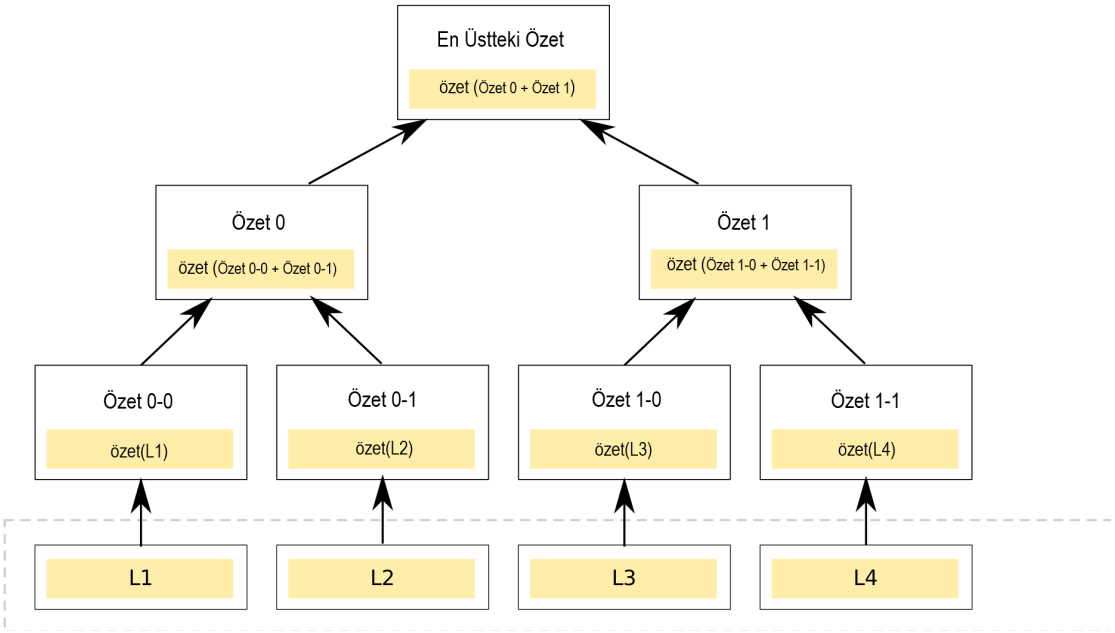
Bir önceki bölümde anlatıldığı gibi Bitcoin kriptoparası yıllar içerisinde ciddi anlamda önem kazanmış ve Bitcoin için çeşitli araştırmalar, makaleler ve kitaplar yazılmış ve film ve belgeseller çekilmiştir. Hatta daha da ilerisi çeşitli haber kanallarında, farklı vizyona sahip kuruluşların toplantılarında ciddi tartışmaların konusu olmuş ve nihayet devletler Bitcoin ve kriptoparalar için olumlu ya da olumsuz çeşitli hukukî düzenlemelere gitmiştir. Peki ya Bitcoin'in bu kadar meşhur olmasını sağlayan blokzincir teknolojisi nedir?

Blokzincir teknolojisi en basit tabiriyle İnternet dünyasında alışılagelmiş "geleneksel" yöntemlerle aktarılan Multimedya, web arayüzü gibi verilerden ziyade **değer** atfedilen varlıkların transfer edilmesini sağlayan **dağıtık bir veritabanıdır**, [1]. Bir diğer deyişle blokzincir kriptografiden yararlanılarak birbirlerine bağlanmış ve sürekli büyüyen kayıtlar listesidir. Bu kayıtlara **blok (block)** adı verilir, bu nedenle teknolojinin adına blokzincir denilmiştir. Her bir blok bir önceki bloğun kriptografik özet (cryptographic hash) bilgisini, bir zaman damgası (timestamp) ve işlem bilgisini içerir, [19]. Bitcoin gibi kriptoparalar için bu bilgi bir adresten farklı bir ya da daha fazla adrese aktarılan işlem bilgisidir.

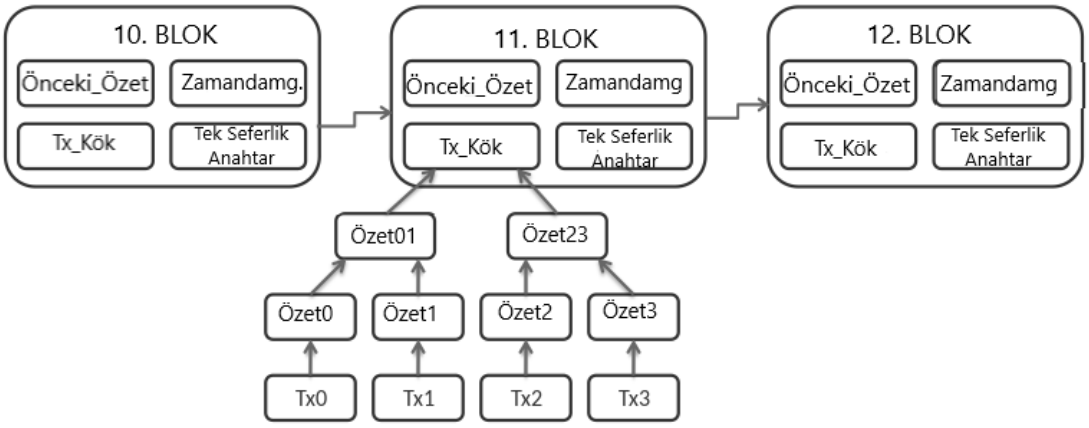
Blokzincir teknolojisi günümüz teknolojilerinde en önemli sorunlardan birisi olan tek merkeze dayalı güven sistemlerindeki merkezi güven yapısı dağıtarak dağıtık ve genellikle açık (public) olan ve dijital kayıt defteri (digital ledger) denilen veritabanı sistemleri yapısını ortaya çıkarmıştır, [19]. Şekil 2.1'de merkezi güvene dayalı sistemde tüm kullanıcıların nasıl sadece tek bir merkez vasıtasıyla haberleştiği açıkça anlaşılmaktadır, [55]. Merkezi sistemin ele geçirilmesi, hatta en başta bu kişilerin kötü amaçlı kişiler tarafından oluşturulmuş olması gibi durumlarda sistemi kullanan kullanıcıların tümü büyük risk altında olacaktır. Dağıtık yapı olan blokzincirler sayesinde herhangi bir düğümün yahut kullanıcının ele geçirilmesi sistemin tümünü risk ve töhmet altında bırakmayacaktır.



Şekil 2.1: Çeşitli Güven Sistemlerine Dayalı Sistemler



Şekil 2.2: Merkle Ağacı [1]



Şekil 2.3: Merkle Ağacı [24]

Kriptografik olarak güvenliği sağlanmış blokzincir çalışması ilk defa 1991 yılında Stuart Haber ve W. Scott Stornetta tarafından yapılmıştır. Bu sayede belge zamandamgasının oynanamayacağı bir sistem oluşturmak istemişlerdir. 1992 yılında da Haber, Stornetta, ve Dave Bayer tasarıma Şekil 2.2'deki resimde belirtilmiş olan **Merkle ağacı**nı (Merkle tree) ekleyerek bir bloğa birden fazla belge sertifikasının eklenmesini sağlamış; bu sayede de tasarımın daha etkili ve verimli olması sağlanmıştır, [19]. Ne var ki blokzincir ilk defa Satoshi Nakamoto tarafından 2008 yılında kavramsallaştırılıp 2009 yılında bilinen ilk blokzincir uygulaması olan Bitcoin kriptoparası hayata geçirmiş ve Bitcoin'in kriptoparayla ve kriptoparanın da blokzincir terimiyle özdeşleşmesine neden olmuştur. Şekil 2.3'da da görüldüğü gibi Bitcoin kriptoparası Merkle ağacı yapısını kullanır, [55].

Blokzincirde kaydedilen verinin içeriği gerçek bir elektronik paradan bir kişinin kimliğine, iki farklı grup arasında yapılan bir anlaşmadan lambanın ne kadar elektrik kullandığına kadar çok farklı bilgiler olabilir. Blokzincir teknolojisi Bitcoin ile beraber tanıtıldığından dolayı genellikle sadece Bitcoin ve halefleri olan kriptoparalarda blokzincir teknolojisinin kullanıldığı zannedilir. Ancak kriptoparalar haricinde akıllı telefonlarda, bankacılık ve finans sistemlerinde, değerli belgelerin yaratılması ve saklanmasında, bağış sistemleri ve mikro ödemelerde, tedarik zincirlerinde hatta domain isimlerinde kullanıldığı gözlemlenmiştir, [1] [19].

Blokzincirdeki dağıtık kayıt defterlerinin üç anahtar özelliğe sahip olmaları beklenir [15]:

1. **Kaydedilmiş (Recorded):** Veritabanına kaydedilen bilgi zaman damgalıdır.
2. **Şeffaf (Transparent):** İsteyen herkes işlemlerin kayıt defterini görebilir.
3. **Dağıtık (Decentralized):** Kayıt defteri düğüm de denilen birden fazla cihazda yahut bilgisayarda bulunur.

2.1.1 Blokzincir Tipleri

Toplamda üç farklı blokzincir tipi bulunmaktadır, [19]:

1. **Açık (Public) Blokzincir:** Hiçbir erişim kısıtlaması olmayan blokzincir tipidir. İnternet bağlantısı olan herkes blokzincire işlem gönderebilirken aynı zamanda blokzincirin konsensüsü (consensus) için onaylayıcı (validator) olabilir. Bu şekildeki ağ yahut sistemler kendisinin güvenliğini sağlayan ve bir çeşit İşin İspatı (Proof of Work) bilgisini sağlayanlar için ekonomik teşvikler (economic incentives) sağlarlar. Buna en güzel örnek Bitcoin gibi kriptoparalarda bloğu üreten madenciye blok ödülüyle beraber o bloktaki tüm işlemlerin toplam işlem bedelinin verilmesidir. Ayrıca daha sonra anlatılacak olan Dash kriptoparasında da AnaUç'ların yaptıkları çeşitli katkıları sayesinde kendilerine blok ödülünün bir kısmı verilir. Bu örnekler ayrıca bahsedilen teşviğe bir nevi örnek gösterilebilir.

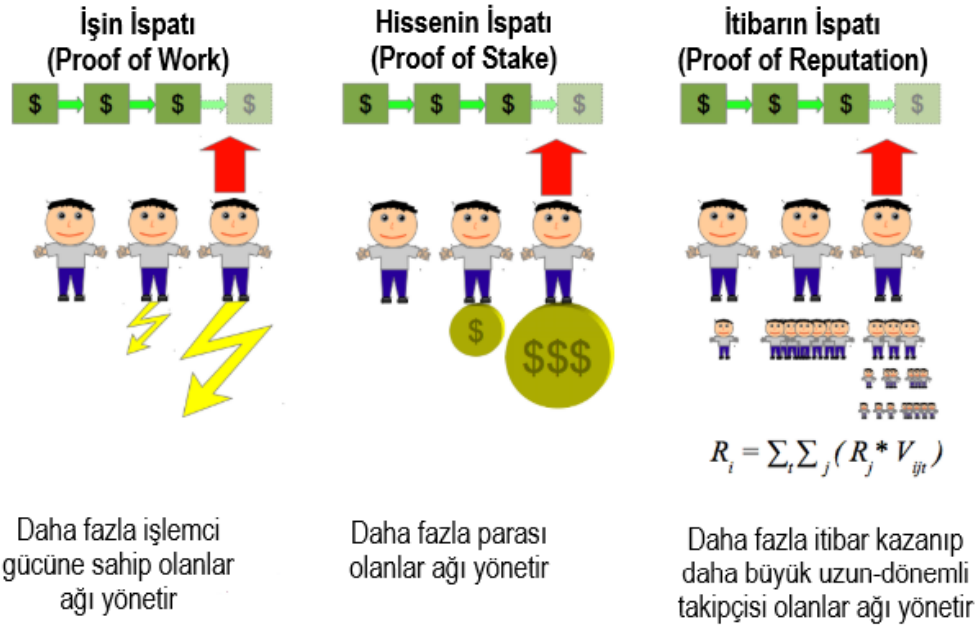
2. **Gizli (Private) Blokzincir:** İzne tabi olan blokzincir tipidir. Ağ yöneticisi tarafından bir şekilde davet edilmeyen kişiler genellikle sistemin yahut ağın bir parçası olamazlar. Aynı zamanda onaylayıcı ve katılımcı rolleri kısıtlıdır.

3. **Hibrit (Hybrid) Blokzincir:** Merkezi güvene dayalı sistemle güvenin dağıtıldığı sistemin birleştirildiği blokzincir tipidir. Zincirin nasıl çalıştığı, ne miktarda merkezileşme ve merkezisizleşme yapılıp bunların ne derece uygulandığına göre değişir.

4. **Yanzincirler (Sidechains):** Bir blokzincir temel alınarak ona paralel olarak çalıştırılan blokzincir kayıt defterine ait tasarıma yanzincir denilir. Ana blokzincirdeki girdiler yanzincire eşleştirilip ilişkilendirilebilir (linkled to and linked from). Böylece yanzincir, ana blokzincir bağımsız bir şekilde çalışabilir.

2.1.2 Kriptoparalarda Konsensüs

Blokzincirler gibi dağıtık işleme tabi olan sistemlerdeki en büyük sıkıntılardan birisi çeşitli hataların olması durumunda bile sistemin genel güvenilirliğinin sağlanabilmesidir. Sistemin tepesinde onu yöneten herhangi bir merkezi yapı olmadığından dolayı sistemde yaşanacak ve güven kaybına sebep olacak her türlü hata, saldırı ya da işlem yavaşlığı dalga halinde tüm yapının ve kullanıcıların etkilenmesine neden olarak o sistemi töhmet altında bıracaktır. Merkezi sistemlerde "merkezi bir yönetici" sistemi yönetme yetkisine sahip olduğundan bu şekilde bir soruna tabi değildir. Bitcoin gibi yüzbinleri, belki de milyonları bulan kullanıcı sayısı olan dağıtık sistemlerde herhangi bir yetkiye sahip hiçbir



Şekil 2.4: Konsensüs Tipleri [14]

kullanıcı yahut mekanizma olmadığından bu dağıtık sistemler etkili, adil, gerçek zamanlı, fonksiyonel, güvenilir ve emniyetli bir yapıya ihtiyaç duyarlar.

Dağıtık sistemlerdeki güvenilirliğin sağlanması konsensüs mekanizmasıyla gerçekleştirilir. Blokzincir, santral saat senkorinizasyonu, insansız hava araçlarının kontrolü gibi çeşitli farklı sistemler konsensüs mekanizmasını kullanır. Kısaca konsensüs dağıtık sistemlerdeki tek bir veri yahut tek bir durum üzerine tüm onaylayıcıların zorunlu olarak mutabakata (necessary agreement) varmasıdır. Blokzincirde konsensüs, sayısı yüzbinleri bulabilen onaylayıcıların bloklara işlenmiş işlemlerin ve blok madenciliği işlemlerinin onaylanıp tasdik edilmesinin sağlanmasıdır, [21].

Çeşitli konsensüs tipleri bulunmaktadır, kriptoparalarda ise genellikle aşağıdaki iki konsensüs tipi kullanılmaktadır, [20]:

1. **İşin İspatı (Proof of Work aka. *POW*):** Bitcoin ve Litecoin gibi popüler kriptopara ağları tarafından kullanılan konsensüs tipidir. İşlem gönderen bir düğüm yahut kullanıcının oluşturup ağa gönderdiği bloğun üzerine blokzincirde yeni bloklar eklenmesine hak kazanmasıdır. Yani örneğin X kriptoparası için 1000. bloğu oluşturup ağa gönderen bir kullanıcının üzerine başka kullanıcılar tarafından 1001. blok; o 1001. blok üzerine de 1002. blok ürettirilir ve bu böylece devam eder. Yapmış olduğu işlemler onaylayıcıların büyük çoğunluğu tarafından kabul edilmesi

takdirde ürettirilen 1000. blok için konsensüs oluşturulmuş demektir. Ne var ki bu yöntem yüksek miktarda enerji gerektirir ve daha uzun sürer.

2. **Hissenin İspatı (Proof of Stake aka. *POS*):** Katılımcı olan bir düğüme sahip olduğu sanal para birimi tokenları sayısıyla orantılı olarak açık kayıt defterinin devamlılığının sağlanmasındaki sorumlulukların paylaştırılmasıdır. POW algoritmasına göre daha az enerji tüketir ve dolayısıyla daha az masraflıdır.

3. Bahsedilen ispatların yanında ayrıca Proof-of-Burn (PoB), Proof-of-Stake-Velocity (PoSV), Proof-of-Importance (PoI) ve Proof-of-Reputation (PoR) gibi daha birçok çeşitli konsensüs tipleri/modelleri bulunmaktadır, [14].

Şekil 2.4'da basit bir şekilde 3 farklı konsensüs tipi gösterilmektedir. PoW için kim daha fazla işlem gücüne sahip olursa onun ağa daha çok etki ettiği; PoS için kimin daha fazla parası varsa ağa daha çok etki ettiği ve PoR için kimin daha fazla ünü (reputation) ve daha uzun dönemli takipçi tabanı varsa ağa o düğümün daha çok etki ettiği belirtilir.

Konsensüs protokolü için resmi gereklilikler aşağıdakilerini içerebilir [21]:

1. **Anlaşma (Agreement):** Tüm doğru işlemler aynı değer üzerinde mutabık olmalıdır.

2. **Zayıf Doğrulama (Weak validity):** Herbir doğru işlem çıktısı doğru bir işlemin girdisi olmalıdır.

3. **Güçlü Doğrulama (Strong validity):** Bütün doğru işlemler aynı girdi değerini alıyorlarsa hepsinin aynı çıktı değerini vermesi gerekir.

4. **Sonlandırma (Termination):** Tüm işlemler eninde sonunda bir çıktı değerinde karar kılmalıdır.

2.1.3 Bloklar

Bloklar özeti alınıp (hashed) şifrelenmiş (encoded) olan geçerli işlemler kümesini Merkle ağacında tutulduğu düğümlerdir. İlk blok hariç tüm bloklar kendisinden önceki bloğun kriptografik özetini tutar, böylece her iki blok birbirine bağlanmış olur. Birbirine bağlı olan bloklar da böylece zinciri oluşturur. Yinelemeli şekilde sürekli vuku bulan bu işlem ta ilk bloğa kadar blokzincirdeki tüm blokların bütünlüğünü sağlar, [19], [55].

Bazen aynı anda farklı madenciler tarafından farklı blokların üretilmesi durumu oluşabilir, bu da geçici bir "iki kola ayrılmaya" (fork) sebep olur. Her bir blokzincirin kendine has tarihin farklı versiyonlarının derecelendirilmesi algoritması vardır. Bu derecelendirme

kullanılarak aynı anda üretilen bloklardan en yüksek puana sahip olan seçilir. Derecelendirme sonrası seçilmeyen bloklara yetim blok adı verilir. Bu sayede belli bir süre sonra bir blokzincir için birden fazla zincirin oluşmasının önüne geçilmiş olunur, [19].

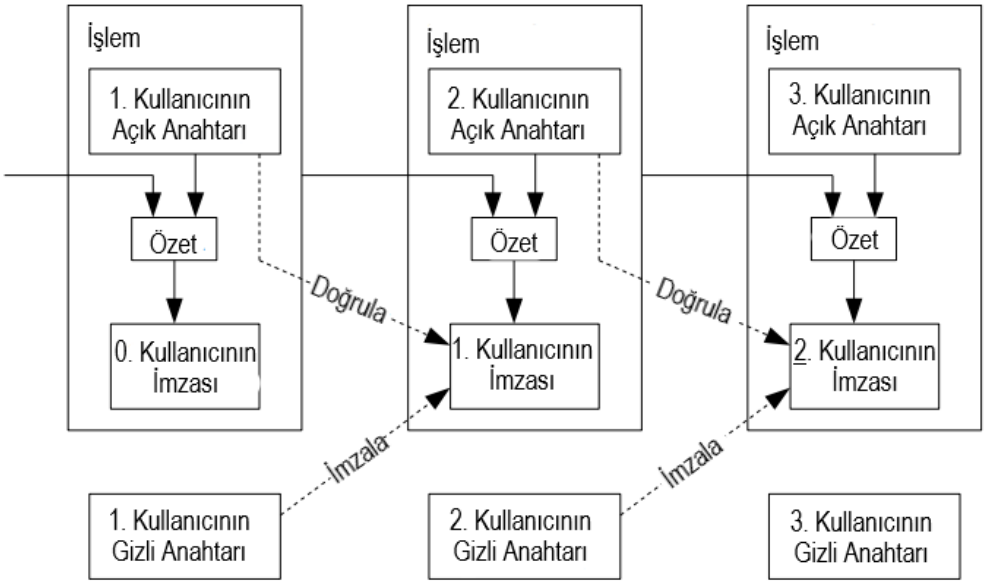
Blok süresi blokzincir ağında yeni bir bloğun üretilmesi için gerekli olan süredir. Bloğun üretilmesinin tamamlanmasıyla beraber ilgili blok doğrulanabilir olur. Bloğun üretilip doğrulanması ve zincire dahil edilmesi demek kullanıcıların yaptıkları işlemlerin gerçekleşmesi demektir. Bunun anlamı blok üretme süresi ne kadar hızlıysa o kadar hızlı işlemler gerçekleştirilir. Ethereum için blok üretme süresi 14-15 saniye civarındayken Bitcoin için bu süre ortalama 10 dakikadır, [18].

Blokzincire kaydedilen her bir blok tekil bir kriptografik anahtar ile korunur. Zincire yeni bir blok ekleneceği zaman bir önceki bloğun anahtarı da dahil her şeyi yeni bloğun anahtarının üretilmesi için kullanır. Bu da iki blok içerisinde bir önceki bloğun özetinin alınmasının yanında farklı bir bağımlılığın oluşmasını sağlar. Üçüncü bir blok ekleneceği zaman ilk iki bloktaki içerikler üçüncü bloğun anahtarının üretilmesi için kullanılır. Böylece bu bağımlılık sayesinde tüm bloklar birbirleriyle "zincirlenmiş" olur, [15], [19].

2.1.4 İşlemler

İşlemler "Forth" benzeri bir komut yazma diliyle tanımlanmışlardır. Coin sahibi olan herhangi bir kullanıcı sahip olduğu coinin sonuna bir önceki işlem olan harcanmamış çıktı (unspent output) çıktısının ürettirmiş olduğu özetiyle beraber bir sonraki coin sahibi olacak (coini transfer ettiği) kullanıcının adresinin açık anahtarını coinin sonuna ekler. Coini alacak olan kişi kendi özel anahtarını kullanarak bu işlemi onaylar ve coinin yeni sahibi olur, [55]. Şekil 2.5'de bu durum daha anlaşılır bir şekilde gösterilmiştir.

Ne var ki, coini alan kullanıcı bu coinin bir defadan fazla kez harcanıp harcanmadığını (double spend) kontrol edemez. Bu durumda blokzincirin bünyesinde bulundurduğu kullanıcıların ellerindeki coinleri defalarca harcamadıklarından bir şekilde emin olması gerekir. Bunun bir yolu güvenilir bir merkezi otorite yapısı kullanmaktır. Ancak bu durum blokzincir teknolojisinin kurmuş olduğu dağıtık güven sisteminin amacının yok edilmesi demek olacağından daha önce de bahsedilen konsensüs mekanizmasına başvurulur. Kullanıcının gönderdiği aynı harcanmamış çıktı değeri için birden fazla işlem olması durumunda blokzincir bunlardan sadece ilkini kabul eder ve daha sonraki tüm işlemler geçersiz sayılır. Bunun mümkün olması için tüm işlemlerin bilinmesi gerekir. Bunun sağlanılabilmesi için ilk olarak işlemlerin umuma arz edilmesi (publicly announced) gerekir. Zincirdeki tüm kullanıcıların büyük çoğunluğu yani konsensüs bu işlemlerden bir tanesini; yukarıda açıklanan durumda ilk gönderileni geçerli işlem olarak kabul eder. Ödemeyi



Şekil 2.5: Bitcoin'deki İşlemlerin Yapısı [55]

gerçekleştirenin her bir işlemi için ispatı olması gerekir, böylece bu ispatı kullanarak konsensüs mekanizması ilgili işlemi onaylayabilir, [55].

Bir işlem içerisinde bir yahut daha fazla girdi ve bir yahut daha fazla çıktı olabilir. Daha sonraki konularda bahsedilecek olan Zcash gibi gizli kriptoparalarda ise hiç girdi ve çıktı kayıt defterinde görünmeyebilir, ancak maden ödülünün olduğu işlemler haricinde daima en az bir girdi ve en az bir çıktı vardır. Birden fazla girdi olması demek birden fazla harcanmamış çıktı değeri kullanılarak kullanıcı veya kullanıcılara coin transferi yapmış olduğu anlamına gelir. Bu harcanmamış çıktılar tek bir adrese ait olduğu gibi birden fazla farklı adrese de ait olabilir. Aynı zamanda birden fazla çıktının olması da coin gönderecek kişinin birden fazla adrese coin gönderilebilmesini sağlar. Coinin gönderildiği bu çıktı adresleri birden fazla adresi olan bir kullanıcıya ait olabileceği gibi birçok farklı kullanıcının adreslerine de ait olabilir. Blokzincir haricindeki İnternet üzerinden çevrimiçi (online) yapılan EFT işlemi, havale yahut kredi kartı alışverişi gibi diğer tüm mevcut para gönderme sistemlerinde Bitcoin gibi kriptoparalarda yapıldığı gibi tek bir "işlemde" birden fazla kullanıcının yine birden fazla kullanıcıya farklı miktarlarda para göndermesini sağlayan herhangi bir yapı yahut mekanizma mevcut değildir. Bu da kriptoparalar için oldukça önemli bir avantaj anlamına gelir.

İşlem bedeli, kullanıcıların işlemleri gerçekleştirmek için madenciye ödedikleri bedeldir. İsteğe bağlı olmasıyla beraber bloğu üretmek isteyen madenciler genellikle en fazla işlem bedeli içeren işlemleri seçme eğilimi gösterirler. Bu da işlem bedeli yüksek olan işlemlerin işlem bedeli az olan yahut hiç olmayanlara göre daha çabuk seçilmesi anlamına gelir. İşlem

bedeli genellikle işlemin boyutuna göre belirlenir. İşlemin boyutu da işlemi oluşturan girdi ve çıktı sayısına göre belirlenir.

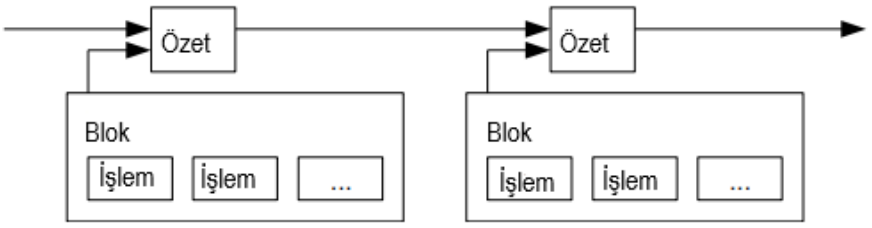
2.1.5 Madencilik

Madencilik (mining) işlemci gücü kullanılarak yapılan bir çeşit kayıt tutma işidir. Madencilik işi yapan kişilere **madenci (miner)** adı verilir. Madenciler blokzincir kullanıcıları tarafından genellikle havuz gibi bir yapı içerisinde yayınlanmış ve henüz blokzincire eklenmemiş işlemleri bir blok içerisine toplayıp ağda yayınlayarak blokzincirin tutarlı, tam ve değiştirilmez bir biçimde kalmasını sağlarlar. Bahsedildiği üzere herbir blok kendisinden bir önceki bloğun SHA-256 kriptografik özetini tutar, [19].

Blokzincire dahil edilebilmesi için bir bloğun **işin ispatını** içermesi gerekir. Blokzincirdeki konsensüsün büyük çoğunluğu, üretilmek için en fazla çaba sarfetmeyi gerektiren en uzun zincirle temsil edilir. Hesaplama/işleme gücünün büyük çoğunluğı dürüst (honest) düğümler tarafından kontrol edilirse blonzincirdeki "dürüst" zincir diğer rakip zincirlere göre daha hızlı büyüyecektir [19]. Bir blokzincir için aynı anda birden fazla blok üretilmesi ihtimali her zaman olduğundan dolayı bir blokzincirde birden fazla zincirin oluştuğu görülecektir. Bu zincirlerden daima en uzun kayıtları/blokları olan seçilir. Konsensüsün büyük çoğunluğu bahsedildiği gibi dürüst düğümlerden oluşuyorsa kabul gören zincir dürüst zincir olur. Kötü niyetli kişilerin bu zincirdeki herhangi bir blokta değişiklik yapmayı istemesi durumunda bloğu tekrardan üretmesi ve ondan sonra gelen tüm blokları da yine ayrıca üretmesi gerekir. Kötü niyetli kişi bir yandan eski blokları tekrardan üretmeye çalışırken bir yandan da en iyi zincire sürekli olarak dürüst düğümler tarafından yeni bloklar eklenir. Bu nedenle kötü niyetli kişilerin blokzincire tam anlamıyla etki edebilmeleri için bloğu üreten madenciler ve manenci havuzlarından çok daha iyi ve hızlı işlemci ve hesaplama gücüne sahip olmaları gerekir. Bu işlemi de "geleneksek" olarak bahsedilen günümüz bilgisayarlarıyla beraber yapmak mümkün değildir; kuantum-bilgisayarlar gibi kıyaslanmayacak derecede hızlı sistemlerle blokzinciri kırmak biraz daha mümkün olur.

2.1.6 Zaman Damgası Sunucusu

Üretilecek olan bloktaki işlemlerin/kayıtların özeti alındıktan sonra zaman damgası alınıp herkese ve her yere yayınlandıktan sonra zaman damgası sunucusunun işi başlar. Zaman damgası sayesinde üretilen bloğun üretildiği zamanda içerisindeki verilerin (yani işlemlerin ve işlemlerdeki para transferlerinin) gerçekten de var olduğu ve o zamanda üretildiği ispatlanmış olur. Herbir zaman damgası kendi özetinin bünyesinde bir önceki bloğun zaman damgasını içerir. Yani Şekil 2.6'de gösterildiği gibi herbir blok kendisinden sonra



Şekil 2.6: Zaman Damgası Alınan Bloklar, [55]

gelecek blokların zaman damgasına katılan özetine katkıda bulunarak tüm blokların birbirleriyle alakalı olduğu bir zincir oluşturulmuş olur, [55].

2.1.7 İşin İspatı (Proof-of-Work)

Dağıtık zaman damgası sunucusunu eşler arası *P2P* ağda uygulayabilmek için daha önce birkaç defa daha bahsedilmiş olan işin ispatı sisteminin kullanılmasını gereklidir. Bu sistem Adam Back'in 1997 yılında HashCash adını verdiği anti-spam şemasına dayanır. İşin ispatı, SHA-256 özet algoritmasında olduğu gibi sıfır bitleriyle başlayan özetle özetlenmiş bir değerin taranmasını içerir. Özetteki gereken sıfır biti sayısınca yapılması gereken ortamala iş doğru orantılı olarak artar. Çıkan sonuç tek bir özet çalıştırılarak doğrulanabilir, [19].

Zaman damgasının çalışabilmesi için, blokzincirde üretilecek bloğun ihtiyacı olan sıfır bitleri veren bir değer bulununcaya kadar bloktaki bir kereye mahsus üretilen anahtar (nonce) sürekli olarak artırılarak işin ispatı uygulanır. İşlemcinin yapmış olduğu iş işin ispatının istemiş olduğu şartları bir kez sağladıktan sonra üretilen blok yapılan bu işler tekrardan yapılmadığı sürece değiştirilemez. Daha önce de bahsedildiği gibi, eklenen bloğu değiştirmek kendisinden sonra gelecek olan tüm blokları da değiştirmeyi kapsayacaktır, [19].

İşin ispatı sistemi ayrıca Altkısım 2.1.2'de bahsedilen konsensüsün yani çoğunluğun karar vermesinde karşılaşılan bir sorunu da çözer. Konsensüs, IP temel alınarak karar verilseydi; yani bir IP adresi bir oy kullanabilir kuralı olsaydı bir kişi paket üretme gibi yöntemlerle bir sürü IP göndererek konsensüs kararını etkileyebilirlerdi. İşin ispatı sistemi özellikle işlemci tabanlıdır, yani bir işlemci bir oy verebilir kuralı geçerlidir, [21]. Yukarıda da bahsedildiği gibi en çok işlemci gücüne sahip olan en uzun zincire sahip olur; en uzun zincir de en iyi zincir yani blokzincirin ana zinciri olur.

İşlemcilerin her geçen gün artan işlem gücü hızı ve düğümlerde beraber çalışmayla gelen hızla mücadele edebilmek için geçerli bir özeti bulma zorluğu yani işin ispatının üretilebilmesinin zorluğu ortalama her iki haftada bir düzenlenir. Bloklar çok hızlı üretilirse işin ispatı ve özet bulma zorluğu, dolayısıyla yeni bir blok üretme ve blokzincire bu bloğu ekleme hızı buna orantılı olarak artar, [18].

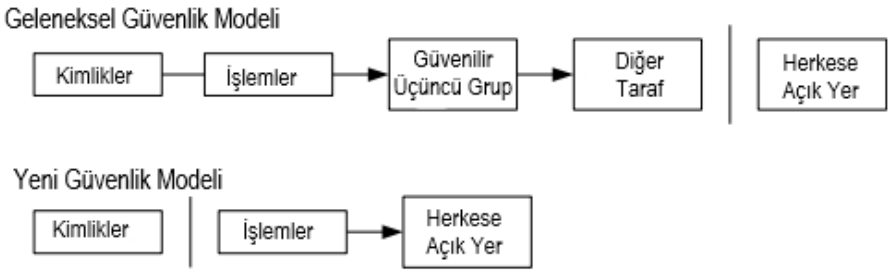
2.1.8 Ağ

Blokzincirlerde ağın çalışabilmesi için gerekli olan adımlar aşağıdaki gibidir, [19]:

1. Yeni işlemler tüm düğümlere yayınlanır.
2. Herbir düğüm işlemleri bir bloğa yerleştirir.
3. Herbir düğüm kendi bloğu için zor bir işin ispatı bulmaya çalışır.
4. Düğümlerden biri işin ispatını bulduğu an ürettirmiş olduğu bloğu tüm düğümlere yayınlar.
5. Düğümler, bloktaki tüm işlemler geçerli olup yeniden harcanma durumu olmadıysa ilgili bloğu kabul eder.
6. Düğümler, mevcut bloğu kabul ettiklerini tüm blokzincire yayınlamak ve belirtmek adına ilgili bloğu "bir önceki blok" kabul edip o bloğun özetini kullanarak yeni bir blok üretmeye çalışırlar.

Düğümler daima en uzun zinciri doğru zincir olarak kabul ederler. Aynı anda iki bloğun ürettirilip farklı düğümler bu iki bloğa yeni bloklar ekledikleri takdirde iki farklı zincir oluşmuş olur. Bu durumda düğümler kendi zincirleri doğru zincir kabul ederken diğer zinciri de en uzun olma ihtimaline karşın kaydederler. Eninde sonunda zincirlerden birisi diğerinden daha uzun olacağından uzun olan tüm düğümler tarafından kabul edilir ve kısa kalan zinciri esas zincir olarak kabul eden düğümler uzun zincire geçerler. Böylece blokzincirde daima sadece bir tane tam zincirin bulunması garanti altına alınmış olunur, [19].

Bunun yanında yeni blokların tüm düğümlere hemen ulaşmasına gerek yoktur. Üretilen blok, düğümlerin çoğunluğu tarafından kabul edilmesi yeterlidir. Ayrıca üretilen bloklar kaybolmaya karşı korumalıdır. Herhangi bir düğümün eksik bir blok alması durumunda bir sonraki bloğu aldığında eksik blok olduğunu fark edecek ve eksik olan o bloğu talep edecektir [19].



Şekil 2.7: Geleneksel Bankadaki Gizlilik - Blokzincirdeki Gizlilik [55]

2.1.9 Gizlilik

Geleneksel bankacılık modeli erişim kısıtlaması (mümkün olan asgari erişimi verme politikası) ve güvenilir üçüncü kişilerin kullanılması gibi yöntemler vasıtasıyla belli bir seviyede gizlilik elde ederler. Blokzincirlerin dağıtık yapısı ve tüm işlemlerin tüm düğümlere açık bir şekilde yayınlanması bu yöntemleri kullanarak gizliliğin sağlanmasını imkansız kılar. Özellikle para transferleri gibi ciddi önem arz eden işlemlerin olduğu sistemlerde taraflar özellikle gizliliği ve anonimliği talep edeceğinden dolayı her şeyde olduğu gibi blokzincirde de gizlilik ihtiyacı elzemdir. Bitcoin gibi blokzincirlerde bu gizlilik açık anahtarların ve işlemlerin yapıldığı adreslerin tamamının anonim kalması vasıtasıla gerçekleştirilir. Blokzinciri inceleyen herhangi biri yapılan coin transferinin hangi adresten hangi adrese, ne zaman ve ne kadar coin miktarında yapıldığını rahatça görebilir; ancak hiçbir gerçek kişi, kuruş, kurulum grup yahut varlıkla transferlerin yapıldığı adresler ilişkilendirilmediğinden bu işlemi kimin yaptığını anlaması mümkün olmaz. Şekil 2.7'te geleneksel bankacılık ve blokzincir karşılaştırılması yapılmıştır.

Bitcoin gibi ilk blokzincirlerde sadece adresler ve açık anahtarlar anonim tutularak tam anlamda bir gizlilik sağlanılacağı düşünülmüştür. Ancak yıllar içerisinde çeşitli kişi ve gruplar tarafından yapılan farklı araştırmalar, siber saldırılar veya çeşitli analizler bu düşüncenin oldukça yanlış olduğunu acı bir şekilde kanıtlamıştır. Bu nedenle misal olarak kriptoparaları tamamıyla anonim zanneden kötü niyetli gruplar yahut suç örgütleri tarafından yapılan işlemler tespit edilebilmiş; bu işlemlerde kullanılan tüm coinler artık "kirlenmiş coin" olarak kötü bir şekilde damgalanmışlardır, [15]. Bir sonraki başlık olan Kısım 2.3'te anonim adreslerde gizliliğin neden neredeyse hiçbir şekilde gizlilik sağlamadığı ve bunun için zaman içerisinde nelerin önerildiği anlatılacaktır.

2.2 Bitcoin Nedir?

Bitcoin, eşler arası (peer-to-peer) teknolojisini kullanarak bankalar gibi herhangi bir merkezi otorite (central authority) olmadan çalışır. İşlemlerin yönetimi ve bitcoinlerin dağıtımı toplu olarak ağ tarafından idare edilir. Bitcoin açık kaynaklıdır (open-source), yani tasarımı halka açıktır, [2]. 6 Haziran 2020 23:00 tarihinde bir bitcoin (1 BTC) tam olarak 66.278,13 TL'ye eşittir, Şekil 2.8'deki grafikte Bitcoinin Amerikan Dolarına karşısıdaki yıllara göre değişimi verilmiştir. **BTC**, Bitcoin kriptoparasının para birimidir. Blokzincirin bünyesinde bulundurduğu şifreli işlemlerden dolayı Bitcoin ve haleflerine kriptopara (cryptocurrency) adı verilir.

Bitcoin'in toplam arz sayısı 21 milyon ile sınırlıdır, yani en fazla 21 milyon BTC üretimi yapılabilir. Piyasadaki 04 Haziran 2020 tarihi itibariyle mevcut toplam BTC sayısı 18,39 milyon BTC'dir. Ayrıca yine mevcut durumdaki Bitcoin'in toplam piyasa değeri 180,24 milyar dolardır ki TL bazında 04 Haziran 2020 tarihinde yapılan basit bir hesaplamaya göre yaklaşık 1.22 trilyon TL'ye tekabül etmektedir. 2017 yılında Cambridge Üniversitesi tarafından yapılan bir araştırmada birçoğunun Bitcoin kullandığı tahmin edilen 2.9 ile 5.8 milyon kriptopara kullanıcısının olduğu tespit edilmiştir, [18].

Yüzlerce yıl boyunca yapılan klasik ticari işlemlerin aksine Bitcoin tamamıyla dağıtıktır. Anonim bir şekilde para aktarımı ve alış-veriş gibi ticari işlemler sağladığından dolayı çeşitli yapıcı ve yıkıcı eleştirilere maruz kalmıştır. En başta Bitcoini ve blokzincir teknolojisini bulan Satoshi Nakamoto'nun kimliğinin 12 yıl sonra bile ortaya çıkmaması çeşitli spekülasyonlara yol açmıştır. 2010 yılında Satoshi, Bitcoin'i bir başka isme devretmiş; 2012 yılında Bitcoin'in sürekliliğinin ve devamlılığının sağlanması amacıyla Bitcoin Foundation kurulmuştur, [18].

Bitcoin ile yapılan ilk satın alma işlemi 2010 yılında 10.000 BTC'ye pizza satın alınmasıyla gerçekleştirilmiştir. 2013 yılında Amerikan'ın FBI gibi çeşitli kurumları Bitcoin kullanılarak yapılan çeşitli suçlardan tutuklamalarla beraber çeşitli miktarlarda Bitcoin parası ele geçirmişlerdir. 5 Aralık 2013'te Çin Halk Bankası Çin'in finans merkezlerinin Bitcoin kullanmasını yasaklamıştır, [18]. Bu gibi olayların yanında ayrıca Bitcoin kriptoparası yıllar içinde çeşitli ciddi eleştirilere maruz kalmıştır. Özellikle sağladığı anonimlik ve yapılan para transferlerinin tespitinin zorluğu vergi kaçakçılığı, elektronik hırsızlık, terörizm, mafya, uyuşturucu ve insan kaçakcılığına bağlı kara para aklama işlemleri gibi birçok suç teşkil eden eylemleri yapanları Bitcoin'e mıknatısının demiri çekmesi gibi çekmiştir. Bu durum beraberinde çeşitli hukuki hatta dini tartışmaları beraberinde getirmiş; yıllar içerisinde çeşitli kısıtlayıcı mevzuatların yayınlanmasına neden olmuştur. Bunun yanında Amerika'daki sanal para kanunları detaylı bir şekilde açıklanmaktadır, [26]. Ayrıca Türkiye'de Bitcoin'in yasal statüsü, [62] ve Türkiye'deki Bitcoin ve sanal para



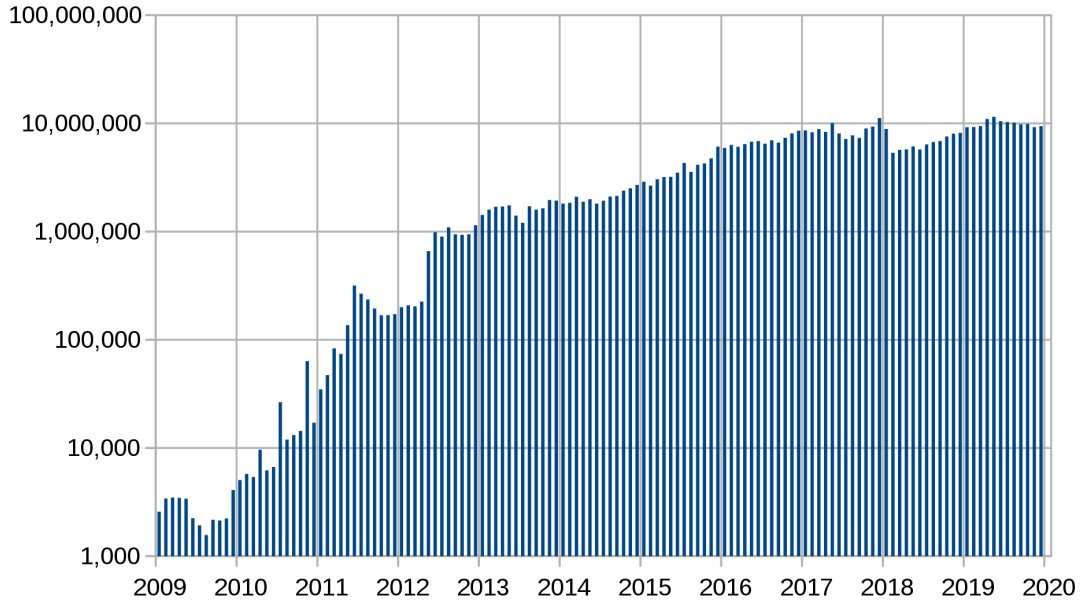
Şekil 2.8: Yıllara Göre BTCUSD (Bitcoin Amerikan Doları) Grafiği [17]

olan kriptoparaların yasal mevzuatlar karşısındaki durumu açıklanmıştır, [16]. Cezayir, Pakistan ve Mısır da dahil 9 ülkede Bitcoin tamamıyla yasakken Çin, Kuveyt Ve Litvanya gibi 15 ülkede de kısmi yasak olduğu belirtilmektedir, [18].

Ekim 2011'de ilk defa Bitcoin'in açık kaynak kodlu yazılımı kullanılarak Liteocin adında yeni bir kriptopara çıkartılmıştır. O tarihten beri belki de yüzlerce yeni kriptopara çıkartılmış, halen de çıkartılmaya devam etmektedir. Tezin devamında bahsedilecek olan tüm anonim kriptoparalar da Bitcoin'den sonra yayınlanmışlardır. Bunlardan Dash, Zcash, PIVX ve Verge açık kaynak kodlu Bitcoin yazılımı üzerine geliştirilmiştir. Monero ise Litecoin kodu kullanılarak çatallandırılmıştır.

Bitcoin'in değeri tamamen "arz talep" ilişkisi ile belirlenir. Alım-satım yapan çeşitli platformlarda alıcı ve satıcıların emirlerini birbiri ile eşleştiren yazılımlar kullanılır. Kullanıcıların yaptığı alım ve satım işlemlerini fiyat ve piyasa bilgileri olarak yayınlayan kriptopara alım satım platformları birbirine ya da bir merkeze bağlı değildir. Her platform üzerinde Bitcoin fiyatı bağımsız olarak oluşur. Kullanıcıların alım satım platformları arasında yaptığı alım satım işlemleri kriptopara alım satım platformlarında fiyatların birbirine yakın olmasına zemin hazırlar [13].

Bitcoin'in temel para birimi yukarıda da bahsedildiği gibi **bitcoin**'dir. Bitcoin kelimesi büyük harfle **Bitcoin** şeklinde yazıldığında tüm kriptosistemle beraber kriptoparanın kendisi olarak belirtlilir. Küçük harfle **bitcoin** şeklinde yazıldığında da para biriminden bahsedilmiş olunur. Bitcoin kısaca **BTC** olarak da belirtilir. BTC aynı zamanda **XBT** ile beraber Bitcoin'in "hisse senedi kodu (ticker)" sembolleridir [18]. En küçük Bitcoin birimi **miliBitcoin** (***mBTC***) ve **satoshi** (***sat***)'dir. 1 satoshi 10^{-9} BTC ve 1 mBTC 10^{-3} BTC yahut 10^{6} satoshidir. Oluşturulan Bitcoin kriptoparasının kısıtlarından dolayı en fazla 21 milyon bitcoin değerine ulaşılabilir. Mevcut durumda yaklaşık 18 milyon bitcoin

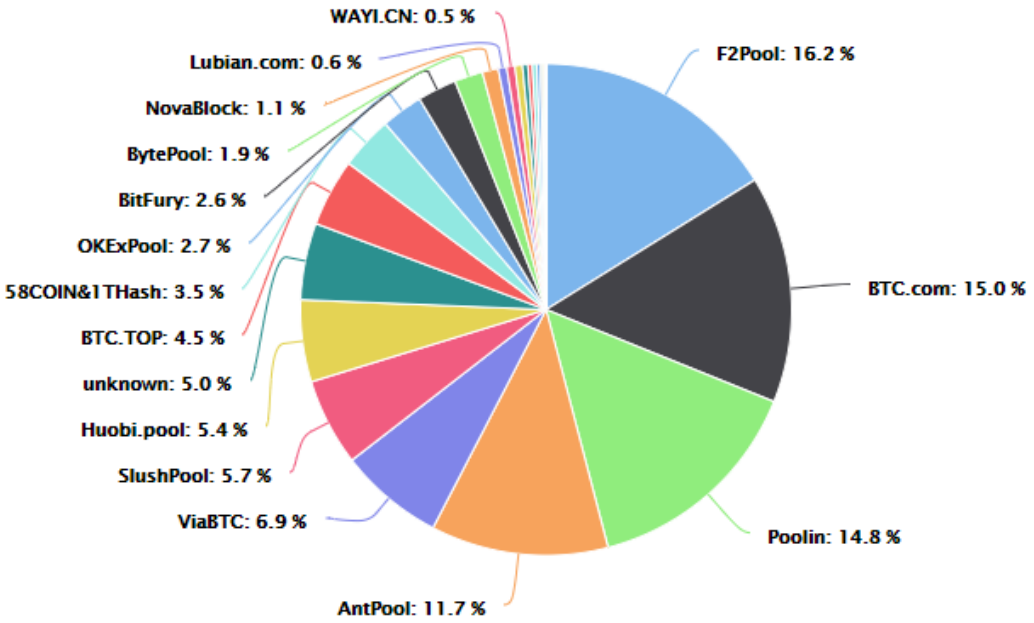


Şekil 2.9: Yıllara Göre Bitcoin İşlemleri Grafiği

bulunmaktadır. Tüm bu veriler birlikte değerlendirildiğinde Bitcoin kriptoparasının yıllar içerisinde tüm dünyada ciddi anlamda popilarite kazandığı anlaşılacaktır. Şekil 2.9'deki grafikte de görüldüğü gibi yıllar içinde yapılan Bitcoin işlemleri ciddi şekilde artmıştır.

Bitcoin kayıt defteri (ledger) 3 Ocak 2009'da başlatılmış ve 9 Ocak 2009'da ilk Bitcoin bloğu Satoshi Nakamoto tarafından ürettirilmiştir. İlk başlarda Bitcoin blok ürettirme ödülü 50 BTC iken her 210,000 blokta bir Bitcoin blok ürettirme ödülü yarıya düştüğü için Haziran 2020 ile beraber bu ödül 6.25 BTC değerine kadar düşmüştür. İlk yıllarda kriptopara madenciliği bireysel kullanıcılar tarafından yapılmaktayken kazancın yüksek olması gibi çeşitli sebeplerden dolayı zaman içerisinde Bitcoin madenciliği büyük bir sektöre dönmüş ve artık madencilik daha çok bünyesinde çok fazla madenci barındıran madenci havuzları yahut devasa madencilik yapan cihazlara sahip olan madenciler tarafından yapılmaktadır. Şekil 2.10'teki grafikte son 1 yıldaki tüm madencilerin ve maden havuzlarının Bitcoin blok ödülü "pastasından" aldıkları payları görülmektedir. Şekil 2.11'deki tabloda da son 1 yıldaki en büyük 10 maden havuzunun Özet (Hash) oranı yüzdesi, ürettirilen blok sayısı gibi veriler gösterilmektedir.

Bitcoin işlemleri yapabilmek için evvela bitcoin sahibi olmak gerekir. Bitcoin sahibi olmanın çeşitli yolları bulunur. Genellikle sıfırdan bitcoin sahibni olmak için Bitcoin sağlayıcılarından (exchanges) Amerikan Doları yahut Türk Lirası karşılığında satın alınabilir. Bir diğer yöntem Bitcoin madenciliği yapmaktır, ki çeşitli madenci havuzlarına üye olup üretilen bloğa işlemci gücü vasıtasıyla yardımcı olma karşılığında blok ödülünden



Şekil 2.10: Son 1 Yıldaki Tüm Madencilerin ve Maden Havuzlarının Blok Ödülü Pastasındaki Payları [12]

	Havuz	Hash Oranı Hissesi	Çıkarılmış Bloklar	Empty Blocks Count	Boş Blok Yüzdesi	Ort. Blok Hacmi (Bytes)	Ort. Her Blok İçin İ. Harçları (BTC)	Blok Ödülü başına İ. Harcı Yüzdesi
0	NETWORK	100.00 %	53,704	213	0.40 %	1,073,615	0.30611244	2.53 %
1	F2Pool	16.16 %	8,678	59	0.68 %	1,071,165	0.30277384	2.51 %
2	BTC.com	14.95 %	8,031	46	0.57 %	1,064,094	0.31506323	2.59 %
3	Poolin	14.84 %	7,969	1	0.01 %	1,074,699	0.28676248	2.36 %
4	AntPool	11.68 %	6,274	42	0.67 %	1,078,370	0.31121648	2.58 %
5	ViaBTC	6.88 %	3,696	9	0.24 %	1,073,766	0.30554745	2.51 %
6	SlushPool	5.74 %	3,084	11	0.36 %	1,086,419	0.33400586	2.74 %
7	Huobi.pool	5.39 %	2,893	18	0.62 %	1,050,587	0.28835876	2.38 %
8	unknown	5.05 %	2,710	1	0.04 %	1,048,621	0.25989099	2.08 %
9	BTC.TOP	4.46 %	2,394	13	0.54 %	1,084,298	0.34799191	2.84 %
10	58COIN&1THash	3.49 %	1,874	3	0.16 %	1,086,933	0.28377243	2.42 %

Şekil 2.11: Son 1 Yıldaki En Büyük 10 Maden Havuzu Tablosu [12]

pay alarak daha hızlı ve kolay bitcoin sahibi olunabilir. Bir diğer yöntem de bitcoine sahip olan bir adresten doğrudan bitcoin transferi yapılmasıdır.

Herhangi bir şekilde bitcoin sahibi olabilmek için aslında yukarıdaki işlemlerden de önce ilk olarak bir çeşit Bitcoin hesabı gibi düşünülebilecek bir Bitcoin adresine sahip olmak gerekir. Bunun en kolay yolu bir Bitcoin **cüzdanı (wallet)** yüklemektir. Mevcut durumda 3 çeşit cüzdan kullanılmaktadır. İlki en güvenilir yöntem olan tam istemcileri (full client) kullanmaktır. Bitcoin için kullanılan tam istemci **Bitcoin Core** [1] uygulamasıdır. Şekil 2.12'da herhangi yerel makineye indirilmiş Bitcoin Core tam istemcisinin **bitcoin-qt** uygulaması görülmektedir. Tam istemciyi kullanabilmek için bütün Bitcoin blokzincirini yerel makineye indirmek gerekmektedir, ki bu da yaklaşık 250-300GBlık bir verinin indirilmesi ve tüm geçmiş blokların doğrulanması demektir.

Bu kadar karmışık ve pahalı bir işlemi yapmak herkes için mümkün olmadığın dolayı ikinci seçenek olarak hafif istemciler (lightweight clients) sunulmuştur. Hafif istemciler bütün bir blokzinciri yerel makineye indirmezler ve işlem gönderip almak için tam istemcileri kullanılarlar. Bu sayede daha hızlı kurulabilirler ve akıllı telefonlar gibi düşük bant-aralığında çalışan cihazlarda kullanılması mümkün olur. Hafif istemcilerin en büyük problemi, kullanıcı yapılan işlemler için hafif istemciye güvenmek zorundadır. Çünkü tam istemcilerle yapılan bağlantılarda çeşitli hatalar yahut saldırılar olması durumunda yapılan işlemlerin hatalı olması ihtimali artar. Şekil 2.13'de Electrum'un sunduğu hafif istemci uygulaması görülmektedir.

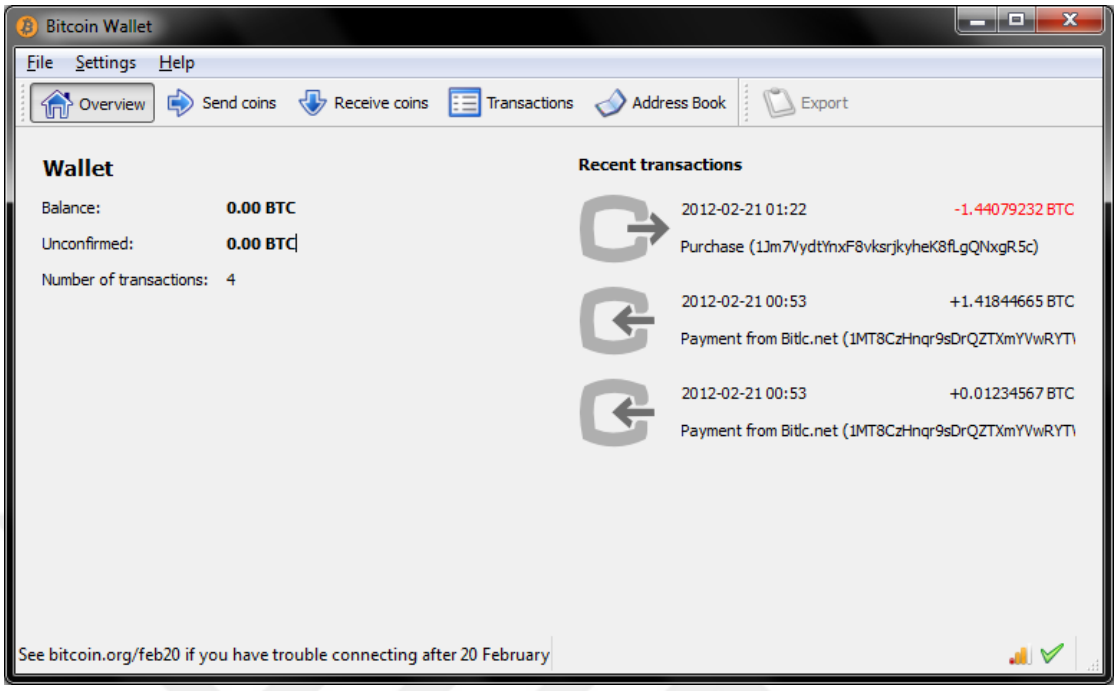
Bitcoin hesabının yönetimi için bir diğer yöntem online cüzdanların kullanılmasıdır. Her ne kadar diğer iki yöntemden daha hızlı ve daha az karmaşık olsa da kullanıcı ilgili adrese tamamen güvenmek zorundadır. Bu durumda kötü niyetli online cüzdanlar kullanıcının çeşitli bilgileriyle bera<ber BTC'lerini çalıp kullanıcıları zarara uğratabilecekleri anlamına gelir. Online cüzdanlar tüm cüzdan çeşitlerinden en güvenilmez olanıdır.

Blokzincir kütüğü, işlemler ve madenciler gibi terimler bir sonraki bölüm olan Bölüm 2.1 Blokzincir Teknolojisi bölümünde daha detaylı bir şekilde anlatılacaktır.

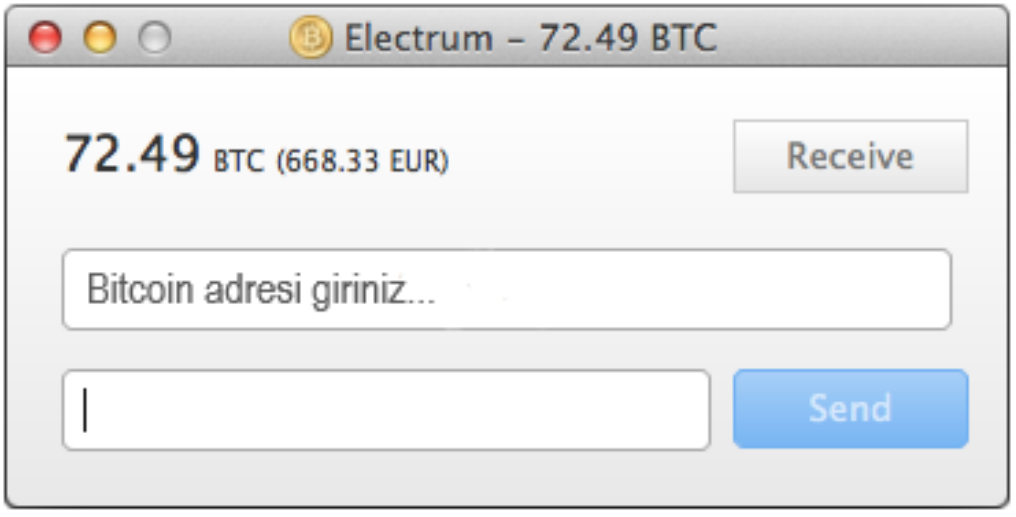
2.3 Bitcoinde Gizlilik

Çıktığı ilk zamanlarda Bitcoin kriptoparası kullanıcı mahremiyetini ve dolayısıyla yapılan işlemlerin güvenliğini daha önce de bahsedildiği gibi yapılan işlemlerde kullanılan adreslerle onları kullanan kullanıcılar arasında hiçbir ilişki tutmayarak sağlamıştır. Yani adres sahiplerinin gerçekten de o adrese sahip olduğunu belirten ülke kimlik numarası, herhangi

[1] https://bitcoin.org/tr/indir web sayfasından Windows, Linux ve Mac OS gibi çeşitli platformlar için indirilebilir.



Şekil 2.12: Son 1 Yıldaki En Büyük 10 Maden Havuzu Tablosu



Şekil 2.13: Son 1 Yıldaki En Büyük 10 Maden Havuzu Tablosu

bir IP yahut herhangi bir dijital kayıt numarası (birincil anahtarlı tablo ID yahut GUID gibi) gibi hiçbir veri tutmaz. Bu sayede genellikle Bitcoin'in güvenli olduğu ve Bitcoin'de yapılan işlemlerin herhangi bir şekilde anonimliğe ve kişi mahremiyitine halel ve zarar getirmeyeceği düşünülmüştür. Öyle ki, özellikle siber suçlarla mücadele veren emniyet güçleri dahil devletin bünyesindeki çeşitli kurumlar Bitcoin işlemlerinin takip edilemeyeceği ve işlem yapanların gerçek kimliklerine hiçbir zaman ulaşılamayacağı konusunda endişenmişlerdir. Gerçekten de teoride yapılan işlemlerin kimin yaptığıyla beraber hangi kullanıcının kime ne kadar bitcoin gönderdiğini blokzincir bünyesinde doğrudan anlamak mümkün değildir. Böylece başta Bitcoin olmak üzere kriptoparalar zamanla vergi kaçakçılığı ve kara para aklama gibi çeşitli suçların merkezi olma potensiyeli elde etmiştir.

Ne var ki, yıllar içerisinde blokzincir üzerinde yapılan analizler, blokzincir öğelerine yapılan saldırılar veya çeşitli algoritmalar vasıtasıyla elde edilen veriler Bitcoin'in düşünüldüğü gibi gizlilik ve anonimlik sağlamadığını ispatlamıştır. Buna en güzel örnek Silk Road isimli internet üzerinden uyuşturucu da dahil çeşitli yasadışı ürünlerin Bitcoin kullanılarak satıldığı online alışveriş sitesidir. Dread Pirate Roberts lakaplı Silk Road'ın kurucusu olan Ross Ulbricht isimli şahısı yakalamadan önce FBI bünyesinde çalışan eski federal ajanın 3760 işlemi 12 ay boyunca takip ettiği belirtilmiştir. Kara para aklama, online uyuşturucu ticareti, bilgisayar korsanlığı hatta 6 kişinin ölümüne azlettirme gibi birçok suç itham edilen Ross Ulbricht 2 Ekim 2013'te tutuklanmış ve Silk Road web sayfası Ekim 2013'te FBI tarafından kapatılmıştır, [25], [47].

Bahsedilen örnekten de anlaşılacağı üzere Bitcoin işlemleri her ne kadar gizlilik sağladığı düşünülse bile aslında hiçbir şekilde gizlilik ve anonimlik sağlamamaktadır. Bitcoin işlemleri tamamen herkese açık olduğundan dolayı herhangi bir adresin gerçek kimliğini yahut gerçekte kullandığı eposta adresi gibi bir bilgisini bilen üçüncü bir şahıs o adresin yaptığı tüm işlemleri, nereden bitcoin temin edip nerelere ne kadar coin transfer ettiğini çok rahat bir şekilde görebilir. Bu durum da gizliliğe önem veren kişi ve kurumlar için çok ciddi bir mahremiyet ihlali anlamına gelmektedir.

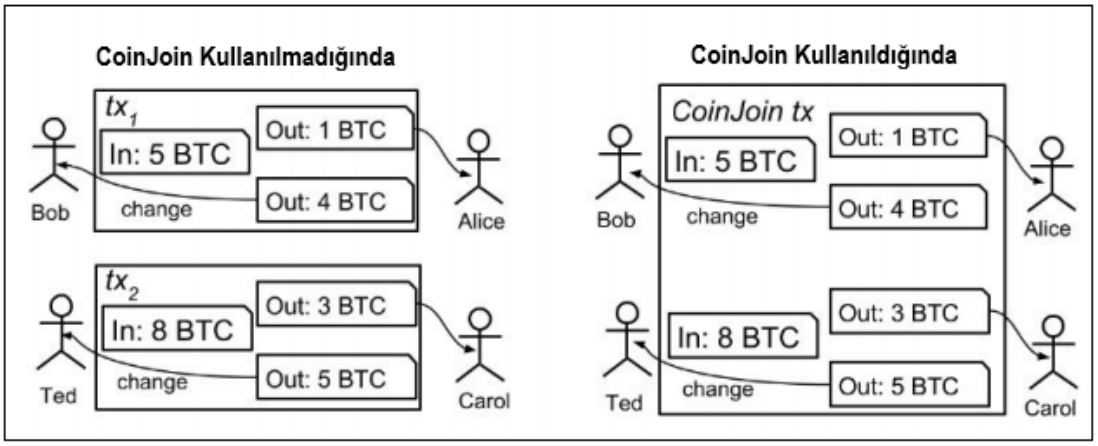
Gizliliğin önemi farklı açılardan anlatıldığı taktirde önemi daha iyi anlaşılacaktır. İlk olarak müşteri açısından bakıldığında çeşitli firmaların müşterilerin yaptığı tüm işlem geçmişini görmesi tek kelimeyle ekonomik anlamda ciddi zarar veren sonuçlara neden olacaktır. Bu şekilde mesela firmalar daha varlıklı olduğunu düşündükleri müşterilerine daha ayrıcalık tanıyabilir yahut bu müşterilere aynı ürünü dinamik bir şekilde daha pahalı satabilirler. Kullanıcı açısından bakıldığında misal olarak kişisel özgürlüklerin kısmen daha az olduğu bölgelerde işlem yapan bir kişinin yaptığı işlem geçmişinin açığa çıkması demek kişinin hapis hatta belki de idama kadar varabilecek çeşitli cezalara maruz kalmasına sebep olabilir. Felsefi ve mantıksal olarak blokzincirlerin ve tabii ki de kriptoparaların temel amacı ekonomik gücün büyük anlamda merkezi otoritelerde

toplanmasının önüne geçip bu otoritelerin kişinin gizliliğine bağlı olarak veri güvenliğinin yanlışlıkla yahut kasıtlı olarak ihlalinin önüne geçmektir. En başta blokzincirin kendisi kullanıcıların bu gizliliğini sağlayamazsa yapılan işlemlerin hiçbir anlamı olmayacaktır. Son olarak anayasal anlamda gizliliğe bakıldığında gizlilik ve anonimlik yasalar tarafından tüm bireylere tanınmış olan bir haktır. Dolayısıyla hükümetler de dahil olmak üzere hiç kimse gereksiz yere, yani herhangi bir suç isnatı yahut Sıkı Yönetim gibi özel bir durum olmadan kasıtlı olarak bireylerin gizliliğini ihlal edemezler, [61].

Bitcoin gibi kriptoparalar için anonimliğin, dolayısıyla gizliliğin önemi anlaşılacağı üzere gerçekten de elzemdir. Farklı açılardan bakıldığından gizlilik ve anonimlik için çeşitli farklı tanımlamalar yapılmıştır. Bu tanımlamalardan en çok kabul göreni anonimlik (anonymity) = takma ad/rumuz (pseudonymity) + takip edilememezlik (unlinkability) şeklindedir, [61]. Takma ad/rumuz özelliği zaten Bitcoin'in ilk sürümlerinden beri sağlanan bir özelliktir. Daha önce de bahsedildiği gibi bitcoini gönderene bir adres ve bitcoini alana başka bir adres tahsis edilirken bu adreslerin gerçek kimlik bilgileriyle hiçbir şekilde eşleşmesi yapılmaz. Bu adreslerle adresin sahipleri arasında hiçbir ilişki bulunamadığı sürece takma ad anonimliğin sağlanması için yeterli olmaktadır. Ne var ki, yeterli bilince sahip olmayan adres sahiplerinin sosyal medya yahut forumlarda adres bilgilerini paylaşması, Amerikan Doları yahut Türk Lirası gibi herhangi bir döviz yani reel para karşılığı bitcoin temin edilen sağlayıcıların web sayfalarındaki açıklarla işlem yapan kişinin IP adresi bilgisiyle bu sayfaya kayıt olmak için gerekli olan eposta adresi gibi bilgilerin sızması yahut bitcoin karşılığı ürün satılan online alış-veriş sitesinin eposta adresi, ad-soyad gibi kişisel bilgi temin etmesinden sonra web sayfasının kurulduğu sunucudaki açıklar gibi çeşitli sebeplerden bu bilgilerin ifşa olması gibi bir sürü farklı çeşitli sebepten kullanıcıların bitcoinde bulunan açık adresleri ile kişisel bilgiler eşleşmesi yapılabilmektedir.

Kullanıcılar tabii olarak kriptosistem ile sürekli olarak temas halinde olacak, sürekli olarak birçok farklı işlem gerçekleştireceklerdir. Takip edilememezlik özelliği üçüncü şahıslar ve hatta blokzincir sisteminin kendisi tarafından bu işlemlerin birbirleriyle herhangi bir şekilde bağlantı tespit edilememesidir. İşlemin takip edilemez sayılması için gönderici adresiyle başka adresler ve işlemler arasında ilişki kurulması, alıcının adresiyle başka adresler ve işlemler arasında ilişki kurulması ve ödemenin göndericisi ile alıcısı arasında bile bir ilişki kurulmasının zor hatta imkansız olması gerekir.

Bitcoin kriptosisteminin işlemlerinden düğümlerine, madencilerinden ağ yapısına ve hatta cüzdanlarına ve bitcoin sağlayıcılarına kadar çok geniş çaptaki farklı öğelerine analiz ve saldırılar yapılmıştır, [53]. Bu durum özellikle Bitcoin'de dahil tüm kriptoparalar için ciddi prestij ve dolayısıyla müşteri ve kullanıcı kaybı anlamına gelir. Bu nedenle zamanla çeşitli araştırmalarda aşağıdaki gibi gizliliği ve anonimliği iyileştirip üst seviyelere taşıyan çözümler önerilmiştir.



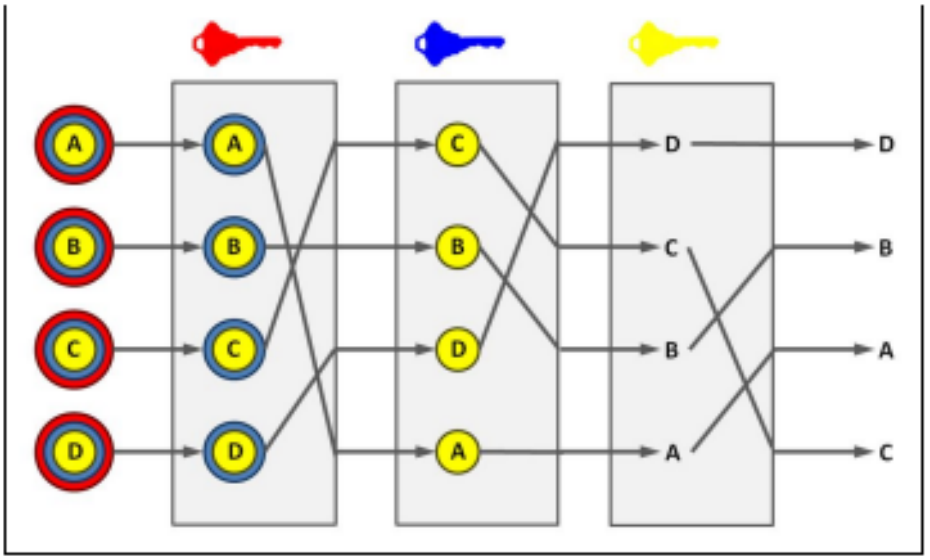
Şekil 2.14: Coinjoin Şeması [53]

2.3.1 Mixin Protokolü ve CoinJoin

Mixin protokolü karıştırıcı (mixer) denilen güvenilir bir otorite kullanarak coinlerin sahipliğini değiştirerek hangi coinin kime ait olduğunun takip edilememesini sağlar. Böylece bitcoin işlemlerinin anonimliği artmış olur. Karıştırıcılar yapılan işlemleri daha küçük parçalara ayırır ve rastgele aynı işlemde farklı kullanıcıların işlemleriyle bu yapılan işlemleri karıştırır. Böylece hangi işlemin kime gittiğini anlamak zorlaşır. Eşler arasında karıştırma işlemi yapan en çok bilinen mixin protokollerinden birisi de CoinJoin'dir. Şekil 2.14'teki resimde de görüldüğü gibi Coinjoin kullanılarak yapılan farklı işlemler tek bir CoinJoin işleminde toplanır. Bu sayede gönderici ve alıcı arasındaki bağın kopması amaçlanır. Ancak zaman içerisinde yapılan çalışmalar Mixin protokolünün yetersiz olduğunu göstermiştir, [61].

2.3.2 Karıştırma Ağları (Mix Nets)

Mixin protokolü güvenilir bir karıştırıcıya ihtiyaç duymasından dolayı izlenibilirlik ve güvenilirlik problemleri yaşar. Karıştırma ağları herhangi bir karıştırıcıya ihtiyaç duymaz, oluşturdukları "karıştırmaları (mix)" birbirlerine zincirleyerek çalışırlar. Bu karıştırmalar göndericiler kümesinden mesajları alır ve karıştırıp bir sonraki karıştırma düğümüne rastgele bir sırada yollarlar. Bu karıştırma düğümlerinde yapılan işlemlerin sonunda yeterince karıştırma işlemi yapıldığı düşünüldüğünde mesaj alıcıya ulaştırılır. Mesajlar Şekil 2.15'teki resimde de görüldüğü gibi her bir düğüm için ayrı olan açık anahtarlı kriptografik bir katmana sahiptirler. İlgili mesaj her yeni karıştırma düğümüne geldiğinde ilgili düğümün şifreli katmanlarından birisi deşifre edilerek mesajın nereye iletileceğine karar verir. Böylece herbir düğüm sadece kendisinden önceki düğümle kendisinden sonraki



Şekil 2.15: Mixnet Mekanizması Şeması [61]

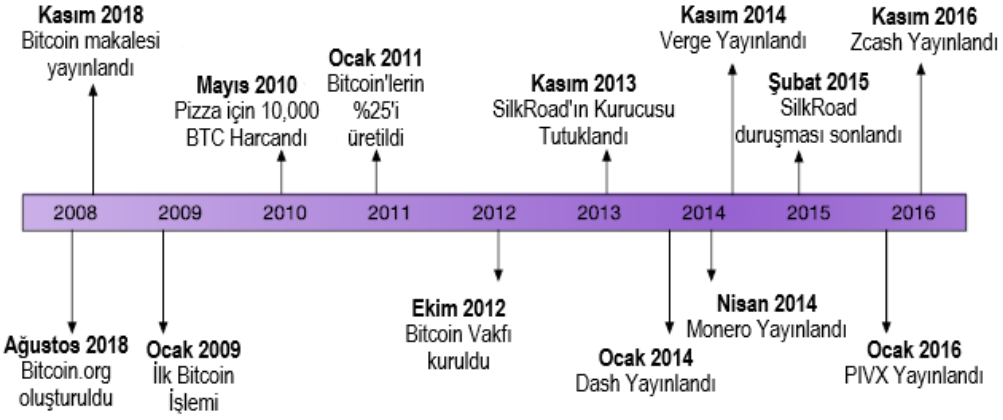
düğümü bilir; bu da kötü niyetli bireysel düğümlere karşı önemli bir güvenlik ve koruma sağlar, [61].

Karıştırma ağlarının en büyük sıkıntısı anonimlik kümesinini boyutunun çok büyük olmasıdır. Anonimliğin ne derece sağlanabildiği anonimlik kümesinin ne kadar iyi örneklenip ne kadar büyük olduğuyla doğru orantılıdır. Boyutun çok büyük olması sebep gösterilip bir yahut birkaç karıştırıcı kullanmaksa normal karıştırıcı servislerinin başka bir benzeri olup aynı zayıflıkları paylaşayacaklardır. Bu nedenle karıştırma ağlarının kullanılması da Mixcoin protokolünde de olduğu gibi etkili değildir, [61].

2.3.3 Tor (The Onion Router)

Tor, Tor ağındaki yönlendiriciler üzerinden trafiği proxy olarak geçirerek anonimlik sağlayan devre tabanlı bir iletişim hizmetidir. Tor ağı yaklaşık 7000 gönüllü ile çalışan ve anahtarlayıcı (relay) da denilen onion yönlendiricilerinden (onion routers / the ORs) oluşan dağıtık bir bindirme (overlay) ağıdır. Bir kullanıcı Tor istemcisini çalıştırdığı zaman Tor istemcisi giriş (entry), orta (middle) ve çıkış (exit) denilen üç anahtarlama seçerek Tor ağında gezinmesini sağlayacak bir Tor devresi oluşturur ve her bir anahtarlama için oturum anahtarı tesis eder. Örnek olarak Ahmet'in Mehmet'e Tor istemcisini kullanarak bağlanmak istediği durumda Ahmet kendi yerel makinesiden Tor ismtecisini çalıştırdığı takdirde istemci şu üç sekmeli devreyi oluşturur, [52]:

Ahmet ↔ Giriş anahtarlaması ↔ Orta anahtarlaması ↔ Çıkış anahtarlaması



Şekil 2.16: Bitcoin ve Anonim Kriptoparaların Kısa Tarihçesi [47]

Daha sonra Tor istemcisi Mehmet'e anahtarlamalarda tesis edilmiş olan oturum anahtarlarıyla beraber veriyi üç anahtarlamanın şifrelemesi kullanarak sarmalar ve gönderir. Devredeki her bir anahtarlama kendisine karşılık gelen şifrelemeyi deşifre eder ve son olarak veri Mehmet'e iletilir. Devredeki herbir anahtarlama sadece kendisinden öncekinin ve sonrakinin IP adresini bilir. Mesela giriş anahtarlaması Ahmet'in IP adresini bilse bile gönderdiği veriyi bilmez. Çıkış anahtarlaması veriyi bilse bile kimin gönderdiği bilmez. Böylece işin sonunda hiçbir anahtarlama Ahmet ile Mehmet'in arasındaki ilişkiyi bilemez, [52].

Yukarıda bahsedilen Mixin ve Mixnet konularında olduğu gibi Tor ağı kullanarak bitcoin işlemlerinin yapılmasının düşünüldüğü kadar anonimlik sağlamayacağı ile alakalı çalışmalar da yapılmıştır, [52], [38], [27]. Mesela [52] araştırma makalesinde Tor oturumlarının birbirleriyle ilişkilendirilmesinin nasıl anonimliğin ihlali için bir saldırı olacağı detaylı bir şekilde açıklanmıştır.

2.4 Anonim Kriptoparalar

Kısım 2.3'te bahsedilen örnekler haricinde Bitcoin kriptoparasında anonimliği sağlamak için başka öneriler, çalışmalar ve tavsiyeler de sunulmuştur. Ne var ki Bitcoin'in canlı bir sistem olması ve sürekli olarak yeni işlemlerin ve blokların ağa eklenmesi gibi çeşitli sebeplerden ötürü Bitcoin'de çok ciddi değişiklerin yapılması oldukça zor görünmektedir. Bundan ötürü Bitcoin için anonimliğe dayalı şüphe ve güvensizlikler devam etmektedir. Bu nedenle zaman içinde Şekil 2.16'da da görüldüğü gibi zamanla anonimliğe daha çok odaklanan kriptoparlar farklı geliştiriciler ve girişimciler tarafından yayınlanmıştır, [47].

Anonim kriptopara, kendi kullanıcılarına anonimlik sağlamak için yüksek seviyede kriptografik nitelik sağlaması amacıyla tasarlanmış kriptoparalardır. Anonimliği sağlayabilmesi için anonim kriptopaların aşağıdaki üç özelliği sağlaması beklenir, [47], [18]:

1. **Gizlilik (Privacy)**: Yapılan işlemlerdeki gönderen, alan ve işlemin miktarı yetkisiz hiçbir üçüncü şahıs tarafından gözlemlenebilir olmadığı garanti edilir.
2. **Takip Edilememezlik (Untraceability)**: Gönderilen yahut alınan coinler, işlem geçmişiyle herhangi bir ilişki kurulamadığı ve bu coinlerin işlem geçmişinde takip edilemediği temin edilir.
3. **Birbiriyle Değiştirilebilirlik (Fungibility)**: Kriptoparadaki tüm coinlerin birbirlerinden hiçbir şekilde ayırt edilemez olduğu, böylece karşılıklı olarak değiştirilebileceği; yani daha önce farklı birçok işlemde kullanılan bir coin, geçmişte yapılmış olan işlemlerin neler olduğuna bakılmaksızın tüm işlemlerde kullanılabileceği garanti edilir.

Yapılan araştırmalar sonucunda Zcash, Dash ve Monero gibi çeşitli anonim kriptoparaların kullanıcılar tarafından istenilen anonimliği sağlayabileceği düşünülmektedir. Bu tez çalışmasında bahsedilen bu anonim kriptoparan anonimlik ve gizlilik analizi yapılmaya çalışılacaktır. Bu anonim kriptoparalar hakkında detaylı bilgi aşağıdaki alt kısımlarda açıklanmıştır.

2.4.1 Zcash

Merkezi Olmayan Anonim Ödeme planı olan (Decentralized Anonymous Payment scheme) **Zerocash** [41] protokolü kullanılarak geliştirilmiş olan Zcash, Bitcoinin üzerine geliştirilmiş bir kriptoparadır (Bitcoin's fork). Bunun yanında Bitcoin'den farklı olarak, karmaşık bir sıfır bilgi ispat şeması (zero-knowledge proving scheme) olan zk-SNAKRs kullanılarak matematiksel olarak daha fazla gizlilik ve anonimliğin sağlanması amaçlanır. **zk-SNAKRs** korumalı işlemlerdeki adres ve işlemin miktarını hiçbir şekilde göstermeden işlemin geçerliliğini ve coinlerin birden fazla kez harcanmadığını doğrulayarak ispat etmek için kullanılan kriptografik bir ispattır, [10].

Blokzincirin kendisi harcanmamış işlem çıktısı (unspent transaction output (UTXO)) tabanlıdır ve "işin ispatı" fonksiyonu olarak "Equinhash"i kullanır. Equinhash, oldukça verimli doğrulamayla birlikte bellek odaklı (memory-oriented) bir işin ispatı maden algoritmasıdır. Zcash anonim kriptoparası Bitcoin gibi şeffaf işlemlerin (transparent transactions) yanında aynıca korumalı bir havuzu (shielded pool) kullanarak coin transferi

yapılmasını sağlayan korumalı işlemleri (shielded transactions) de destekler. Coin sahibi olan kullanıcı dilerse şeffaf, dilerse korumalı işlem gerçekleştirebilir, [45], [10].

Zcash işlemleri herkese açıktır, ilgili bloklar kronolojik bir sıralamada blokzincirde tutulur ve tüm Zcash kullanıcılarınyla yine açık bir şekilde paylaşılır. Bitcoin'de olduğu gibi Zcash'te de blokzincir, işlemlerin devamlılık ve kalıcılığını sağlayıp çoklu coin harcamayı engellemek için kullanılır. Zcash'te kullanılan para birimi **ZEC**'tir. En küçük para birimineyse **Zatoshi** adı verilir ve 1 ZEC 10^8 Zatoshiye eşittir. Bitcoin'de olduğu gibi ZEC göndermek için adresler kullanılır. Bitcoin'den farklı olarak ise açık adreslerin yanında aynı zamanda zk-SNARKs kullanılarak gönderilen coin miktarıyla beraber şifrelenmiş gizli adresler de kullanılır, [10].

Bitcoin'de 10 dakikada bir olan blok üretme (yani bloğun madenciler tarafından oluşturulup konsensus tarafından kabul edilmesi) süresi Zcash'te 2.5 dakikadır. Başarılı bir şekilde üretilen blok sonrası bloğu üreten madenciye blok ödülü tahsis edilir. Zcash'de blok ödülünden hem madenciye hem de kurucuya (founder) pay verilir. Bloğu bulan madenciye (yahut madenci havuzuna) blok ödülünün %80'i, kurucuya da %20'si verilir. İlk başlarda blok ödülü 12.5 ZEC'ti; bunun 10 ZEC'i madenciye giderken 2.5 ZEC'i kurucuya giderdi. 850,000. blok sonrası maden ödülü 6.25 ZEC'e düşürülmüştür; bunun 5 ZEC'i madenciye, 1.25 ZEC'i kurucuya gitmektedir. Her 840,000 blok sonrası maden ödülü yarıya düşecektir, [10].

Zcash'te iki farklı havuz (pool) bulunmaktadır. Bunlarda ilki şeffaf işlemlerin yapıldığı ve herkese açık olarak görünen işlemlerde kullanılan coinlerin tutulduğu şeffaf havuzdur (transparent pool). Diğer havuz ise korumalı işlemlerde kullanılmış olan coinlerin tutulduğu korumalı havuzdur (shielded pool), [10]. Korumalı havuza direk olarak kimin ne kadar coin koyduğu, yani hangi gizli adresin ne kadar harcanmamış ZEC çıktısı olduğu doğrudan yapılan korumalı işlemler kullanıldığı takdirde bilmek mümkün değildir. Ancak şimdiye kadar üretilmiş olan tüm coinlerin toplamıyla birlikte mevcut durumda açık olarak defterde görülebilen coinlerin toplamının farkı alındığında korumalı havuzda toplamda ne kadar coinin gizlendiği bilgisine ulaşılacaktır.

Zcash adreslerinde açık adreslere (transparent-address) t harfi ile başladıkları için kısaca t-adres, gizli adreslere (private-address) de z harfi ile başladıkları için kısaca z-adres denir. Zcash'te z-adreslerin geçtiği işlemlere korumalı işlemler ya da **EkleBöl (JoinSplit)** işlemleri (kısaca EB-işlemleri (JS-transactions)) adı verilir. Bir EB işlemi girdi veya çıktı olarak sadece iki adrese kadar destekleyebilir. Yani girdisi yahut çıktısı EkleBöl olan bir işlemde sadece iki tane gizli girdi ya da gizli çıktı adresi bulunabilir.

Toplamda 4 farklı EB işlemi bulunmaktadır, [45], [11]:

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 yahut miktarlar ve alınan miktar yahut miktarlar tamamen gizlidir. Sadece böyle bir işlemin gerçekleştiğine dair bir işin ispatı vardır. İşlemde gözlemlenebilecek tek açık veri işlem bedelidir. Zcash kriptoparasının gizliliğinin sağlandığı temel EB-işlemidir. Kriptografik olarak zk-SNARKs algoritması üzerinde başarılı bir saldırı yapılmadıkça buradaki verileri bilmek mümkün değildir. Burada yapılan işlemler korumalı havuzdan korumalı havuza yapılan bir işlem olmasından mütevellit bu işlemlere korumalı işlemler (shielded transactions) de denilir.

2. **z'den t'ye işlemler (z-to-t transactions):** Girdi olarak sadece z-adres(ler)i varken çıktı olarak ise bir veya daha fazla t-adresi bulunur. Korumalı havuzdan herkese açık şeffaf havuza para aktarımı olduğundan dolayı bu işlemlere korumanın kaldırılması işlemleri (deshielding transactions) de denilir. Bu işlemlerde girdi miktarı 0 ZEC iken çıktı tamamıyla herkese açık 0'dan büyük bir değerdir. Toplam çıktıyla beraber işlem bedelinin toplamı korumalı havuzdan çıkan işlemin girdisini verir. Korumalı havuza giren Zcash miktarını veren denklem şu şekilde olacaktır, korumalı girdi değeri = çıktı adresleri değerleri toplamı + işlem bedeli.

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 hiç kimseye açık olmayan korumalı havuza coin 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 herkese açıkken çıktı gizlidir; yani blokzincirde 0 ZEC olarak görülür. Girdilerin (daha önce de bahsedildiği gibi açık işlemlerde birden fazla girdi ve çıktı olabilir, sınırlama yoktur, onlarca hatta daha fazla girdi yahut çıktısı olan işlemler bulunmaktadır) toplamından işlem bedeli çıkartıldığı zaman çıkan sonuç korumalı havuza giden coin miktarını verecektir. Korumalı havuzdan çıkan Zcash miktarını veren denklem şu şekilde olacaktır, korumalı girdi değeri = girdi adresleri değerleri toplamı - işlem bedeli.

4. **tz'den tz'ye işlemler (tz-to-tz transactions):** Hem işlem girdisinde hem de işlem çıktısında hem t-adres ve hem de z-adres bulunur. Zcash bünyesinde en az karşılaşılan EB-işlemi tipidir. Bu işlemlerin tümü için bir genelleme yapmak zordur. Girdilerin toplamıyla çıktıların toplamıyla beraber işlem bedelinin toplamının farklı alınır. Farkın pozitif çıkması durumunda korumanın sağlanması işlemi, farkın negatif çıkması durumunda korumanın kaldırılması işlemi yapılmış denilebilir. Farkın 0 çıkmasıysa bu işlemi bir çeşit korumalı işlem konumuna sokar. Korumalı havuza giren yahut korumalı havuzdan çıkan Zcash miktarını veren denklem şu şekilde

olacaktır, korumalı girdi değeri = girdi adresleri değerleri toplamı - çıktı adresleri değerleri toplamı - işlem bedeli.

2.4.2 Dash

18 Ocak 2014 yılında Bitcoin kriptoparasındaki anonim eksikliğini farkeden Evan Duffield isimli bir uygulama geliştiricisi ilk olarak Xcoin, daha sonra da DarkCoin ismini verdiği ve rakiplerinin ilki olan anonim odaklı bir kriptopara geliştirmiştir. Nihayet 25 Mart 2015 yılında ilgili anonim kriptopara Digital Cash'in kısatlması olan Dash ismini almıştır. Nisan 2018'de Dash kriptoparası 4.3 milyar $ piyasa değerine ulaşmış ve en çok kullanılan 12 kriptoparadan birisi olmuştur. Der Speigel dergisine göre Şubat 2019'da Dash, Venezuela'da en çok kullanılan kriptopara olmuştur. Zcash ve diğer anonimliği temel alan kriptoparalara göre karşılaştırma yapıldığı zaman bu durum gerçekten de ciddi bir başarıdır, [5].

Dash, ödeme endüstrisine odaklanan açık kaynaklı ve eşler arası (P2P) bir kripto para birimidir. Dash, taşınabilir, ucuz, bölünebilir ve hızlı bir "para biçimi" sunar. Hem İnternet üzerinden çevrimiçi bir şekilde hem de şahsi olarak cüzi bir işlem bedeli karşılığında güvenli bir şekilde harcanabilir. Bitcoin'de bulunan özelliklerin yanında hızlı coin aktarımı (HızlıGönderim) ve gizli işlemler (ÖzelGönderim) hizmetlerini de sunar. Ayrıca Dash kendi kendine yeten ve kendi kendini yöneten bir kriptografik sistemdir, [3].

İlk Dash bloğu 18 Ocak 2014'de üretilmiştir. X11 özetleme algoritması kullanılır, CPU/GPU/ASIC madenciliği vardır. Ortalama blok üretme süresi 2.6 dakikadır. Blok ödülü her yıl %7.14 oranında azalır. 17.74 milyon ile 18.92 milyon arasında toplam coin tedarik edilebilir. ChainLocks kullanarak blockchain yeniden yapılanma olaylarına (genellikle % 51 saldırıları denir) karşı koruma sağlanır. Blokzincir ile Merkezisizleştirilmiş Yönetim, AnaUç sahiplerinin Dash'i etkileyen bütçe teklifleri ve kararları üzerinde oy kullanmalarına izin verir. Yani AnaUç sahiplerinin Dash üzerinde önemli bir seviyede söz söyleme ve yönetme hakkı bulunur, [4].

Bitcoin'de blok ödülünün tamamı bloğu üreten madenciye giderken Dash kriptoparasında Zcash'te olduğu gibi ödülün bir kısmı kuruculara gider. Zcash'ten farklı olan kısmı ise ödül sadece kurucu ile madenci arasında değil aynı zamanda AnaUç'a da paylaştırılır. Ödülün %45'i bloğu üreten madenciye, %45'i AnaUç'a ve %10'u da Dash kurucularına gider, [4].

Dash için normal işlemin işlem bedeli kb başına 0.00001 DASH'tır. HızlıGönderim için kb başına 0.001 DASH ve ÖzelGönderim için ortalama yapılacak her 10 karıştırma başına 0.001 DASH'tır, [4].

Dash kriptoparası için önemli özellikler ve hususlar aşağıdaki gibidir, [4]:

2.4.2.1 AnaUç (MasterNode)

Birçok kriptoparada olduğu gibi işin ispatının ödülü olan "Dash bloğunun üretilmesi" ödülü Dash kriptoparasında da madencilere temin edilir. Bunun yanında Dash kullanıcıları AnaUç adı verilen bir çeşit özel sunucuları çalıştırıp Dash anınim kriptoparasını yönetir ve Dash'ın devamlılığını sağlamaya yardım ettikleri için de bu blok ödülünden bir pay kazanırlar. AnaUçlar, ÖzelGönderim ve HızlıGönderim ile beraber yönetim ve hazine sistemlerine güç vermek için kullanılır. Bunun anlamı AnaUçlar kripto-sistemdeki ÖzelGönderim ve HızlıGönderim denilen iki tane çok önemli işlemden sorumludur. Ayrıca yapılan işlemlerin doğruluğunun kontrolü, güvenliğinin sağlanması gibi çeşitli farklı görevleri de vardır. AnaUçlar bu nedenle ciddi bir maliyet gerektirir; bir kullanıcının AnaUç olabilmesi için 1000 Dash'e sahip olması gerekir ki bu da 5 Mayıs 2020 10:00 tarihinde [2] Dash'ten TL'ye çevirme işlemiyle hesaplandığında 562,444.71 TL'ye karşılık gelir. Yaptıkları bu yatırıma karşılık AnaUçlar herbir üretilen bloktan üretilen ödülün yaklaşık %45'ini alır, [4].

AnaUçlar aşağıda listelenmiş olan hizmetleri sağlarlar, [4]:

- **ÖzelGönderim:** Dash işlemlerinin CoinJoin mantığı geliştirilerek gizli bir şekilde yapılmasını sağlar.
- **HızlıGönderim:** İşlemlerin neredeyse "anında" gönderilmesini sağlar.
- **ChainLocks:** Blokları imzalayarak %51 madenci saldırılarına karşı blokzinciri korur.
- Yönetim ve Hazine (Governance and Treasury), Dash'teki paydaşların projenin yönünü ve nereye gittiğini belirlemesine izin verir ve blok ödülünün % 10'unu proje ve ekosistemin gelişimine ayırır.
- Dash Gelişimi (Evolution), Dash kriptoparasının PayPal kadar kullanımının kolay olmasına olanak sağlar.

2.4.2.2 ÖzelGönderim (PrivateSend)

ÖzelGönderim kullanımı ile gönderilen işlemlerin takip edilemezliği sağlanarak anonimlilik ve gizlilik sağlanır. Cüzdanlarda bulunan Dashler ayrı birer coin olarak da düşünülebilecek

[2] https://tr.coinmill.com/DASH_TRY.html#DASH=1000 sayfasından yapılmıştır.

farklı girdilerin birleşimidir. ÖzelGönderim, kullanmış olduğu karıştırma yöntemleriyle kullanıcıların sahip olduğu Dashleri en az üç farklı kullanıcı ile beraber karıştırır. Ancak karıştırılan Dashler aslında cüzdandan asla başka bir yere gitmez. Kullanıcılar sahip oldukları Dashlerin kontrolüne daima sahiptirler, [4].

ÖzelGönderim işlemi aşağıdaki gibi çalışır, [4]:

1. ÖzelGönderim ilk olarak gönderilmek istenen işlemin girdilerini "10" sayısının katsayılarına böler. Bu katsayılar 0.001 Dash, 1 Dash yahut 10 Dash gibi katsayılardır. Bir nebze gerçek hayattaki paraların sadece 10 sayısının katsayılarından oluşması gibi düşünülebilir.

2. Daha sonra ilgili kullanıcının Dash cüzdanı ağda özel olarak ayarlanmış olan yazılım düğümleri olan AnaUçlara karıştırmak istediği 10'un katsayısı olan değerler için istek yollar. Bu AnaUçlar kullanıcının ne kadarlık bir değeri karıştırma işlemine sokmak istediğiyle alakalı olarak bilgilendirilir. Bilgilendirme işlemi sırasında hiçbir teşhis etmeye yarayabilecek bir bilgi paylaşılmadığından AnaUç isteği yollayanın kim olduğunu bilmez.

3. Diğer iki farklı kullanıcı da (toplamda üç kullanıcı) aynı 10 sayısının katsayısı için istek yolladığı zaman karıştırma oturumu başlatılır. Karıştırma işlemi sonrası AnaUç üç kullanıcının her birinin cüzdanına karıştırılmış katsayı değerlerini kendilerine geri ödemelerini söyler. Daha sonra ilgili cüzdanlar değiştirme adresi (change address) adı verilen farklı yeni bir adresi kullanarak karıştırılan Dash'i kendisine öder.

4. İlgili cüzdanlar bu işlemi herbir katsayı değerleri için birkaç defa tekrarlaması gerekmektedir. Bu sürecin tamamlanmış her bir döngüsüne sefer (round) adı verilir. Kullanıcı 1 ile 16 karıştırma seferi arasında seçim yapar. Yapılan herbir sefer coinlerin nereden geldiğinin anlaşılmasını daha da zorlaştırır.

Yapılan bu karıştırma işlemleri tamamıyla arka planda gerçekleştirilir. Kullanıcının herhangi bir şekilde fazladan bir işlem yapmasına ihtiyaç yoktur. ÖzelGönderim işleminde girdideki tüm coinler harcanır; bu nedenle kullanıcı karıştırma sürecine girmeyen paraların işlem bedeline aktarılmasını engellemek için o paraları kendisine yahut başka bir yere geri aktarması gerekir, [4].

Bir kullanıcı cüzdanında toplamda 1000 tane değiştirme adresi bulunmaktadır. Herbir karıştırma işlemi olduğunda bu adreslerden birisi kullanılır. 1000 adresin tamamı kullanıldığında cüzdanın daha fazlasını üretmesi gerekir. Bu işlem de sadece otomatik geridönüşler (automatic backups) etkinleştirilmişse yapılabilir. Geridönüşlerin pasifleştirilmesi ÖzelGönderim işlemlerinin de pasifleştirilmesine neden olur, [4].

2.4.2.3 HızlıGönderim

Yapılan işlemlerin geri dönüşünün mümkün olmadığından ve fazladan değer harcanmadığından emin olunması için yeterince bloğun oluşturulmasını beklemek normalde 15 dakikadan 1 saate kadar sürmektedir. Dash, ikinci katman AnaUç ağı sayesinde bu durumdan etkilenmez. AnaUçlar, gönderilen bir işlemin geçerli olup olmadığını kontrol etmek için düzenli olarak oy çokluğu / konsensus (quorums/consensus) oluşturur. İşlem geçerliyse AnaUçlar bu işlemi kilitleyip bu bilgiyi ağda paylaşırlar. Böylece işlemin bir sonraki üretilen bloğa ekleneceğinin ve onaylama süresi boyunca bu işlemle alakalı ikinci bir harcama yapılmayacağının teminatını verirler, [4].

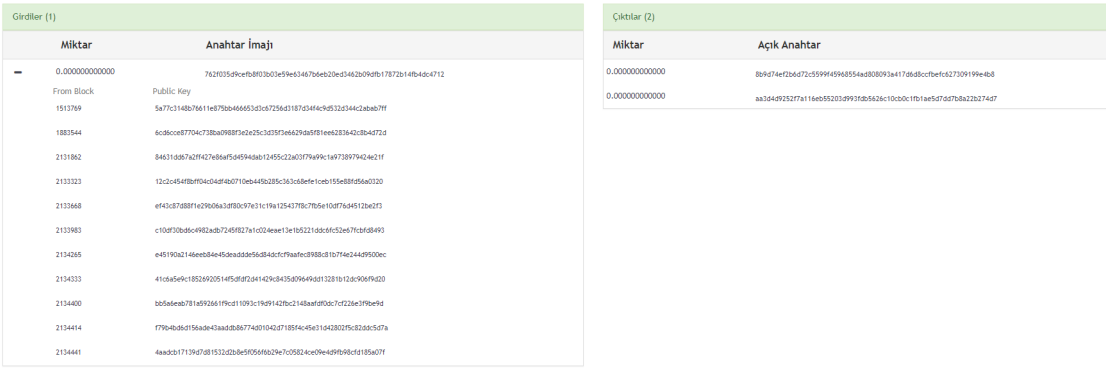
HızlıGönderim sistemi de Dash kriptoparasının kredi kartı gibi anında ödeme sistemleriyle hiçbir merkezi otoriteye bağlı kalmadan neredeyse rekabet etmesini sağlayan sistemdir. Bu sistemle cüzi bir bedel karşılığında birkaç saniyede işlem yapmak mümkün olmaktadır.

2.4.3 Monero

18 Nisan 2014'te yayınlanan Monero, Zcash ve Dash gibi mahremiyet ve işlem gizliliğine odaklanan bir anonim kriptoparadır. Monero gizlenmiş bir açık deftertir (obfuscated public ledger); yani herkes işlem gönderip alabilir ancak hiçbir kimse bu işlemlerdeki adres ve gönderilen miktarları göremez. Diğer kriptoparalar gibi yeni madeni paralar çıkarmak ve madencileri "ağı korumak ve işlemleri doğrulamak" için teşvik etmek amacıyla yine işin ispatı mekanizmasını kullanır, [8], [9].

Zcash ve Dash kriptoparaları Bitcoin kodu kullanılarak üretilmiş ve yayınlanmış anonim kriptoparalardır. Bu nedenle yapılan şeffaf/açık işlemler Bitcoin'deki işlemlerin bir benzeridir. Ancak Monero Bitcoin'den türetilmiş bir kriptopara değildir, Bytecoin isimli kriptoparanın çatallanmasıyla oluşturulmuştur. Ayrıca CrptoNote protokolü kullanılarak üretilmiş CryptoNight işin ispatı algoritması tabanlıdır. Özetle açıklamak gerekirse CrpytoNote'da kullanılan halka imzalarıysa coin harcamak isteyen kullanıcının girdisini başkalarının girdisiyle karıştırır. Bu sayede daha sonra yapılacak işlemlerle ilgili mevcut işlemin birbirleriyle ilişkilendirilebilmesini zorlaştırır. Yapılan bu karıştırma işlemi CoinJoin tabanlı Dash'ten farklı bir karıştırmadır, [8].

Para birimi **XMR** olan Monero'nun 27 Mayıs 2020 tarihi itibariyle toplam miktarı 17,575,954 XMR kadardır. Ortalama 2 dakikada bir yeni bir blok üretilir, blok üretim hızının çeşitli faktörlere göre değişmesi öngörülmektedir. Daha önceki adı BitMonero'dur. İşin ispatı için 9 Mart 2019'den itibaren **CryptoNight v3.0**, CrytoNight'a alternatif olarak 30 Kasım 2019'dan itibaren de **RandomX v0** kullanılmaktadır, [8].



Şekil 2.17: *dfd89aa42cbe00d6862be21a7cde582fc5606f23f5297adca3c7d4a6f54f3410* koduna sahip 2134748. nolu bloktaki işlem

Blok ödülü ilk blokta 17.592169267200 XMR olarak belirlenmiştir ve her blokla bu ödül düşmektedir. 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. Toplam miktarı 18.132 milyon XMR ile beraber her iki dakikada bir 0.6 XMR kadardır. Bunun anlamı teknik olarak Monero sonsuz miktarda üretilebilir, ancak pratikte kayıp coinler hesaba katılırsa daha az olacaktır, [8].

Monero anonim kriptoparasında göndericinin, alıcının ve gönderilen miktarın gizliliği sağlanır. Gönderici gizliliği halka imzasıyla sağlanır, halkada 10 tanesi sahte/tuzak (decoy) olan 11 adresin imzası alınır. Şekil 2.17'de de görüldüğü gibi toplamda 11 gönderici varmış gibi görünür; ancak sadece bir tanesi gerçek göndericidir. Coini alan adresler yani çıktı adresleri gizli (stealth) adreslerdir. Ayrıca gönderilen miktar blok üretme ödülünün olduğu işlemler hariç diğer tüm işlemlerde daima halka imzasıyla beraber uygulunanan kriptografik gizleme yöntemleri sayesinde 0 XMR olarak görünür, işlemle alakası olmayan üçüncü şahıslar ne kadar coinin gittiğini bilemezler, [8].

2.4.3.1 Halka İmzalar (Ring Signatures)

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 imzaların en önemli özelliklerinden birisi de imzayı atan asıl kişinin grupta bulunan imzacılardan hangisinin olduğunun ayırt edilememesidir, [7].

Monero, halka imzalarını üçgen bir dağıtım yöntemi kullanılarak blok zincirden alınan hesap anahtarlarıyla beraber çıktılar olarak da bilinen ortak anahtarlar kümesini kullanarak oluşturur. Daha öncesinden çıktı olarak kullanılmış olan anahtarlar daha sonra zaman içerisinde "muhtemel imzalayıcı katılımcılar" olarak birçok kez kullanılabilirler. Yapılan işlemin halka imzasında kullanılacak olan imzalayıcıların tamamı eşit ve geçerlidir. İmzalama algoritması geçerli olduğu sürece asıl imzayı atanın imzalayıcı grubundaki hangi imzacı olduğunu anlamak mümkün değildir. Böylece halka imzaları işlem çıktılarının geriye doğru takip edilememesini sağlar. Ayrıca işlemlerdeki tüm çıktılar makul bir şekilde reddedilebildiğinden (plausible deniability) coinlerin birbirleriyle değiştirilebilesi ile alakalı bir sorun yaşanmaz. Misal olarak ağı izleyen herhangi bir üçüncü kişi muhtemel imzalayıcı çıktılar birden fazla işlemde harcansa dahi sahte/tuzak imzalayıcı olarak halka imzalama işleminde kullanıldığı için çıktının o işlemde gerçekten de harcanıp harcanmadığını anlayamaz, [7].

Şöyle bir örnekle daha detaylı açıklanacak olursa X_1, X_2 ve X_3 şeklinde üç farklı zamanda ve dolayısıyla blokta gerçekleştirilmiş Monero işlemi olduğu ve herbir işlemin girdilerine bakıldığından halka imzalayıcılarından bir tane "harcanmamış çıktı" değerlerinin ortak olduğu varsayılsın. Bu harcanmamış çıktı değerinin gerçekte hangi işlemin esas girdisi olduğunu tespit etmek; X_1, X_2 yahut X_3 işlemlerinden hangisinde gerçekten de harcandığını tespit etmek mümkün değildir. Hatta bu harcanmamış çıktı değerinin artık harcanıp harcanmadığı bile çıktı adresinin sahibi haricinde bilmek imkansızdır. Bu harcanmamış çıktı adresi daha sonraki bir X_4 işleminin asıl girdi adresi olabilir, üçüncü kişiler tarafından bu bilginin bilinmesi yine mümkün olmaz.

Şekil 2.17'de de görüldüğü gibi bir tane girdi olmasına rağmen toplamda 11 tane imzalayıcı girdisi bulunmaktadır. Bunlardan sadece bir tanesi gerçek imzalayıcıdır. Ayrıca 2 tane çıktı bulunmaktadır. Bunlar alıcının doğrudan kendi adresinden ziyade gizli adreslerdir; hangi alıcıya gittiğini bilmek bu sayede mümkün olmamaktadır. [3]

2.4.3.2 Açık Adresler

Diğer tüm kriptoparalarda olduğu gibi, Monero'da da adresler işlemlerin yapıldığı anahtarlardır. Monore'da tüm adresler açık adrestir. Başka kriptoparalarda şahsa münhasır olan açık adresi paylaşmak anonimliği kişi için yok ederken Monero'da açık adresi paylaşmak hiçbir şekilde anonimlik ve mahremiyete halel ve zarar getirmez. Çünkü Monero işlemleri açık adreslerden türetilmiş "gizli adreslere" yapılır, [6].

Monero'nın bünyesinde toplamda üç farklı adres tipi bulunmaktadır, [6]:

[3] **https://moneroblocks.info/tx/dfd89aa42cbe00d6862be21a7cde582fc5606f23f5297adca3c7d4a6f54f3410** bağlantı adresi kullanılarak ilgili işlemin detayına ulaşılabilir.

1. **Standart Adres (Standard Address):** Ham adres (raw address) adı da verilir. Daha öncesinden genellikle standart adresler tercih edilmekteydi. Bu nedenle en çok karşılaşılacak adres tipidir. Ne var ki, standart adresler yerine daha çok aşağıda anlatılacak olan alt-adreslerin kullanılması tavsiye edilir. Daha güncel sürümlerde standart adresler, alt-adresler ve tümleşik adreslerin türetilmesinde kullanılır. Diğer adres tipleri desteklenmediğinden madencilikte üretilen blokların blok ödülünü aldığı işlemlerle beraber madenci havuzlarının çoklu adreslere blok üretme ödülünün madenci payını ödeme yaptığı ödül paylaştırma işlemlerinde çıktı adresi olarak kullanılırlar. Açık harcama anahtarı ve açık görüntüleme anahtarı olmak üzere iki farklı açık anahtarı vardır.

2. **Alt-adres (Subaddress):** Standart adres kullanılarak türetilir. Monero'da coin transferinde çıktı olarak kullanılması tavsiye edilen adres tipidir. Herbir yapılacak işlem için alt-adres türetilir. Tek bir işlemde kullanıldığından kullanıcının yaptığı tüm diğer işlemler için gizlilik ve takip edilememezlik sağlar. Bir sonraki maddede anlatılacak olan tümleşik adresler de buna benzer bir görev için kullanılabilir. Bu nedenle alt-adreslerin daha çok göndericinin alıcıya ait tüm diğer işlemlerinin (coin transferlerinin yahut çeşitli ödemelerinin) ne olduğunu anlamasını engellemek ve fonları (funds) çeşitli hesaplarda gruplayabilmek için tercih edilmesi önerilir.

3. **Tümleşik Adres (Integrated Address):** Tümleşik adresler "Çevrimiçi mağazalar ve borsalarda" yapılan otomatik işlemler gibi işlemlerde Monero ödemesini kabul etmek için kullanılması idealdir. Tümleşik adresler bünyelerine birer ödeme ID'si yerleştirirler. Böylece "neyin ödendiği" daha iyi anlaşılmış olunur. Bu ID'ler Monore'ya münhasır teknik ödeme ID'leridir, herhangi bir işlemin işlem anahtarı (businesskey) yahut fatura numarası (invoice number) değildir. TÜmleşik adrese yerleştirilen ödeme ID'si sadece gönderici ve alıcının bildiği tek-seferlik bir rastgele anahtarla şifrelendiğinden dolayı yapılan işlemlerde görünmez. Sadece işlemin alıcısı ödeme ID'si ile işlem arasında eşleştirme yapabilir.

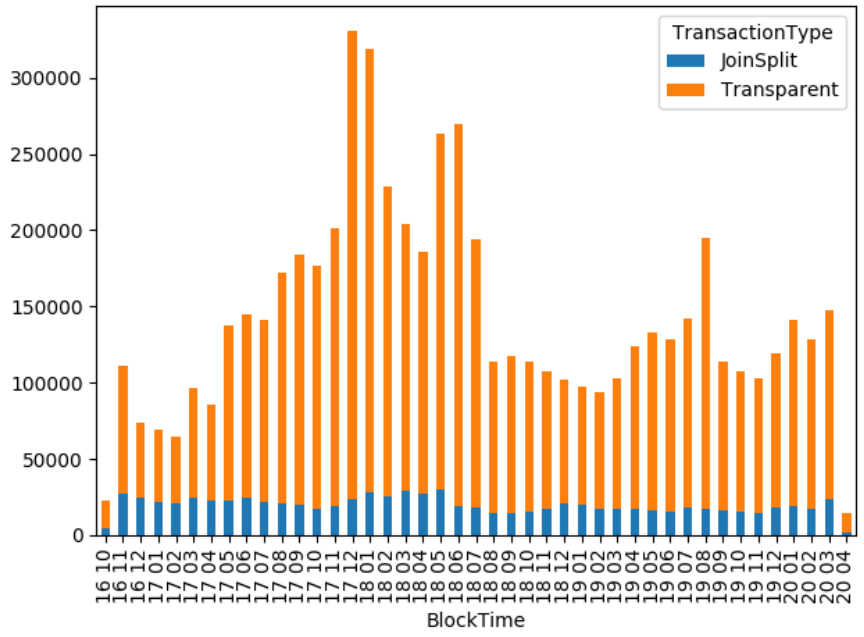
Bölüm 3

Uygulama ve Analiz

Bölüm 2'de anlatıldığı gibi Bitcoin'in kullanıcı gizliliğini ve işlem anonimliğini neredeyse hiçbir şekilde sağlayamadığı detaylı bir şekilde anlatılmıştır. Her ne kadar anonimliği artırmak adına CoinJoin uygulanması veya ToR kullanımı gibi çeşitli yöntemler önerilmesine rağmen bu yöntemlerinde de istenilen oranda etkili olmadığı ve anonimliği sağlayamadığı gözlemlenmiştir. Bu nedenle zamanla daha çok anonimliği ve gizliliği amaçlayan ve anonim kriptoparalar da denilen Dash, Zcash ve Monero gibi çeşitli anonim kriptoparalar yayınlanmıştır.

Yine Bölüm 2'de bu kriptoparaların çalışma mantıkları ve anonimliği nasıl sağlamaya çalıştıkları anlatılmıştır. Gerçekten de bu kriptoparaların tamamıyla istenilen seviyede anonimlik sağladığı ve hiçbir şekilde gizlilik ve takip edilememezliği ihlal etmedikleri düşünülmüştür. Ne var ki, blokzincirdeki kriptosistemin analiz edilmesi, kriptopara sistemindeki zaafiyetlere yapılan saldırılar, kötü niyetli düğüm ve/veya madencilerin yaptıkları faaliyetler veya saldırılar, kriptoparanın ağının analiz edilmesi hatta anonim kriptopara işlemlerinin bilinçsiz bir şekilde kullanılmasıyla beraber kullanıcı alışkanlarından çıkartılan şablonların analiz edilmesi gibi birçok çeşitli farklı yöntemlerle bahsedilen bu anonim kriptoparaların da düşünüldüğü kadar anonimlik ve gizliliği sağlayamadığı gözlemlenmiştir. Mesela Zcash kriptoparası kullandığı zk-SNARKs ile teoride kırılması günümüz yöntemlerinde kolay olmayan bir çeşit algoritmik güvenlik mekanizması sunar. Ancak pratikte mesela madenci havuzlarının kendi madencilerine yaptığı ödemeler analiz edildiğinde korumalı işlemler ile şeffaf işlemler arasında ilişki kurmak mümkün olmaktadır. Bu örnek bile tek başına Bölüm 2'deki Kısım 2.4'te bahsedilmiş olan Takip Edilememezlik özelliğinin ihlali anlamına gelmektedir.

Tezin bu kısmında Alex Birkuyov tarafından hazırlanmış olan [28] makalesinde yapılan çalışmalar temel alınarak anonim kriptoparaların işlemleri üzerinde analizler yapılacaktır.



Şekil 3.1: Yıl ve Aylara Göre İşlem Tipi (Transaction Type) Grafiği

Yapılan bu analizler neticesinde anonim olan işlemlerin gizlilik ve takip edilememezliklerinin ne derecede ihlal edilebileceği hesaplanacaktır. Kriptoparaların analizi için Bitcoin ve Bitcoin kodundan türetilme Dash kriptoparası 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 çatallaması[2] kullanılacaktır.

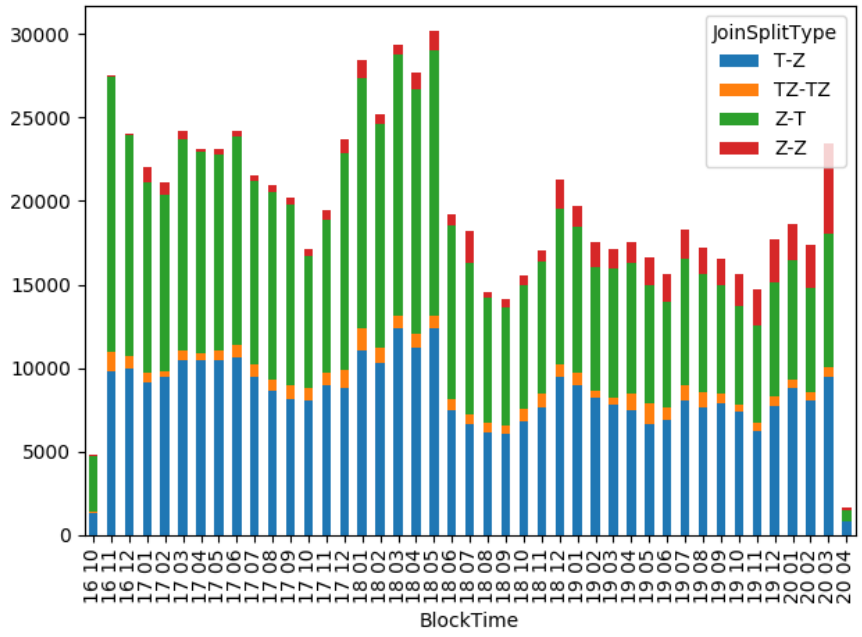
3.1 Zcash Analizi

Zcash için analize 784834. bloğun üretildiği tarih olan 04 Nisan 2020 Cumartesi 12:03:06 tarihinde başlanmıştır. Yani Zcash kriptoparası için aşağıda detaylıca anlatılacak olan analiz çalışması 04 Nisan 2020 tarihinden önce üretilmiş olan 1. bloktan 784834. bloğa kadar olan blokzincirdeki tüm blokları kapsar. 784834. bloktan sonra üretilmiş ve üretilecek olan bloklar, yapıacak olan analiz çalışması her bir yeni blok için sürekli olarak tekrar edilmesi mümkün olmadığından bu tezin analiz çalışması kapsamınının dışındadır.

Yapılan çalışmada ilk olarak Zcash kullanıcılarının korumalı coin aktarımı sağlayan EB-işlemlerini ne oranda kullandıklarına bakılmıştır. Şekil 3.1'de gösterilmekte olan

[1]Princeton University - Center for Information Technology Policy tarafından hazırlanan Blocksci açık kaynaklı uygulama koduna Github - Blocksci bağlantı adresine tıklayarak ulaşabilirsiniz.

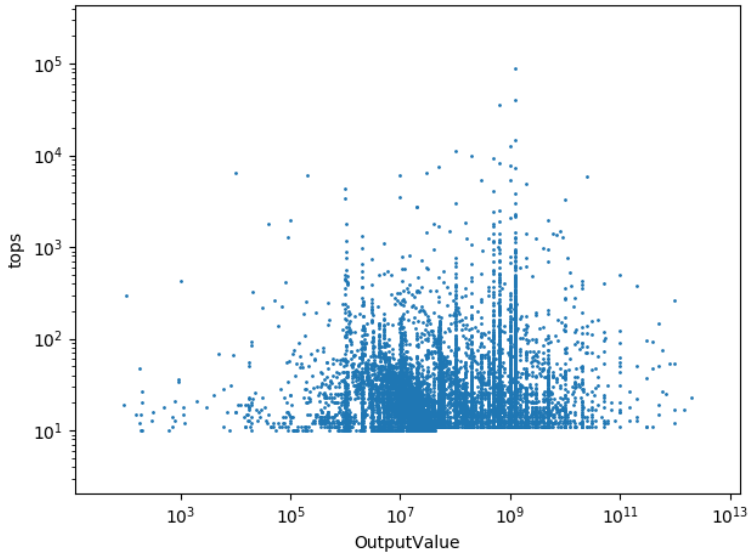
[2]CryptoLux Research Group at SnT, University of Luxembourg tarafından hazırlanmış olan Blocksci uygulamasının Zcash için hazırlanmış çatallaması Github - Zcash için Blockscibağlantı adresine tıklayarak ulaşabilirsiniz.



Şekil 3.2: Yıl ve Aylara Göre EkleBöl İşlemleri Tipi (JoinSplit Transactions Type) Grafiği

grafik Zcash için yıl ve aylara göre değişen işlem tiplerinin grafiğidir. Sadece bu grafik incelendiği zaman Zcash kriptoparasını tercih eden kullanıcıların "anonim bir kriptopara" olan Zcash'in EB-işlemlerini istenilen düzeyde tercih etmedikleri gözlemlenmektedir. Korumalı işlemlerinin kullanımının artması işlem anonimliğini ve takip edilememezliğini ciddi bir şekilde artırmaktadır; ancak en başta kullanıcılar tarafından EB-işlemlerinin yeterince tercih edilmemesi Zcash'in istenilen düzeyde anonim olmamasına neden olur. Zcash'in ilk çıktığı zamanlar olan 2016 Ekim, Kasım ve Aralık aylarında gizli adrese sahip işlemlerin tüm işlemlere oranı %25 - %30 oranı civarında çıkmaktadır. Zamanla bu EB-işlemlerinin oranın artması beklenirken 2019-2020 yılları arasında bu oranın %10 - %15 civarına kadar düştüğü gözlemlenmektedir. Mart 2020 ayı için bu oran %15.91 olarak hesaplanmıştır.

Analiz çalışmasında daha sonra gizli adrese sahip EB-işlemlerini tercih eden kullanıcıların hangi EB-işlemi tipini ne oranda kullandıkları incelenmiştir. Şekil **??**'deki grafikte yıl ve aylara göre tercih edilen EB-işlemleri tipi grafiği gösterilmektedir. 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 civarındayken zaman içerisinde yavaş da olsa bu oran önemli bir artış göstermiştir ve Mart 2020'de bu oran %23.17'ye kadar çıkmıştır. Bu grafik EB-işlemlerini kullanan Zcash kullanıcılarının zaman içerisinde iyiye işaret olarak daha da 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



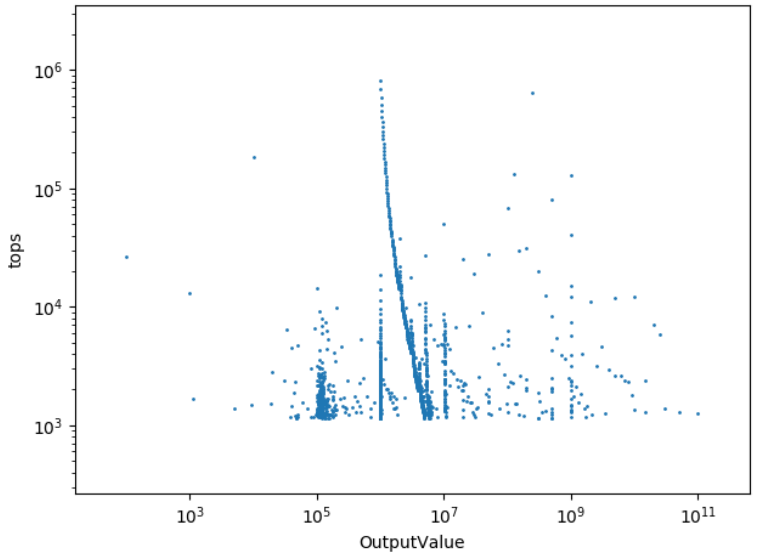
Şekil 3.3: En Çok Kullanılan 10,000 İşlem Çıktısı

havuzdan çıkan ZECler hakkında bilgi verirler. zden zye işlemler olan korumalı EB-işlemlerinin artması demek takip edilemezlik özelliğinin artması demektir. Sonuç olarak bu da Zcash işlem anonimliğinin artması demektir, ki bu durum da Zcash kriptoparası için iyiye işaret eden bir durumdur.

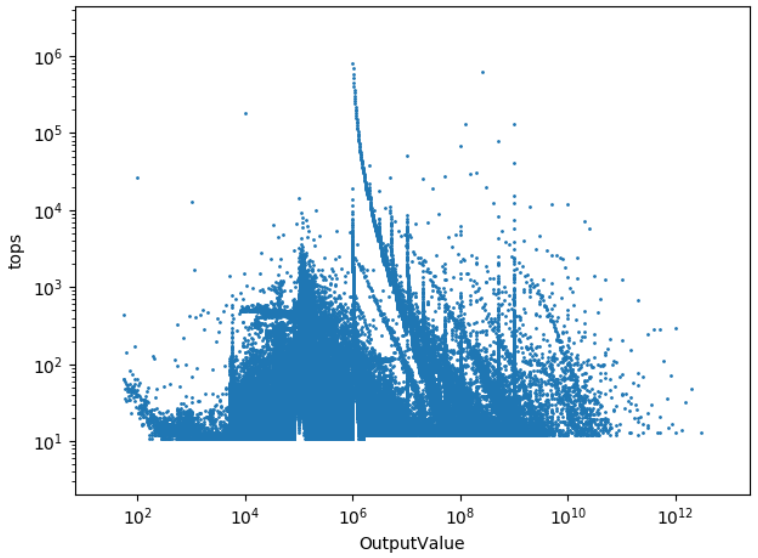
Bir sonraki iş olarak Şekil 3.3'teki grafikte gösterildiği gibi bu zamana kadar yapılmış tüm işlemler için en çok kullanılan 10,000 işlem çıktısına, yani çıktı değeri 0'dan büyük olacak şekilde t-adreslerine gönderilen işlemlerin çıktı değerine bakılmıştır[3]. Ne var ki, sadece bu grafiğe bakarak herhangi bir şey söylemek maalesef ki mümkün olmamamıştır. Zcash kullanıcıları genel olarak düşünüldüğünde çıktı miktarlarını seçerken belli bir "alışkanlık kalıbına" bağlı kalmamışlardır. Her ne kadar çıktılar daha çok 10^9 Zatoshi yani 10 ZEC üzerinde yoğunlaşmış olsalar da doğrudan bir şey söylemek ve buna göre bir gruplandırma yapmak Şekil 3.3'teki grafik için mümkün değildir.

Tüm "işlemler" için en çok kullanılan 10,000 işlem çıktısına bakıldığında herhangi bir elle tutulur sonuç elde edilmediğinden daha sonra tüm "işlem adresleri çıktıları" için en çok kullanılan 10,000 adres çıktısı da ayrıca incelenmiştir. Şekil 3.4'teki grafikte en çok kullanılan 10,000 işlem adresleri çıktısı değeri verilmiştir. Burada en çok kullanılan 10,000 işlem çıktısı değerinden ziyade en çok kullanılan 10,000 işlemin çıktı adresleri değeri incelenmiştir. Bunun anlamı da 10,000 adres için toplam işlem sayısı muhtemelen 10,000'den çok daha azdır. Misal vermek gerekirse, 4 ZEC, 5 ZEC ve 6 ZEC şeklinde 3 tane çıktısı olan bir X_i işlemi düşünülürse işlem çıktı değeri 15 ZEC olurken işlem çıktısı adresleri değerleri sırasıyla 4 ZEC, 5 ZEC ve 6 ZEC şeklinde üç farklı değer olacaktır.

[3]İşlem çıktısı tek başına işlem girdisini vermez, işlem çıktısı ile işlem bedelinin toplamı işlem girdisini verir. Bu hususun karıştırılmaması adına tekrar hatırlatmakta fayda vardır



Şekil 3.4: En Çok Kullanılan 10,000 Adres Çıktısı



Şekil 3.5: En Çok Kullanılan 1,000,000 Adres Çıktısı

Şekil 3.4'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 azalacak şekilde değiştiği gözlemlenmektedir. Bu da Zcash kriptoparasında özellikle 0,01 ZEC ve civarındaki ZEC miktarlarının azımsanmayacak bir farkla en çok kullanılan adres çıktısı değerleri olduğunu gösterir.

Yine tüm işlemlerin çıktı adreslerinin en çok kullandığı 1,000,000 adres çıktısı değeri incelenmek istendiğinde Şekil 3.5'teki grafikte görülmekte olan sonuç ortaya çıkmaktadır. Şekil 3.4'teki grafikte olduğu gibi 3.5'teki grafikte de 0.01 ZEC değeri etrafında önemli derecede

bir yoğunlaşma rahatlıkla gözlemlenebilmektedir. Madenci havuzlarının bünyesinde bulundurdukları madencilere genellikle 0.01 ZEC civarında katılım payı verdikleri bilinmektedir. Bu sayede Şekil 3.4 ile Şekil 3.5 grafiklerinde gözlemlenen yoğunlaşmanının madenci havuzlarının yaptıkları madenci ödemelerinden kaynaklandığını sonucuna varılabilir. Aynı zamanda elde edilen bu sonuç madencilerle birlikte 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 yani korumalı işlemler aracılığıyla gönderdiği bilindiğinden dolayı bu yoğunlaşmanın tamamıyla madenci havuzlarının yaptıkları ödemelerden kaynaklı olduğunu henüz söylemek kolay değildir.

3.1.1 Madencilerin Analizi

Daha önceki bölümlerde bahsedildiği üzere Zcash blokları madenciler tarafından kriptografik olarak çeşitli işlemler yapıldıktan sonra üretilerek Zcash ağına gönderilir ve konsensus üretilen bu blokta çoğunluğa ulaşarak asıl blokzincirde yeralmasını sağlar. Bloğun üretilmesi sonrasında Zcash kriptoparasını oluşturan kurucular tarafından belirlenen bir "blok üretme ödülü" (mevcut durumda 5 ZEC'tir) ile beraber bloktaki her bir işlemin işlem bedelleri toplamı bloğu üreten madenciye verilir. Blok üretimi özellikle kriptoparaların çıktığı ilk yıllarda bir yahut birkaç makine ile hesaplama yapan bireysel madenciler tarafından yapılmaktaydı. Zamanla rekabetin artmasıyla beraber madenciler blok üretme hızını, kapasitesini ve performansını artırarak blok üretme şanslarını daha yüksek seviyelere çıkarmak amacıyla bireysel blok üretiminden grup halinde blok üretimini tercih etmeye başladılar. Bu durum da üye sayısı günümüzde yüzleri hatta binleri bulan ve ciddi büyüklükte blok mahzenlerine sahip madenci havuzlarının ortaya çıkmasını sağlamıştır. Böylece bireysel çalışan madenciler zamanla üretilen bloktan pay alma şanslarını en yüksek seviyelere çıkarmak amacıyla ciddi manada işlemci gücü ve dolayısıyla ağ özetleme oranı hızına sahip olan maden havuzlarına üye olmaya başladılar.

Şekil 3.6'da Aktif Zcash madenci havuzları gösterilmektedir. Şekildeki madenci havuzları ağ özetleme oranının (network hashrate) %82'sini kapsarken Poolin isimli madenci havuzu toplam ağ özetleme oranının önemli bir kısmını, yani %30.9 kadarını kapsadığı görülmektedir. Bu durum "merkezisizleştirilmiş" olarak bir merkezi otorite olmaksızın işlem yapan blokzincirler için oldukça tehlikeli bir durumdur. %51 saldırılarının kriptoparalar için en büyük tehlikelerden birisi olduğu düşünüldüğünde Zcash anonim kriptoparası için bu durum elzem bir tehlike arz etmektedir. Gerçekten de Nisan 2020'de yapılmış olan madenciler analizinde Poolin isimli madenci havuzunun blok üretme madenciliği ödülü pastasından en fazla payı aldığı gözlemlenmiştir. Poolin isimli madenci havuzunu F2Pool

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 3.6: Aktif Zcash Madenci Havuzları https://www.poolwatch.io/coin/zcash bağlantı adresini kullanarak ulaşabilirsiniz. 1 Temmuz 2020 1:37 tarihinde erişilmiştir.

ve Antpool isimli madenci havuzları takip etmiştir. Çıkan sonuç Şekil 3.6'de gösterilmiş olan grafikle eşleşmektedir.

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 dahil olması gibi sebepler nedeniyle aşağıda detaylı olarak açıklanacak işlem analizleri yukarıdaki grafiklerde yapıldığı gibi 784834 bloğu kapsatacak şekilde blokzincirdeki o zamana kadar üretilen tüm bloklar için yapılmamıştır. Ayrıca belki de milyonlarca işlemle beraber bu işlemlerde ZEC gönderip alan milyonlarca adresi sürekli olarak analiz işlemine girdirmek analiz performansı açısından etkili sonuçlar almayı zorlaştıracaktır. Bahsedilen bu nedenlerden dolayı Zcash anonim kriptoparası için yapılan 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 belirli analizlere sokularak karşılaştırılmış ve hız ile beraber performans - efektiflik karşılaştırması yapıldığında son 25,000 bloğun analizininin yapılmasının en doğrusu olacağına karar verilmiştir.

Tablo 3.1'de tüm Zcash madenci ve madenci havuzlarının toplamda üretmiş oldukları blok sayısıyla elde ettikleri blok ödülleri Zatoshi cinsinden gösterilmektedir. 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 bahsedilenler tespit edilemeyen diğer madenci yahut madenci havuzlarına ait adreslerdir. Bunlara havuz denmeyişinin tek sebebi bu adreslerin madenci havuzuna mı yoksa doğrudan bir madenciye mi ait olduğu

Tablo 3.1: Son 25,000 Blok İçin Madenci Havuzları ve Madencilerinin Ürettikleri Blok Sayıları ve Kazandıkları Toplam Blok Ödüllerinin Tablosu

Madenci Havuzu	Üretilen Blok	Elde Edilen Ödül
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$_1$	1671	835,613,483,844
t-Havuz$_7$	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$_8$	119	59,505,023,033
t-Havuz$_9$	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$_{10}$	48	24,001,376,828
t-Madenci$_8$	40	20,002,890,351
t-Havuz$_{11}$	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

tespit edilememesinden kaynaklanır. 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 madenci yahut madenci havuzlarının neden bu şekilde bir işlem yaptıklarıyla alakalı herhangi bir bilgiye ulaşılamamıştır. Ayrıca ödülü paylaşan bu t-adresler yüzünden TOPLAM kısmında toplamda üretilen blok sayısı 25,000 olması gerekirken 25,395 blok üretilmiş gibi görünmektedir. Fazladan tabloya giren dört t-adres toplamda aslında 203 blokta üretilen blok ödülünü palaşırlar. Bu adresler incelendiği zaman bulundukları toplam blok sayısının 395 olduğu gözlemlenmiştir.

Madenciler edindikleri maden ödülünü ilk olarak korumalı havuzdan geçirip daha sonra elde ettikleri ödülü kullanmaları şartı bulunur. Bu nedenle elde edilen tüm ödüller bir şekilde korumalı havuza aktarılırlar, yani üretilen ödüllerin coinleri korumalı havuza aktarılmak maksadıyla EB-işlemleri ile en azından bir kere temasta bulunurlar. Madenci havuzları da ilk olarak ödülü korumalı havuza koyar, daha sonra madencilere ödeme için pay ederler. Yukarıdaki madenci havuzları incelendiği zaman üç farklı şekilde bünyelerindeki madencilere blok ödülünden pay verdikleri görülmüştür:

1. İlk yöntemde madenci havuzları korumalı havuzdan coini bir t-adrese aktarır. Daha sonra madencilerine sahibi oldukları bu t-adresi üzerinden ödeme yaparlar. Yani zden tye bir EB-işlemi gerçekleştikten sonra ödeme tamamen şeffaf işlem denilen tden tye olacak şekilde gerçekleştirilir. Bu şekilde ödeme yapan madenciler **TMadenciler** denilir. Üretilen ödül madenci havuzunun bir t-adresine aktarılır. Daha sonra madenci havuzu kendisine ait bir z-adresine ödülü aktararak ödülün korumalı havuzda toplanmasını sağlar. Bir süre sonra madenci havuzu bu ödülü tekrar kendisine ait farklı (bazen aynı) bir t-adrese yollar. Madencilere ödülden pay aktarımı bu t-adres üzerinden olur. Madencilerin adresleri de yine açık olan t-adreslerdir.

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 bulabilen çıktılar olan t-adreslere ödeme yapılmasıdır. Bu t-adresler genellikle madencilere ait olan adresler olmaktadır. Bu şekilde bir coin gönderimini madenci havuzları dışında herhangi bir kullanıcı grubu tarafından yapıldığı gözlemlenmemiştir. Bu şekilde payı dağıtan madenci havuzlarına **ZMadenciler** adı verilir. Ödülün havuza kadar olan kısmı TMadenciler ile aynıdır. Korumalı havuzda bulunan ödül daha sonradan doğrudan korumalı havuzdan z-adresini kullanarak madenci havuzu bünyesindeki madencilere ödül payını paylaştırır. Madencilerin adresleri yine açık olan t-adreslerdir.

3. Üçüncü ve son yöntemde madenci havuzları pay dağıtımını tamamen korumalı işlemler denilen zden zye işlemler vasıtasıyla yaparlar. Korumalı işlemleri analiz etmek mümkün olmadığı için de bu madenci havuzları mecburen es geçilecektir. Burada korumalı havuza kadar olan kısım TMadencilerle ZMadencilerde olduğu gibidir. Aradaki en önemli fark, ödeme madencilerin z-adreslerine yapılır. Yani ödül hep korumalı havuzda kalır.

3.1.1.1 TMadencilerin Analizi

Alex Birkuyov'un hazırlamış olduğu [28] makalesinden yola çıkılarak TMadencilerin analizi yapılmıştır. Ne var ki, makalede kısaca belirtilmiş olan Tmadencilerin analiz edilmesini sağlayan algoritma oldukça yüzeysel belirtilmiştir. Bu nedenle ilgili algoritmadan yola çıkılarak yeni bir TMadenci bulma algoritması yazılmıştır. Tmadencileri bulma algoritması Kısım A'daki Algoritma 1'de detaylıca gösterilmiştir.

TMadencileri bulma algoritması olan Algoritma 1 şu şekilde açıklanabilir:

1. İlk olarak Zcash blokzincirindeki son 25,000 blok çekilir.
2. Daha sonra çıktı sayısı 30 ve daha fazla olan ancak EB-işlemi olmayan (yani girdi yahut çıktısında gizli z-adres barındırmayan) tüm şeffaf tden tye işlemler listelenir. 30 adresten daha fazla adrese coin aktarımını madenci havuzlarından başka herhangi bir kullanıcı grubunun yapması olma ihtimali düşük olmasına rağmen sıfır değildir. Bu nedenle Bu işlemlere TMadenci olma ihtimali olan "muhtemelTMadenciListesi" denir. Çıktı sayısı olarak 20, 25, 40 ve 50 çıktılı işlemler gruplanmıştır. En etkili sonuçlar 30 ve daha fazla çıktılı işlemlerde alındığı için 30 çıktılı işlemler listeye alınmaktadır.
3. Analiz edilmek üzere zden tye EB-işlem olan tüm işlemler "korumaliHavuzdanCoinAlanListesi" denilerek listelenir.
4. muhtemelTMadenciListesi ile korumaliHavuzdanCoinAlanListesi içerisinde bulunan işlemlerden ortak olanlar alınarak tekrardan muhtemelTMadenciListesi'ne atanır. Burada yapılan işlem madencilerine şeffaf işlemlerle ödeme yaparken bu adrese daha önceki işlemlerde korumalı havuzdan ZEC aktarılmış muhtemel madenci havuzu adreslerini tesptit etmektir. Böylece listede sadece korumalı havuzla ilişkisi olan muhtemel madenci havuzları adresleri listelenmiş olur. Aynı işlem korumaliHavuzdanCoinAlanListesi için de yapılır.
5. Bazı muhtemel madenci havuzları birden fazla adres kullanarak korumalı havuzdan ZEC alıp madencilerine ödülden ödeme yaparlar. Bu nedenle ortak adresleri kullanan madenci havuzları adresleri TMadencilerGrupla prosedürü kullanılarak gruplanmıştır. Herbir muhtemel TMadencinin madenci adresleriyle teker teker karşılaştırılarak tüm diğer muhtemelTMadenci adresleri karşılaştırılır. İlk önce döngüye sokulan muhtemel TMadencinin ödülden pay aktarımı yaptığı madenci adresleri listeye alınır. Daha sonra muhtemelTMadenciListesi döngüye sokularak kendisi hariç diğer tüm muhtemel TMadencilerin madenci adresleriyle karşılaştırma yapılır. Karşılaştırmada ortak adresler varsa ve ortak adreslerin sayısı 30 ve daha

Tablo 3.2: Algoritma 29 Sonucunda Bulunan MUhtemel TMadenciler Tablosu

Ödül Adresi	#Blok	Coin Değeri	Ödeme Adresi	#Blok	Coin Değeri
$Havuz_1$	11	5,502,394,915	$Adres_1$	11	5,502,174,915
$Havuz_2$	1864	991,096,475,562	$Adres_2$	1848	991,559,348,012
$Havuz_3$	10	64,504,511,838	$Adres_3$	9	64,500,000,000
$Havuz_4$	46	2,049,331,846,484	$Adres_4$	22	2,049,331,406,484
TOPLAM	1931	1,061,103,382,315	TOPLAM	1890	1,061,561,522,927

fazlaysa bu iki muhtemel TMadenci adresi aslında tekbir madenci havuzuna aittir denilir. Bu şekilde tüm muhtemel TMadenciler birbirleriyle karşılaştırılır.

6. TMadencileriGrupla işlemi sonrası sonuç olarak "korumaliHavuzdanCoinAlanGruplanmisListesi" adı verilen liste elde edilir. Bu liste, korumaliHavuzdanCoinAlanListesi'nde bulunan muhtemel TMadenci havuzu adreslerinin TMadencileriGrupla işlemi sonrası ortak adreslere sahip muhtemel TMadenci havuzlarının gruplanmasıyla oluşturulmuş listedir.

Bahsedilen algoritma 6. aşamadan sonra sona erer. Daha sonra bu korumaliHavuzdanCoinAlanGruplanmisListesi ile daha önce tespit edilmiş olan madenci havuzları listesi karşılaştırılır. Karşılaştırma, blok üretme ödüllerini korumalı havuza koyan madenci havuzlarının yaptıkları tden zye işlemlerinin girdi toplamlarıyla korumaliHavuzdanCoinAlanGruplanmisListesi'ndeki muhtemel TMadencilerin yaptıkları zden tye işlemlerinin çıktı toplamları karşılaştırılır. Bu karşılaştırma sonucunda bulunan veriler aşağıdaki gibidir:

Son 25,000 blok içerisinde toplamda 17,656 EB-işlemi yapılmıştır. TMadenci analizi ile beraber 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 izlenebilmektedir. TMadencilerin analizi ile son 25,000 blok için tüm EB-işlemlerinin %21.6'sının anonimliği ve gizliliği analiz edebilmiştir. Son 10,000 ve 50,000 blok analizi yapıldığında da yine benzer oranlar elde edilmiştir.

3.1.1.2 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 doğrudan korumalı havuzdan madencilerine olacak şekilde yaparlar. Yani ödemeler zden tye EB-işlemleri vasıtasıyla yapılır. ZMadencileri bulmak için kullanılmış olan Algoritma 2, EK B bölümünde bahsedilmiştir.

ZMadenci Havuzlarının Bulunması algoritması olan Algoritma 2 özet olarak şu şekilde açıklanabilir:

1. Evvela blokzincirdeki son 25,000 blok çekilir.
2. Daha sonra çıktı sayısı 30'dan fazla olan ve EB-işlemi olan tüm işlemler "muhtemelZ-Madenciler" adıyla listelenir. Burada TMadencilerde olduğu gibi ikinci bir liste alıp her iki listedeki ortak adresleri bulmaya iki sebepten görek yoktur; ilki madencilere ödemeler doğrudan korumalı havuzdan yapılır. İkincisiyse zaten zden tye yapılan işlemlerde girdi adresi gizlendiği için hangi z-adresten işlem yapıldığını bilmenin imkanı yoktur.
3. Tmadencilerde olduğu gibi ödeme yapılan ortak madenci adresleri kullanılarak aynı madenci havuzunun TMadenci adreslerini de gruplamak 2. maddede anlatılan sebepten dolayı yine mümkün değildir. Bu nedenle ZMadencileri için ödeme yapılan adresler kullanılarak farklı bir gruplandırma yapılacaktır. Yapılacak bu gruplandırma için tüm muhtemelZMadenciler listesindeki tüm ödeme yapılan madenci adresleri "odemeYapilanMadenciListesi"nde toplanır.
4. muhtemelZMadenciler listesi döngüye sokularak herbir muhtemelZMadenci içindeki ödeme yapılan madenci adresleri "ZMadencileriGrupla" isimli prosedürde birbirleriyle karşılaştırılır.
5. ZMadencileriGrupla prosedüründe yapılacak karşılaştırma için ilk olarak mevcut muhtemelZMadencinin ödeme yapılan madenci adresleri listesi "mevcutIslemAdres-Listesi"nde toplanır ve bu listedeki tüm adresler "eskiAdresListesi" adında ikinci bir listeye atanır.
6. muhtemelZMadencilerListesindeki mevcut muhtemelZMadenci hariç tüm muhtemelZ-Madenciler döngüye sokulur. Döngüye sokulan herbir muhtemelZMadenci için ayrıca ödeme yapılan madenci adresleri listesi zMadenciIslemiAdresListesi adlı üçüncü bir adres listesinde toplanır.
7. mevcutIslemAdresListesi ile zMadenciIslemiAdresListesi isimli listeler içerisinde bulunan ödeme yapılmış madenci adresleri listesi birbirleriyle karşılaştırılır. Aralarında 30 ve daha fazla ortak adres bulunması durumunda tüm yeni adresler mevcutIslemAdresListesi'ne tekrardan atanır; yani madenci havuzları için ortak olabilecek tüm adresler bir işlem altında gruplandırılır. Yapılan gruplandırmalar gruplanmisZMadenciListesi'ne atanır ve bu değer dönülerek algoritma sonlandırılır.

Algoritma sonucunda bulunan gruplanmış ZMadenciler listesi ile Tablo 3.1'te daha önceden bulunmuş olan madenci havuzları bilgileri karşılaştırılır. Karşılaştırma sonuçlarına göre

Tablo 3.3: Algoritma 2 Analizi Sonucunda Bulunan Muhtemel ZMadenciler

Ödül Adresi	#Blok	Coin Değeri	[a]	#Blok	Coin Değeri
Havuz_1	100	57,002,644,529	İşlem_1	98	56,955,178,696
Havuz_2	111	59,004,988,098	İşlem_2	109	58,828,420,000
TOPLAM	211	116,007,632,627		207	115,783,598,696

[a]Ödülü madencilere dağıtan herhabgi bir adres t-adresi yoktur, bu nedenle burası boş kalacaktır.

toplamda 418 korumalı işlem birbirleriyle ilişkilendirilmiştir; bu da son 25,000 bloktaki korumalı işlemlerin %02.4'sine tekabül eder. Böylece TMadenci havuzu analizleriyle beraber toplamda korumalı işlemlerin %24'ü ilişkilendirilmiş olunur.

TMadencilerle yahut ZMadencilerle ilişkilendirilememiş 24 madenci daha bulunmaktadır. Bu madencilerden bir kısmı belki de madenci havuzu değil ciddi miktarda işlemci gücü toplamış madenci gruplarıdırır. Ayrıca bahsedilen madencilerin TMadenci ve ZMadenci algoritmalarında tespit edilememesinin bir nedeni de madenci havuzlarınının bünyesinde bulundurdukları madencilere blok ödülünden payı zden zye korumalı işlemler vasıtasıyla gerçekleştirmesidir. Kalan madencilerin 2158 EB-işlemi daha bulunmaktadır, ki bu da tüm EB-işlemlerinin %12.2'sidir. Her ne kadar bu işlemler takip edilememiş olmasıyla beraber toplamda tüm EB-işlemlerinin %36.2'sinin madenciler ve madenci havuzları ile bir şekilde ilişkili olduğu söylenebilir.

3.1.2 Gidiş-Geliş İşlemleri

Zcash kriptoparasını kullanan ve yaptıkları coin aktarımlarına mahremiyet kazandırmak isteyen Zcash kullanıcıları bunu daha önce de bahsettiğimiz gibi 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 coin aktarımı gerçekleştirirler. Yapılan bu işlemler sonucunda da coin 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) denir, [46].

Korumalı işlemlerdeki yapılan analizlere geçilmeden ilginç bir veri göze çarpmıştır. Toplamda 325 tden zye EB-işleminde aynı tek adres 125 ZEC'lik değerler korumalı havuza göndermiştir. Bu adres maden üretme ödülünün verildiği ve 0 girdi adresine sahip olan işlemlerdeki kurucu ödül payını alan ve Zcash'in kurucularına ait olan bir adrestir. Ancak korumalı havuzdan hangi işlemlerde çıktığı; hatta hiç çıkıp çıkmadığı

tespit edilemediği için yukarıdaki kalan 23 madenci havuzu adresi gibi bu işlemler de tam olarak analiz edilememiştir.

Gidiş-geliş işlemleri analiz edilirken en başta TMadencilerle ZMadencilerde tespit edilen işlemler analiz edilecek işlemler listesinden çıkartılmıştır. Burada dikkat edilmesi gereken göze çarpan bir durum daha gözlemlenmiştir; madenci işlemleri listeden çıkartılmasına rağmen madenciler ve madenci havuzları ile alakalı EB-işlemleri önemli bir oranda EB-işlemlerinde göze çarpmaktadır. TMadenci ve Zmadenci analizlerinin her ikisinde de bu EB-işlemleri tespit edilmemiş olup, madenci havuzlarının yukarıda bahsedilen tipik coin aktarımına benzeyen farklı yeni işlemler ve bu işlemleri yapan yeni adresler tespit edilmiştir. Ancak girdi-çıktı değerleri karşılaştırmasında bile istenilen şekilde herhangi bir ilişkilendirme verisi elde edilememiştir. bahsedilen bu durumdan çıkartılacak sonuç zaman içerisinde madenci havuzlarının yaptıkları aktarımlarda daha da dikkatli olmaya başladıklarıdır söylenebilir.

Gidiş-geliş işlemleri 3 farklı yöntemle analiz edilmektedir [28]. 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 bir de zden tye işlemin değerlerinin son 4 rakamı karşılaştırılır. Son 4 rakamında benzerlik olan değerler yine asıl değerleri birbirlerine yakınsa aralarında bir ilişki vardır denilebilir.

Tüm gidiş-geliş işlemleri karşılaştırmaları detaylıca aşağıdaki gibi açıklanmıştır. Yapılan analizler karmaşık algoritmalara sahip olmadığı için TMadenciler ile ZMadenciler analizlerinde anlatılan algoritmalar gibi bir algoritma ile gidiş-geliş işlemleri anlatılmayacaktır.

3.1.2.1 Temel Karşılaştırma

Temel karşılaştırma adını verilen ilk karşılaştırma analiz yönteminde korumalı havuza coin 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 coin değeri ile çıkan coin değeri karşılaştırılır ve birbirlerine eşit olmaları halinde bu bu iki işlem arasında bir ilişki olduğu varsayılır. Bu karşılaştırmadaki tek koşul t-z işleminin z-t işleminden önce gerçekleşmiş olmasıdır. Yani t-z işlemi t_1 zamanında gerçekleşmiş ise z-t işleminin t_1+t_i zamanında gerçekleşmiş olması gerekir.

Yukarıda da bahsedildiği gibi bazı coin değerlerinin son 25,000 blok içerisinde yüzlerce defa kullanıldığı tespit edilmiştir. Bunların büyük bir çoğunluğunu madenci havuzlarının yaptığı coin aktarımlarına aittir. Bunun yanında bir kısmı da yine Zcash'in sahiplerine ait adreslerin yaptığı t-z işlemleridir. Bu nedenle çoklamaların engellenmesi adına ilk olarak daha önce ilişki tespit edilen işlemler karşılaştırma algoritmasına sokulmamıştır. Daha sonra kalan işlemlerin girdi ve çıktı değerleri sıralanarak 3 kereden fazla karşılaştırmaya giren değerler de ayrıca sokulmamıştır. Bunların yanında yapılan karşılaştırmalarda ayrıca t-z işleminin z-t işleminden önce olmasına (yani hem blok nosu hem de işlem nosu olarak küçük olmasına) dikkat edilmiştir. Listeden çıkartılmış kayıtlar içerisinde de birbirleriyle ilişkisi olan kayıtların olması çok muhtemeldir. 3 defadan daha fazla karşılaştırmada görünen değerlere sahip işlemlerin sonuç listesinden çıkartılmasının temel sebebi listede ciddi manada kayıt çoklamasına sebep olmasıdır; bu çoklama da doğru bir şekilde aktarılan ZEC'in takip edilmesini zorlaştırmaktadır.

Yapılan karşılaştırmada ilk olarak birbirine eşit değerler karşılaştırılmıştır. Burada muhtemelen ilgili işlemleri gerçekleştiren Zcash kullanıcıları korumalı havuza girdirdiği değeri direk olarak hiçbir z-z (yahut belki tz-tz) işlemine sokmadan direk havuzdan çıkartmışlardır. Yani bashedilen kullanıcılar sadece t-z işlemi yapıp korumalı havuzda biraz ZEC'leri beklettikten sonra z-t işlemi yaparak korumalı havuzdaki parasını geri çekmişlerdir. Her ne kadar teoride bir şekilde anonimlik sağladığı düşünülse bile kullanıcıların yeterince bilinçli bir şekilde sistemi kullanmamaları görüldüğü gibi mahremiyet ve gizlilik ihlallerine sebep olmaktadır.

Ne var ki Zcash kullanıcılar havuza girdirdikleri coinleri karıştırmadan; yani kısaca z-z denilecek olan korumalı işlem yapmadan havuzdan çıkarmazlar. z-z işlemleri sayesinde kullanıcı korumalı havuzda kendisine ait olan ZEC'lerin izini kaybettirir. Bu bilgiden yola çıkarak havuza ZEC değeri girdirip başka hiçbir işlem yapmadan evvel z-z işlemi yapıp daha sonra sahip oldukları ZEC'leri o zaman havuzdan çıkartan Zcash sahiplerinin işlemlerinin de analizi ayrıca yapılmıştır. Bunun için karşılaştırmaya ayrıca işlem bedelleri de dahil edilmiştir.

Bahsedilen ilk temek karşılaştırmada karşılaştırma denklemi "t-z girdi değeri = z-t çıktı değeri" şeklindeydi. Yeni durumda karşılaştırmadaki denklem "t-z değeri = z-t değeri + işlem bedeli * (yapılan muhtemel z-z işlemi sayısı)" şeklinde değiştirilmiştir. İşlem bedellerinde ilk olarak sadece varsayılan işlem bedeli olan 10^5 Zatoshi dahil edilmiştir. Ancak işlem bedelleri coin aktaran kişiler tarafından değiştirilebileceğinden, yahut coin 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.

3.1.2.2 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 girilen değerle aynı yahut yakın bir değeri korumalı havuzdan çıkararak şeffaf havuzda Zcash işlemlerine devam etmek de yine düşünüldüğü kadar anonimlik sağlamamaktadır. Bu durumda anonimlik seviyesinin bir üstü denilebilecek şekilde Zcash kullanıcıları korumalı havuzdan çıkarken ellerinde bulundurkları ZEC'leri iki yahut daha fazla parçaya bölüp bu parçaları farklı t-adreslere göndererek anonimlik ve işlem gizliliğinin artmasını amaçlarlar. Ne var ki, ZEClerini iki parçaya bölerek korumalı havuzdan çıkartan kullanıcıların işlemlerini analiz etmenin de yöntemi bulunmaktadır. (Üç ve daha fazla parçaya bölünmüş olması ihtimali bulunan işlemler için bu analizi denenmiş, ancak performans açısından pek de efektif olmayan sonuçlarla karşılaşılmıştır. Örnek olarak mesela binlerce z-t işleminden hiçbir şekilde birbirleriyle alakalı olmayan 3 farklı işlemin toplamlarını ilgili herbir işlem için hesaplayıp bunu listelemek ciddi anlamda zamana ve işlemci gücüne mâl olmaktadır. Ayrıca çıkan milyonlarca sonucu t-z işlemleriyle karşıştırdıktan sonra elde edilen verilerden herhangi bir sonuç çıkarmak çok da mümkün olmamıştır.

Alt-küme Toplamlarının Karşılaştırılması durumunda iki farklı z-t işlemi çıktı değerleri toplamı bu değerlerden önce gerçekleşmiş olan herhangi bir t-z girdi değeri birbirleriyle karşılaştırılır. Karşılaştırma sonrası bu iki değer eşleştiği takdirde bu değerler arasında bir ilişki vardır denilebilir. 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 karşılaştırmada yapıldığı gibi 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.

3.1.2.3 Parmak İzi Değerleri Karşılaştırması

Zcash kullanıcıları EB-işlemleri kullanarak coin aktarımı yaparken bazen girdi değerinin varsayılan işlem ödülü 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-Madenciler, Z-Madenciler, bir önceki karşılaştırmalarda bulunan işlemler karşılaştırılacaklar listesinden çıkartılır. Ayrıca parmak izi değeri üç kereden daha fazla kez listeye giren değerlere ait işlemler de karşılaştırılacaklar listesinden çıkartılır. t-z işlemi girdi değeriyle z-t işlemi çıktı değeri son 4 rakamı eşit olan tüm işlemler bulunur. Burada dikkat edilmesi gereken en önemli nokta girdi değerinin çıktı değerinden büyük olması; ancak çok büyük olmamasıdır. Bu nedenle bulunan karşılaştırılan 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.

3.2 Dash Analizi

Dash analizine 26 Nisan 2020 16:23:44 tarihinde en son üretilmiş blok olan 1297693. blokla beraber başlanmıştır. Zcash analizinde olduğu gibi 1297693. bloktan sonra üretilmiş bloklar analize dahil değildir. Ayrıca madenci analizleriyle gidiş-geliş işlemleri analizi yine aynı şekilde Zcash kriptoparası için yapıldığı gibi son 25,000 blok temel alınarak yapılacaktır.

Dash analizi için yıllar içerisinde çeşitli araştırmalar yapılmıştır, [48], [30], [22]. Örnek olarak Dash kriptoparası için AnaUçların loglarının okunması (bu saldırıda saldırgan farklı AnaUçların yaptıkları ÖzelGönderim loglarını okur ve bu sayede ÖzelGönderim işleminde adres ilişkilendirmesini yapabilir), Sybil saldırısı (saldırgan Dash blokzincirinin itibar sistemine (reputation system) saldırır) veyahut AnaUç snooping (kötü niyetli AnaUçlarla tüm blokzinciri ele geçirmeye çalışma) gibi çeşitli saldırılar detaylı olarak açıklanmıştır, [30][4]. Kriptopsisteme yahut içerisindeki elemanlara saldırı yapmaktan ziyade bu tez çalışmasında Zcash analizinde bahsedildiği gibi Dash analizinde de birbirleriyle teoride hiçbir şekilde bir alakası yokmuş gibi görünen işlemler arasında girdi ve çıktı miktarları karşılaştırılarak bir ilişki bulunmaya çalışılacaktır.

Zcash kriptoparasında gizlilik, kriptografik yöntemlerle işlemde kullanılan adres ve miktarın gizlenmesi ve bunlar gerçekten gerçekleştiğini ispat eden "işin ispatının" zk-SNARKs

[4]Reply to Kristov's paper linkinde bulunan Dash formundaki ilgili yazıda Kristov'un bahsetmiş olduğu saldırılara karşı alınmaya çalışılan önlemlerden bahsedilmektedir.

adı verilen bir sır vermeyen tanıt (zero knowledge proof) ile sağlanmaktaydı. Dash gizliliği CoinJoin'den türetilmiş bir karıştırma algoritması ile sağlar. Zcash EB-işlemlerinde kullanılan ZEC'leri korumalı havuzda tutarken Dash karıştırmada kullanılan işlemleri yine aynı havuzda tutar; ancak kişinin karıştırılmış parası cüzdanındaki diğer değiştirme adreslerinde tutulur.

Bahsedilen nedenden ötürü Zcash'teki işlemler EB-işlemleri ve şeffaf işlemler olarak ikiye ayrılırken tüm işlemleri şeffaf olan Dash'in işlemleri ÖzelGönderim kullanılarak anonimlik sağlanmış karıştırma (mixing transactions) işlemleri ve normal işlemler olmak üzere ikiye ayrılır. . Doğrudan bu karıştırma işlemlerini analiz etmek adreslerin tek seferlik olmaları gibi sebeplerden ötürü pek de mümkün değildir. ÖzelGönderim işlemleri bu nedenle bir nevi Zcash'teki z-z korumalı işlemlerine benzer. Zcash'in analizi korumalı havuza giren ve korumalı havuzdan çıkan t-z ve z-t işlemleri sayesinde mümkün olmaktadır. Bu nedenle Dash'in analiz edilebilmesini mümkün kılmak için ÖzelGönderim dışındaki normal işlemleri analiz edilebilecek şekilde gruplandırmak gerekmektedir.

Dash kriptoparası için işlem tiplerini aşağıdaki gibi 5 parçaya bölmek mümkündür:

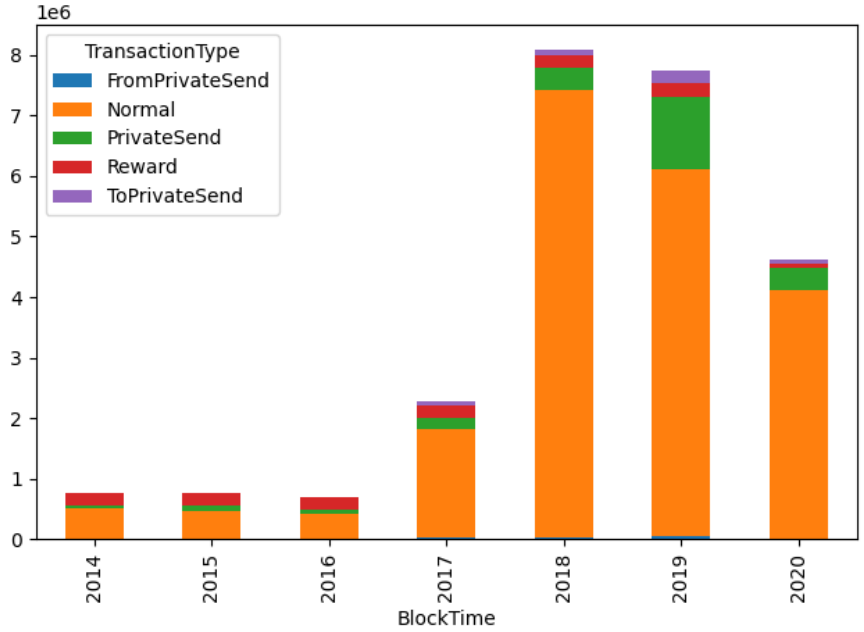
1. **Normal İşlemler:** Bitcoindeki işlemlerin aynısıdır. Zcashde bu işlemler şeffaf işlemler olarak geçer.

2. **Ödül İşlemleri:** Bloğu oluşturan madenciyle beraber ilgili AnaUç sunucusuna blok ödülünün verildiği işlemdir. Girdi adresi daima boştur ve işlem ücreti sıfırdır. Girdi değeri üretilen blok ödülüyle blok içerisinde geçen işlemlerin işlem bedeli değerlerinin toplamıdır.

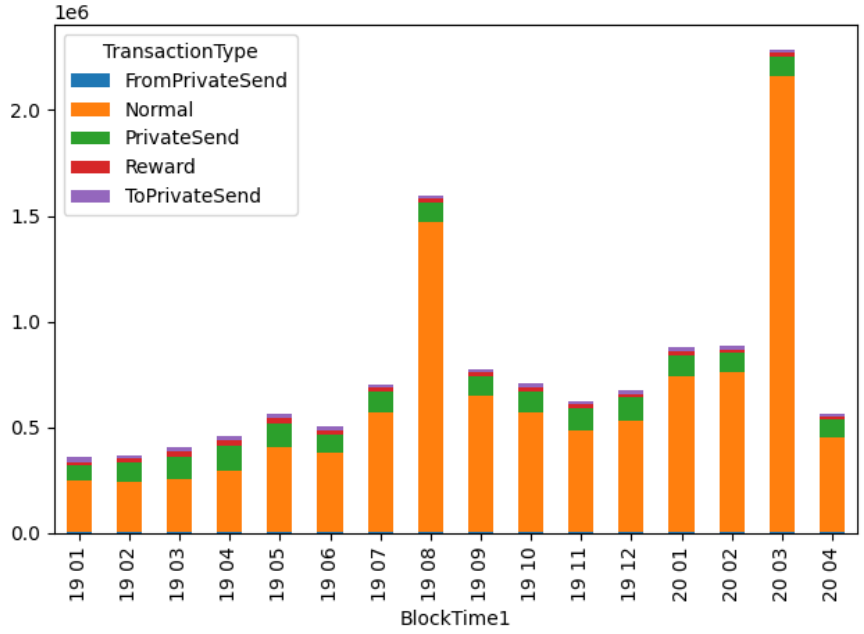
3. **ÖzelGönderim işlemleri:** Anonimliğin gerçekleştirildiği işlemlerdir. **??** bölümünde detaytlı bir şekilde anlatılmışlardır. Yapılan analiz çalışmasından bakıldığı zaman bir nevi Zcash'teki z'den z'ye işlemlere benzer. Girdi sayısı ile çıktı sayısı ve girdi değeri toplamı ile çıktı değeri toplamı daima aynıdır, işlem ücreti sıfırdır.

4. **ÖzelGönderim'e Giden İşlemler:** Elindeki coini anonimleştirmek isteyen kullanıcının bu coinleri ÖzelGönderim makenizmasına girdirdiği işlemdir. İşlem ücreti sıfırdan büyüktür. Bu işlemleri tespit etmek çıktı adreslerin çıktı değerlerine bakılır. Eğer 2 ya da daha fazla 1.00001 sayısına bölünen çıktı adresi değeri varsa bu işlem ÖzelGönderim'e Giden İşlemdir. Zcashteki t-z işlemlerine benzerler.

5. **ÖzelGönderim'den Çıkan İşlemler:** ÖzelGönderim'e Giden İşlemlerin aksine anonimleşen coinlerin sahipleri tarafından harcanmak vs. gibi sebeplerle geri cüzdanlarına ödendiği işlemlerdir. İşlem ücreti sıfırdan büyüktür. Bu işlemleri tespit etmek için bu sefer girdi adreslerin girdi değerlerine bakılır. Eğer 2 ya da daha



Şekil 3.7: En Çok Kullanılan 1,000,000 Adres Çıktısı



Şekil 3.8: En Çok Kullanılan 1,000,000 Adres Çıktısı

fazla 1.00001 sayısına bölünen girdi adresi değeri varsa bu işlem ÖzelGönderim'den Çıkan İşlemdir. Zcashteki z'den t'ye işlemlere benzer.

İşlem tiplerinin iki farklı şekilde zamana göre grafikleri verilmiştir. Şekil 3.7'de Dash'in ilk çıktığı 2014 yılından 1260895. bloğa kadar tüm bloklarının işlem tipi grafiği ve Şekil 3.8'de 2019 ile 2020 yılları içinde 01 Ocak 2019'daki ilk bloktan yine 1260895. bloğa

Tablo 3.4: Tiplere Göre Dash İşlemleri Sayıları

Dash Blokzinciri İşlem Tipi	Toplam İşlem Sayısı	Toplam İşlem Sayısı Yüzdesi
ÖzelGönderim'e Giden	493818	1.976501384
ÖzelGönderim'den Gelen	147193	0.589138444
ÖzelGönderim	2305085	9.226078621
Normal	20732384	82.98115028
Blok Ödülü	1305970	5.227131276
TOPLAM	24984450	100.00

Tablo 3.5: Son 25,000 Blok İçin Tiplere Göre Dash İşlemleri Sayıları

Dash Blokzinciri İşlem Tipi	Toplam İşlem Sayısı	Toplam İşlem Sayısı Yüzdesi
ÖzelGönderim'e Giden	23558	0.890872471
ÖzelGönderim'den Gelen	6336	0.239603021
ÖzelGönderim	150101	5.676239443
Normal	2436524	92.13991667
Blok Ödülü	27855	1.053368396
TOPLAM	2644374	

kadar yine tüm blokların aylara göre işlem tipi grafiği gösterilmiştir. Bu grafiklerden de anlaşılacağı üzere Dash kullanıcıları büyük çoğunlukla normal işlemleri yapmayı tercih etmektedir. Tablo 3.4 tablosunda Şekil 3.7'de gösterilmekte olan ilk bloktan 1260895. bloğa kadar yapılan tüm işlemlerin sayısı verilmektedir. ÖzelGönderim ile alakalı işlemlerin "toplamının" tüm işlemlere oranı %11.79 etmektedir. Bu değer doğrudan ÖzelGönderim işlemi en az 2 seferde (16 sefere kadar da çıkabilmektedir) yapılmasına rağmen Dash kullanıcılarının istenilen ve beklenen seviyede ÖzelGönderim özelliğini pek de kullanmadığını gösterir.

Dash için de yapılan işlem analizi daha efektif ve hızlı sonuçlar vermesi adına son 25,000 blok için yapılmıştır. Tablo 3.5'te son 25,000 blok için işlem tipi sayıları verilmiştir. Bu son 25,000 blokta ÖzelGönderim ile alakalı işlemler toplamda 179995 işlemle %6,81 oranına gerilemiştir. Analiz çalışmasının yapılacağı toplam işlem (ÖzelGönderim'e giden ve ÖzelGönderim'den gelen işlemler) sayısıysa tüm işlemler sayısının %1.13'üne tekabül eden 29894 tane işlemdir.

3.2.1 Madencilerin Analizi

Zcash'ten farklı olarak Dash kriptoparasında blok ödülleri madencilerle beraber AnaUçlara da gönderilir. Ancak hangi adresin AnaUç'a yahut madenciye ait olup olmadığını bilmek mümkün değildir. Bu nedenle madenci analizine mecburen AnaUçlar da eklenmişitr. Madenci havuzlarını ve yaptıkları anonim işlemleri tespit etmek için Zcash'te olduğu gibi yine bünyesinde bulundurdukları madencilere yaptıkları ödemelere göre analiz yapılmıştır.

Tablo 3.6: Dash Muhtemel TMadenciler

M.Havuz Adresleri	Değeri	#İşlem	TMadenci Adresleri	Değeri	#İşlem
HavuzGrubu_1	852530786	6	TMadenci_1	852476979	1
HavuzGrubu_2	10899071	6	TMadenci_2	10840118	1

Madenci havuzu coinleri "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 bahsedildiği gibi varsayılmıştır. Daha sonra bu adreslerden yine aynı 25,000 bloğu içerisinde ÖzelGönderim'e Giden İşlemlerde girdi adresi olanlar tespit edilir. Ödülü alan olası madenci havuzlarının tespitinden sonra sıra ödülü madencilere dağıtan TMadencilerle ZMadencileri tespit etmeye gelir. Bu işlem Zcash'de uygulanan algoritmaya benzer bir algoritmayla gerçekleştirilir. İşlemler sonucunda çıkan sonuç Tablo 3.6'daki gibidir.

Tablo 3.6'da TMadenci olarak tespit edilen kayıtlar gösterilmektedir. ZMadenci olaraksa hiçbir kayıt bulunamamamıştır. Toplamda bulunan 14 işlem son 25,000 bloktaki analiz edilecek işlem sayısının %0.468321402 kadarına denk düşmektedir. Bu nedenle madenci analizi işlemleri Dash için maalesef gözardı edilecektir.

3.2.2 Gidiş-Geliş İşlemleri

Gidiş-Geliş işlemleri Dash kriptoparası için "t" zamanında gerçekleşmiş bir ÖzelGönderim'e Giden İşlemle (bundan sonra "ÖGG işlemi" denecektir) "$t+t_1$" zamanında gerçekleşmiş ÖzelGönderim'den Çıkan İşlemin (bundan sonra "ÖGÇ işlemi" denecektir) 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.

Ancak Zcash'ten farklı olarak coin miktarı hesaplanırken ilgili işlemin tüm girdi değerleri toplamı yahut tüm çıktı değerleri toplamı için coin miktarı değil ÖzelGönderim'e dahil olan adreslerin toplam değerlerinin coin miktarı alınıp karşılaştırma algoritmasına dahil edilir. Bunun nedeni bir ÖzelGönderim işlemi yapılacak iken ÖzelGönderim'e dahil edilmeyen işlemler bu işlemi yapan adrese geri döner; dolayısıyla bu işlemin dahil edilmesi durumunda yapılacak karşılaştırmanın hatalı olması ihtimali doğmaktadır. Örnek vermek gerekirse mesela 23,191222 Dashi olan bir kullanıcı 22,000022 Dashini ÖzelGönderim işlemi yapmak için kullanırken kalan 1,1912 Dash kendi adresine geri ödeyecektir. Bu nedenle 1,1912 Dash'e sahip olan adres analize eklenmez.

3.2.2.1 Temel Karşılaştırma

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

Karşılaştırma işlemi sonrasında toplamda 8795 farklı işlemin listeye girdiği gözlemlenmiştir. Liste incelendiği zaman bazı coin 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.

3.2.2.2 Alt-küme Toplamlarının Karşılaştırılması

Diğer bir gidiş-geliş işlemleri karşılaştırması olan "Alt-küme Toplamlarının Karşılaştırılması" şu şekilde yapılır; "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 olanlar listeye eklenir.

Karşılaştırma sonucunda toplamda 10417 farklı işlemin listeye girdiği gözlemlenmiştir. İlk gidiş-geliş işlemleri karşılaştırılması listesinde olduğu gibi bu listede de aynı coin 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 baz alınarak bu liste gruplandırılır. Yine aynı işlemin 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.

Temel karşılaştırmada çıkan sonuçlarla alt-küme toplamlarının karşılaştırılmasında çıkan sonuç listeleri yanyana getirildiğinde göze birkaç durum çarpmaktadır. Bunlardan ilki alt-küme toplamlarının karşılaştırılmasında doğal olarak çok daha fazla "ilişkisi olma ihtimali" olan işlem bulunmaktadır. İkincisiyse temel karşılaştırmada gruplanan işlemlerin

Tablo 3.7: Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu

Grup	TK #	Yüzde	AKTK #	Yüzde	Toplam #	Yüzde
Sadece 1 Kez	76	%0.254	7832	%26.199	7833	%26.202
7 ve Altı	510	%1.706	9954	%33.298	9971	%33.354
25 ve Altı	1400	%4.683	10183	%34.064	10387	%34.746
100 ve Altı	4427	%14.808	10392	%34.763	11698	%39.131
Gruplama Yok	8795	%29.421	10417	%34.846	14739	%49.304

listede geçme sayısı azaldıkça toplam işlem sayısı çok hızlı bir şekilde azalmaktayken alt-küme toplamlarının karşılaştırılmasında bu azalma oranı çok daha azdır.

Her iki listenden çıkan sonuçlar Tablo 3.7'deki gibidir.

Tablo 3.7'de TK # ifadesi temel karşılaştırma için gruplandırılmış toplam işlem sayısını, AKTK # ifadesi de alt-küme toplamlarının karşılaştırılmasındaki gruplandırılmış toplam işlem sayısını verir. Toplam # ifadesi de bu iki gruplandırmadaki işlem sayılarının toplanıp tekrar gruplanmış halini verir. Mesela sadece 1 kez geçen TK işlemleri toplamı 76 ve AKTK işlemleri toplamı 7832'dir. Bu iki gruplanmış işlem sayıları toplamı normalde 7908 olması gerekirken 7833 olarak hesaplanmıştır. Bunun temel nedeni TK sonuç listesinde bulunan işlemler AKTK analizinde özellikle çıkartılmamışlardır; bu nedenle aynı işlemler iki farklı sonuç listesinde de görünebilmektedirler.

Tablo 3.7'de ilk olarak her iki listede sadece bir kez karşılaştırma 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 son da listede bulunan tüm işlemlerin sayısı verilmiştir. Her bir sayının yanındaki "Yüzde" olarak belirtilen alan ÖGG ve ÖGÇ işlemlerin toplamı olan 29894 sayısına göre o sayının yüzdesini verir.

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. Yapılan ilişkilendirmenin geçerliliği ÖzelGönderim'den çıkan işlemde olan tüm karıştırmalardaki adreslerden geriye giderek anlaşılabilir. Mesela X_1 ÖGG işlemi ve X_2 de ÖGÇ işlem olsun. Listede bu iki işlem arasında ilişki olması ihtimalinin belirtilmesi sonrasında X_2 işlemine girdi olan X_{a_1}, X_{b_1}, X_{c_1} şeklindeki tüm adreslere bakılır. Daha sonra bunların çıktısı olduğu ÖzelGönderim işlemlerinde bulunan tüm işlemlerin $X_{a_{a1}}$, $X_{b_{a2}}$, $X_{c_{a3}}$, $X_{a_{b1}}$, $X_{b_{b2}}$, $X_{c_{b3}}$, $X_{a_{c1}}$, $X_{b_{c2}}$, $X_{c_{c3}}$, şeklindeki girdi adreslerine gidilir. Her bir geriye gidilen seferin bir önceki muhtemel ilişki yolu sayısıyla mevcut ÖzelGönderim işleminin girdi adresi sayısı çarpılır (bahsedilen tüm ÖzelGönderim işlemlerinde tam olarak 3 tane karıştırma adresinin kullanıldığı varsayılırsa ilk ÖzelGönderim işleminde 3 ilişki ihtimali varken ikincisinde 9, üçüncüsünde 27 ve dördüncüsünde 81 ilişki ihtimali

Tablo 3.8: Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu

Grup	TK #	Yüzde	AKTK #	Yüzde	Toplam #	Yüzde
Sadece 1 Kez	41	%0.137	3187	%10.661	3201	%10.708
7 ve Altı	289	%0.967	6160	%20.606	6188	%20.700
25 ve Altı	843	%2.820	6992	%23.389	7216	%24.139
100 ve Altı	2743	%9.176	7280	%24.353	8417	%28.156
Gruplama Yok	4861	%16.261	7607	%25.447	10688	%35.753

olacaktır). Yapılan sefer sayısı arttıkça ilişkilendirmeyi doğrulamanın zorluğu 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 işlem ile ÖGÇ işlem arasındaki ilişkiyi körlemesine bir yöntemle bulmaktan daha kolay olacaktır. Bu durum şu şekilde düşünülebilir; Kaba Kuvvet (Brute Force) kullanarak bir şifreleme algoritmasını kırabilmek için m * n * t birim zaman kadar sürüyorken bu süreyi n kadar azaltarak m * t birim zaman kadar süreye düşürmek algoritmanın tamamen daha kolay kırılmasına olanak sağlayacaktır. Yapılan analiz çalışması sayesinde bir Dash işleminin x * y * z sayıda Dash işlemiyle olabilecek olası ilişki sayısı x * y sayıda Dash işlemine, hatta belki de x sayıda Dash işlemine düşürülmüştür.

Yapılan karşılaştırmalardaki doğrulamayı kolaylaştırmanın bir yöntemi daha vardır. Yukarıdaki tabloda sadece ÖGG işlem ile ÖGÇ işlem arasındaki ilgili girdi ve çıktı adreslerinin değerlerinin toplamları karşılaştırılmıştır. Bu karşılaştırmaya ÖGG'nin çıktı adresi sayısıyla ÖGÇ'nin girdi adresi sayısı eklendiği zaman bu iki işlem arasında bir "ilişki" daha doğmuş olacaktır. Şöyle ki; Xt_1 işlemi ÖGG işlemi ve Xt_2 işlemi ÖGÇ işlemi olarak düşünülsün. Xt_1 işleminin çıktı adresi sayısının 12 olması durumunda sadece girdi adresi sayısı 12 olan ÖGÇ işlemlerinin girdi değeri toplamlarına bakılacaktır. Xt_2 işleminde de 12 girdi olması ve bu işlemin Xt_1 işlemiyle aynı değere sahip olmasından mütevellit bu iki işlem arasında daha güçlü bir ilişkinin var olması ihtimali bulunur.

Adres sayılarının eş olması koşulunun karşılaştırma analizine eklenmesiyle çıkan sonuçlar Tablo 3.8'de gösterilmişlerdir.

İşlemdeki adres sayılarının karşılaştırmaya dahil edilmesiyle gelen sonuçlar neredeyse yarı yarıya düşmüştür. Her ne kadar toplamdaki bulunan işlem sayısı azalmış olsa da, toplam girdi-çıktı adresi sayılarına da bakılacağından ötürü doğrulama için ÖzelGönderim işlemlerinde geriye giderken bakılması gereken işlem sayısı azalmış olacaktır. Gidiş-geliş işlemlerinin karşılaştırmasına girdi ve çıktı adreslerinin toplamlarının eşit olması koşulunun eklenmesinin temel sebebi karıştırmaya gönderilen değer ile aynı değeri çekebilmek için toplam miktarın birebir eşit olması gibi toplam adres sayılarının da eşit olması

gerekmektedir. Şöyle bir örnekle daha iyi anlaşılacaktır: Xt_1 ÖGG işlem olsun. Xt_1 işlemi 34.7 Dash'i karıştırmak için ÖzelGönderim'e gönderdiği zaman 3 x 10 Dash, 4 x 1 Dash ve 7 x 0.1 Dash olmak üzere toplamda 14 farklı adres üzerinden karıştırma yapması gerekmektedir. Bu karıştırmalar sonrası misal olarak 4. seferin sonunda karıştma işlemi bittiğinde karıştırılan Dash'leri ilgili kullanıcı ikinci bir Xt_2 adresinde harcamak için toplamak istediğinde karıştırılan Dashlerin tamamını 14 farklı adresten çekmesi gerekir. Çünkü ÖzelGönderim seferleri öncesinde bir kez 10'un katsayılarına bölme işlemi olduğu takdirde AnaUçlar bu değerleri bir daha 10'un katsayılarına bölmez. Bu sebeple 14 farklı adrese 3 x 10 Dash, 4 x 1 Dash ve 7 x 0.1 Dash olacak şekilde bölünen değer tekrar harcanmak için bir adrese ödenmek (yahut bir adreste toplanmak) istendiğinde yine 3 x 10 Dash, 4 x 1 Dash ve 7 x 0.1 Dash olarak Xt_2 işleminde girdi olmak zorundadır. Bu şekilde ÖzelGönderim kullanıldığı takdirde örnekten de anlaşılacağı üzere ÖzelGönderim'e giren işlemle ÖzelGönderim'den çıkan işlem arasında bir şekilde ilişki doğmuş olur. Xt_2 işleminde girdi olan 14 adresten yola çıkarak bir şekilde Xt_1 işleminin tüm 14 çıktı adresine erişilebiliyorsa Xt_1 ve Xt_2 işlemlerini aynı kullanıcı yapmış ve Xt_1 işleminin girdi adresiyle Xt_2 işleminin çıktı adresi aynı kullanıcıya aittir denilebilecektir. Bu şekilde hangi adreslerin hangi kullanıcılara ait olduğunun anlaşılmasıyla adreslerin kullanıcı bazlı gruplandırılabilmesi sağlanacaktır. Bir kullanıcıya ait farklı adreslerin anlaşılması gizlilik ve anonimlik isteyen kullanıcılar için oldukça elzem sonuçları beraberinde getirir.

3.2.2.3 Parmak İzi Değerleri Karşılaştırması

ÖzelGönderim'e girebilecek en küçük değer 0.001 Dash olduğundan ve bu değer de varsayılan işlem ücretinden büyük olduğundan da madencilerin tespit edildiği analiz algoritmasında olduğu gibi parmak izi gidiş-geliş işlemleri analizi de maalesef Dash için yapılmayacaktır.

Bölüm 4

Sonuçlar ve Tartışma

Bölüm 2'de kısaca Bitcoin kriptoparası detaylıca anlatılmıştır. Yine bu bölümde bahsedildiği gibi, her ne kadar çıktığı ilk zamanlarda birçok kesim tarafından tamamıyla anonimlik ve mahremiyet sağladığı düşünülse de zaman içerisinde yaşanan çeşitli olaylar (Silkroad marketi vakasında FBI ajanının alakalı işlemleri izlemesi gibi) Bitcoin'in hiç de düşünüldüğü gibi anonim olmadığını anlaşılmıştır. Bu nedenle zaman içerisinde Kısım 2.4'te anlatıldığı gibi anonimliğe odaklananan çeşitli "anonim kriptoparalar" yayınlanmıştır. Şekil 2.16'da bu anonim kriptoparaların yayınlanmasıyla alakalı kısa bir tarihçe verilmiştir.

Ne var ki, teoride kullandıkları şifreleme yöntemleri, karıştırma mekanizmaları yahut işin ispatlarıyla ciddi manada anonimlik sağladığı düşünülen anonim kriptopalar pratikte düşünüldüğü kadar anonimlik sağlamadığı görülmüştür. Bölüm 3'de anonim kriptopara olan Zcash ve Dash için analiz çalışmaları yapılmıştır. Bu çalışmalardan elde edilen çıktılar aşağıdaki kısımlar anlatılmışlardır.

4.0.1 Zcash Analizi Sonuçları

Zcash analizi dahilinde detaylı bir şekilde anlatılmış olan analiz işlemlerinin sonucunda son Zcash için 25,000 bloktaki toplam 7,961 işlemde 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 T-Madenci şartlarına uyan z-t işlemi ve 23 Z-Madenci 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 yapılmış yani takip edilememezliği ihlal edildiği görülür.

Elde edilen bu analiz sonuçlarından aşağıdaki bilgiler çıkartılabilir:

- Şekil 3.1'de grafik incelendiğinde Zcash kullanıcılarının Zcash'in anonim işlemlerini olması gerektiği seviyelerde tercih etmedikleri gözlemlenmiştir.
- Şekil 3.2'de JS-işlemleri grafiğinde korumalı havuzda işlemlerin takip edilememesini daha büyük oranda sağlayabilecek z-z korumalı işlemlerin de yeterince kullanılmadığı görülmektedir. Özellikle 2019 yılından sonra gözlemlenen artışın ise bazı madenci havuzlarının kendi madencilerine blok ödüllerini gizli adresten yapma kararının etkili olduğu söylenebilir.
- Zcash'te yapılan işlemlerin önemli bir kısmını madenci havuzlarının yapmış olduğu işlemler kapsar. JS-işlemlerinde bu oran, alınan blok ödülünün genellikle korumalı havuza konulmasından ötürü artar. z-z korumalı işlemlerinin ne derece madenci havuzları tarafından gerçekleştirildiğini bilmek pek de mümkün değildir.
- Zcash madenci havuzlarını, bünyelerinde madencilere yaptığı ödemelere göre üç farklı tipe ayrılırlar. t-t şeffaf işlemleriyle ödeme yapan TMadencilerle ve z-t işlemleri ile ödeme yapan ZMadenci tipindeki madenci havuzları için analiz yapılmıştır, ancak z-z işlemlerinde ödeme yapanları analiz etmek mevcut yöntemlerle mümkün değildir. Yapılan analizlerde JS-işlemlerinin %36.2'sinin madenci havuzları ile ilişkilendirilebilmiştir.
- Madenci havuzları haricindeki JS-işlemlerinin analizi için kalan t-z işleminin girdisiyle z-t işleminin çıktısı karşılaştırılır. Değerlerin eş olması durumuna arada bir ilişki olduğu düşünülebilir. Bu tür işlemleri gidiş-geliş işlemleri denir. Gidiş-geliş işlemleri tüm JS-işlemlerinin %21.1'ini tekabül eder.
- Yapılan analiz işlemlerinin sonuucunda tüm JS-işlemlerinin %57.3'ü ilişkilendirilebilmiştir. JS-işlemlerinde analiz yapılması mümkün olmayan %24,6 oranına sahip z-z korumalı işlemlerini çıkartıldığında kalan analiz edilebilen JS-işlemlerinin %84.4'ü ilişkilendirilmiş olur.
- Zcash kullanıcıları korumalı havuzu kullanıp z-z işlemleri kullanırken dikkat etmeleri gereken hususlara dikkat etmedikleri yahut hiç z-z işlemlerini kullanmadıkları için JS-işlemlerinin yarısından fazlası ilişkilendirilebilmiştir. Bu nedenle Zcash geliştiricilerinin korumalı havuzun kullanımı sırasında kullanıcılarına korumalı havuza girilen t-z işlemiyle korumalı havuzdan çıktıkları z-t işleminde aynı değerleri kullanmamalarını sağlayacak çeşitli koşullar koymaları daha doğru olacaktır.

- Sonuç olarak Zcash kriptografik olarak teoride gerçekten bir anonimlik sağlamış olsa da pratikte istenilen derecede anonimlik, mahremiyet ve takip edilememezlik sağlayamamaktadır.

4.0.2 Dash Analizi Sonuçları

Dash'de yapılan ÖzelGönderim işlemlerini her ne kadar teoride de pratikte de alakası olmamasıyla birlikte yapılan analiz çalışması açısından bakıldığında Zcash'teki z-z korumalı işlemlere benzetmek mümkündür. z-z işlemleri sayesinde yapılan JS-işlemlerinin takip edilememezliği ciddi bir şekilde artmaktadır. Aynı şekilde ÖzelGönderim işlemleri sayesinde de Dash işlemlerinin genel olarak takip edilememzliği artmaktadır. Yapılan analiz açısından bakıldığından z-z işlemlerini analiz etmek mümkün olmadığı gibi, doğrudan ÖzelGönderim işlemlerini analiz etmek hem etkili değildir hem de adres değerleri hep 10'un katsayısı olduğundan bu işlemleri de analiz etmek mümkün değildir. Bu nedenle ÖzelGönderim'e giren ve ÖzelGönderim'den çıkan işlemler analiz edilmiştir.

Daha sonradan katılan adres sayıları dâhil edilmeden yapılan ilk analiz çalışmasında tüm ÖzelGönderim'e giden ve ÖzelGönderim'den gelen işlemlerin %49.304'ü için ilişkilendirilme yapılmıştır. Analize işlem sayılarının eşit olması koşulu konulduğu vakit bu oran %35.753'e düşmektedir. Yapılan ilişkilendirmeler "ÖGG Xt1 ve ÖGÇ Xt2 işlemlerinin adres sayıları ve işlem değerleri birbirine eşittir; bu nedenle aralarında bir ilişki olması muhtemeldir." varsayımı temel alınarak yapılmıştır. Bu ilişkinin doğrulaması tez konusu kapsamında olmadığı için detaylıca açıklanmamıştır. Dash kriptoparası tamamıyla umumi yani herkese açık bir kriptopara olduğundan mütevellit, ilişkilendirmenin doğru olmasını kontrol etmek amacıyla ÖGÇ Xt2 işleminden tüm ÖzelGönderim adresleri kullanılarak geriye doğru gitmek yeterli olacaktır.

Dash analizinden şu sonuçlar çıkar:

- Şekil 3.7 ve Şekil 3.8'de görüldüğü gibi Dash kullanıcıları ÖzelGönderim işlemlerini Zcash'te olduğu gibi çok fazla tercih etmemektedirler. Bu nedenle Dash işlemlerinin büyük çoğunluğu (%90.88) ÖzelGönderim ile alakası olmayan işlemlerdir.
- Yapılacak olan analiz işleminde kolaylık sağlamak adına ÖzelGönderim harici işlemler dörde bölünmüştür. Bunlardan ÖzelGönderim'e giden (analiz açısından bir nevi Zcash'teki t-z işlemi) ve ÖzelGönderim'den gelen işlemler (yine analiz açısından bir nevi Zcash'teki z-t işlemi) analiz edilmiştir.
- Madenci havuzlarının Zcash'te olduğu gibi blok ödülünü ilk önce ÖzelGönderim karıştırmasına girdirip daha sonra ödeme yaptığı durumlarla çok fazla karşılaşılmamıştır. Bu nedenle madenci havuzları analiz edilememiştir.

- Gidiş-geliş işlemleri ilk olarak sadece 10'un katsayısına bölünen adreslerin toplam değerlerinin karşılaştırması temel alınarak yapılmıştır. Bu durumda işlemlerin %49.304'unda bir ilişki olması ihtimali tespit edilmiştir.

- Gidiş-geliş işlemleri daha sonra 10'un katsayısına bölünen adreslerin toplam adres sayılarının eşit olması şartı eklenerek analiz edilmiştir. İlişki olması ihtimali olan işlemlerin sayısı bu durumda %35.753'e düşmüştür.

- Dash kullanıcıları ÖzelGönderim karıştırmasına ellerinde bulundurdukları Dash'leri soktuklarında bu Dash'ler 10'un katsayılarına bölünür. 2 ile 16 karıştırma seferi sonrası ÖzelGönderim karıştırma işlemi son bulur. Kullanıcılar karıştırmaya girdikleri miktarı tek bir adreste toplayıp bu coinleri kullanmaya karar verdikleri zaman son yaptıkları bu işlemle ÖzelGönderim karıştırması öncesindeki coinlerinin katsayılara bölündüğü işlem arasında bir ilişki kurabilme imkanı doğmuş olur.

- Yapılan analizler sonucunda ÖzelGönderim öncesi ve sonrası yapılan işlemlerde bir ilişki kurabilme imkanı doğmuştur. Dash kriptoparası tamamıyla şeffaf ve umumi yani açık bir kriptopara olduğundan dolayı ÖzelGönderim işlemleri üzerinden iki işlem arasındaki ilişkinin gerçekten var olduğunu doğrulamak da mümkün olacaktır. Bu nedenle Dash kriptoparasının teoiride anonim bir kriptopara olmasıyla beraber pratikte çeşitli sebeplerden düşünüldüğü kadar anonimlik ve mahremiyet sağlamadığı gözlemlenmiştir.

4.1 Diğer Analiz Sonuçları

Bu tez içerisinde anonim kriptoparaların işlemleri arasında aktarılan coin miktarı (ve Dash için adres sayısı bakımından) karşılaştırma yapılarak işlemler arasında bir ilişki kurulmaya çalışılmıştır. Muhtemel bir ilişki kurulması anonimliğin şartları olan gizlilik, takip edilememezlik ve hatta birbirleriyle değiştirilebilirliğin ihlal edilmesine neden olacaktır. Bunun yanında anonim kriptoparalardaki "anonimliği sağlayan özelliklerin" ne derece mahremiyet sağladığını öğrenebilmek için çeşitli başka analiz yöntemleri de bulunmaktadır.

İlk olarak [47] makalesinde Jong-Hyouk Lee, kısaca Bitcoin ve anonimliğinden bahsedip daha sonra Dash, Monero, Verge, Zcash ve PIVX anonim kriptoparalarından bahsetmiştir. Daha sonra anonim özelliklerinden ve bu özelliklerin artılarından ve eksilerinden bahsetmiştir. Son olarak kriptoparalarda anonimlik özelliğinin bedava olmayıp genellikle yüksek bir bedel karşılığında sağlandığını söylemiştir. Bahsedilen bu durum, bu tez çalışmasında da tespit edildiği gibi neden Zcash ve Dash için kullanıcılarının anonimlik özelliğini tercih etmediklerinin daha iyi anlaşılmasını sağlar. Makalenin sonunda anonimlik için kriptografik çözümler sunan Zcash ve Monero'nun tam olarak anonimlik sağladığından

bahseder. Ne var ki bu tez çalışmasında Zcash ve Dash anonim kriptoparaları için pratikte pek de öyle olmadığı çıkan sonuçlarda gözlemlenmiştir.

Alex Birkuyov [32] makalesinde Bitcoin için ağ trafiği analizi çalışması yapmıştır. Bitcoin işlemlerinin mesajlarının zamanlamasının bilgi sızdırdığı ve bu açıktan iyi bağlantıya sahip kötü niyetli düğümlerin faydanalabileceği (exploiting) belirtilmiştir. Yapılan çalışmada Birkuyov, Bitcoin'in testnetinde yapılan işlemlerin tamamının anonimsizleştirildiğini söyler. Bitcoin ve benzeri kriptopalar eşler arası ağı mesaj yaymak için kullanırlar.

Bitcoin'de mesaj iletiminde üç önemli özellik bulunmaktadır:

1. Adres İletimi (Address Propagation)
2. İşlem İletimi (Transaction Propagation)
3. Rastgeleleştirme (Randomization)

Ağ analizindeki temel hedef işlemleri onları kimin ağa ilk tanıttığına, yani işlemlerle alakalı olarak Bitcoin ağına kimin ilk mesajı yolladığına bağlı olarak gruplamaktır. İlk olarak önsezi (intuition) yapılır, daha sonra veri toplanıp sunulur. Yapılan analizde ikinci aşamada gruplamanın kalitesiyle anonimsizleştirmenin derecesi değerlendirilir. Daha sonra makalede bahsedildiği gibi 8 adımda deneyler yapılıp deney sonuçları üzerinden değerlendirme yapılır.

Birkuyov, [33] makalesinde yine [32] makalesinde yapmış olduğu ağ analizi çalışmasının Bitcoin üzerinde ziyade anonim kriptoparalar olan Zcash, Dash ve Monero kriptoparaları üzerinde yapar. Analizin yaklaşımı yukarıda bahsedilen [32] makalesindeki yaklaşımın aynısıdır. Analiz aşamaları önsezi, veri toplama, kalitenin değerlendirilmesi, deneyler şeklinde gider. Diğer makaleye ek olarak görselleştirme (visualization) ve ayrıca değerlendirme (evaluation) yapılır. Her iki makalede de bu yaklaşım ve yöntemler detaylıca anlatılmıştır.

[56] makalesinde Nathan Borggren ve çalışma arkadaşları Monero ağında işlem değerleri ve takip edilebilirliği "makine öğrenme (machine learning)" yöntemleriyle blokzincirler simüle edilerek analiz etmiştir. Makalede Borggren kısaca Monero blokzincirini simüle eder, Monero blokzinciri örneklendirilir (featurizing) ve üç farklı makine öğrenme işlemleri yapılır:

1. Sahte ve gerçek işlemlerin makine öğrenmesi: cüzdan analizi gibi analizler vasıtasıyla halka imzadaki asıl imzalayan bulunur.

2. Kullanıcı kimliği ve grup üyeliği makine öğrenmesi: Sınıfladırma için sinir ağları (neural networks) rastgele orman (random forest) yöntemi kullanılır.

3. İşlem değeri makine öğrenmesi: Değer regresyon görevi (value regression task) için model performansı R^2 katsayısıdır (R^2 coefficient).

Yukarıdaki işlemlerin yanında aynı zamanda gerçek Monero ağında makine öğrenmesi yapılır. Son olarak makine öğrenme sonuçları değerlendirilir ve bir sonuç çıkartılır.

Yukarıdaki analizlerin yanında Alex Biryukov [34] makalesinde çeşitli kriptoparalarda madencilerin davranışlarıyla çeşitli farklı madenci tipleri analiz edilmiştir. Madencilerden GPU ve ASIC olarak gruplandırılan madenciler analiz edilmiş, madenci merkezileştirme ve madencilerin gizliliği konularına değinilmiştir.

Bu analiz örneklerine son olarak yine Alex Biryukov ve makalelerinin bir çoğunda kendisine eşlik eden Sergei Tikhomirov [35] makalesinde Bitcoin, Dash, Monero, ve Zcash için mobil cüzdanlardaki güvenlik ve mahremiyet analizi gerçekleştirilmiştir. İlgili kriptoparalar için kullanılan 23 farklı mobil cüzdanın analiz edilebilmesi için ilk olarak gizlilik ve mahremiyet kriterleri belirlenmiş ve tüm bu mobil cüzdanlar için bu kripterlere ne derece uyulduğu elle yapılan kontroller, statik analiz, işlem kümelendirme, Javascript XSS vb. saldırılar ve uygulama açıkları kullanılarak kontrol edilmiştir. Daha sonra [33] ve [32] makalelerinde bahsedilmiş olan ağ analizi aşamaları mobil cüzdanlar için de yapılmıştır. Ağ analizinde de bahsedilen "deneyler" de yapıldıktan sonra sonuçlar karşılaştırılmış ve netice olarak birçok mobil cüzdanın hiçbir şekilde istenilen kriterleri sağlamadığı sonucu ortaya çıkmıştır. Analiz çalışmasında çıkan belki de en önemli sonuç, anonim kriptoparalar blokzincir analizini engellemek adına sofistike ve karmaşık algoritmalarla klriptografik çözümler üretirken ağ analizi yapıldığında Bitcoin kriptoparasından neredeyse bir farkının olmadığıdır.

4.1.1 Monero Analizi

2.4.3. alt-kısmında anlatıldığı gibi Monero da oldukça popüler anonim bir kriptoparadır ve bir iddiaya göre Bitcoin'den sonra en önemli ilk 10 kriptoparadan birisidir[1]. Ayrıca çeşitli forumlarda kara web yahut derin web (dark web or deep web) denilen ve daha çok suç odaklı olduğu düşünülen internet ortamında en çok sevilen ve kullanılan kriptopara olarak addedilir.

Ne var ki, dikkat edildiği gibi Monero kriptoparası için bu tez kapsamında bir analiz çalışması yapılmamıştır. Bunun temel nedeni şudur; yapılan olan tez çalışması farklı zamanlarda yani farklı bloklarda gerçekleştirilmiş olan işlemlerin toplam işlem miktarının birbirleriyle karşılaştırılarak arada bir ilişki bulunmasıdır. Misal vermek gerekirse mesela

[1] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/ web sayfasında bu konu ile alakalı bir yazı kaleme alınmıştır.

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 kriptoparası blok ödülü işlemleri hariç diğer bütün işlemlerde gönderilen ve alınan miktarlar daima gizlidir. Yani yapılan işlemlerde ne kadar XMR gittiğini yahut alındığını bilmek blokzincir kayıt defterine bakılıp anlaşılmaz. İşlemlerde sadece "işlem bedeli" görülebilirdir; ancak işlem bedeli kullanılarak gönderilen ve alınan miktarlara ulaşmak mümkün değildir. Bu nedenle Monero anonim kriptoparası için korelasyon tabanlı mahremiyet analizi yapılamamıştır.

Her ne kadar mevcut tezin kapsamı işlem bedelleri (ve Dash için ayrıca işlemlerdeki adres sayıları) temel alınarak işlemleri ve kullanıcı adreslerini analiz etmek olsa da bu işlemleri analiz etmenin bundan başka yöntemleri de bulunmaktadır. Ayrıca bir önceki kısım olan Kısım 4.1'de anlatıldığı gibi Monero ağı, kullanılan cüzdanlar, madenciler ve madenci havuzları kullanılarak yahut makine öğrenme yöntemlerinden faydanalınarak Monero'yu anonimsizleştirmek mümkündür. Farklı çalışmalarda yapılmış olan bazı anonimsizleştirme çalışmalarından aşağıda kısaca bahsedilmiştir.

Malte Möser [51] makalesinde Monero işlemlerini halkaya giren imzacıları kullanarak analiz etmiştir. Bu işlemi yaparken aşağıdaki iki zayıflıktan yararlanmıştır:

1. Şubat 2017 öncesinde yapılmış olan birçok işlem anlaşılabilir (deducible) işlemleri içermektedir. Bu işlemler kullanılarak işlem geçmişini takip etmek çeşitli analizlerle mümkün olmaktadır. Bu işlemlere sıfır-karıştırmalı işlem (zero-mixin transacation) adı verilir. Yani yapılan işlemde kullanıcı halka imzaya katılması için hiçbir sahte imzayalacı seçimi ayarı yapmadığı için işlemde sadece bir tane adres görülür. Bu adres işlemi gerçekleştiren asıl adrestir.

2. İkinci zayıflık ise karıştırma için kullanılan imzalayıcı adresler gerçek coin harcama davranışının sergilenmediği bir dağıtım mekanizmasından seçilir. Böylece asıl girdiler genellikle bulunabilir.

İlgili zayıflıkları anlattıktan sonra Möser, CyrptoNote protokolünü ve 7 Şubat 2017'ye kadar olan tüm versiyonları inceler. Daha sonra 0-karıştırmalı işlemleri kullanarak 2 ve daha fazla karıştırmalı işlemlerde anlaşılabilir işlemleri tespit edip "zamansal analiz (temporal analysis) ile işlem geçmişi takibi yapar. Analiz sonrası madenciler ve AlphaBay gibi çeşitli Monero kullanıcı gruplarını tanımlandırır (characterizing Monero usage). Analiz sonuçlarına binaen karıştırma imzalayıcılarını gruplama (binned mixing samples) gibi neler yapılabileceği hakkında bilgilendirme yapar.

Monero ile alakalı bir ikinci analiz çalışması [44] makalesinde Abraham Hinteregger ve Bernhard Haslhofer tarafından yapılmıştır. Makales kısaca Monero içinin bilinen ve anonimliğin şartlarından olan "takip edilememzlik" şartına odaklanan analiz yöntemlerinden bahseder ve daha sonra makalede önerilen analiz yöntemi anlatılır:

- Sıfır Karıştırmalıları Kaldırma (Zero Mixin Removal (ZMR)): Bir önceki makalede daha detaylı bahsedilen ve sadece bir tane imzalayıcı adresin olduğu işlemlerdir. Bu işlemlerdeki adreslerin kullanıldığı daha sonraki karıştırma işlemlerinin de anonimliği tehlikeye girmiş olur.
- Kesişim Kaldırma (Intersection Removal (IR)): ZMR analizinin genelleştirilmiş halidir. N tane halka aynı N (karıştırma olmayan (non-mixin)) üyeyi içeriyorsa hangi çıktının hangi halkada harcandığını, yani girdi olarak kullanıldığını bilmek imkansızdır. Ne var ki, bu çıktılar N işlemden birisinde harcandığı için ilgili çıktı harcandı (spent) olarak işaretlenir; böylece daha sonraki tüm işlemlerdeki halkalarda sahte girdi olarak işaretlenebilir. Böylece diğer tüm işlemler için bakılacak olan imzalayıcı çıktı adresi sayısı N-1 olacaktır.
- En Yeni Yaklaşımı Tahmin Et (Guess Newest Heuristic (GNH)): [51] makalesinde yapıldığı gibi Monero'nun eski versiyonlarındaki açıklardan bahsedilir. Her yeni versiyonla bu açıklıkların kapatıldığı anlatılır.
- Çıktı Birleştirme Yaklaşımı (Output Merging Heuristic (OMH)): Bir işlemin farklı girdileri aynı işlemdeki farklı çıktılara referans veriyorsa bu yaklaşıma göre o girdiler gerçek girdilerdir.
- Sert Çatallaşma ve Çarpraz Zincir Analizi: Hinteregger'in makalede kendi yapmış olduğu analizdir. Daha önceki başlıklarda sert çatallaşma anlatılmıştır. Aynı anda 2 farklı madenci aynı bloğu üretmiş olabilir. Bu durumda konsensusu ilk oluşturan madencinin bloğu kabul edilir. Çatallaşma öncesi aynı girdinin iki kez harcanmasını engellemek adına her bir halka bir anahtar imajı (a key image) ile paylaşılır. Çatallaşma sonrası bir coinin iki kez harcandığı gözlemlenirse bunlardan bir tanesi çatallaşmada bulunan girdilerden birisi olurken diğeri (yahut diğerleri) karıştırmada kullanılan girdi olacaktır.

Hinteregger makalesinde daha sonra [51]'nin yapmış olduğu analiz çalışmaları ile beraber kendi makalesinde bahsettiği sert çatallaşma ve çarpraz zincir analizini de yapar. Analizin sonucunda halka boyutu zorunluluğu getirilmeden önce (en az 2 karıştırmalı olmalı - Eylül 2019 öncesi) işlemlerin büyük çoğunluğunun takip edilebildiği gözlemlenmiştir. Daha sonraki versiyonlar için Hinteregger'in yapmış olduğu analiz ise düşünüldüğünden daha az etkili olmuştur. Ancak Hinteregger, çok sayıda işlemin olduğu bir sert çatallaşma olması durumunda analiz sonucunda yine birçok farklı işlemin takip edibileceğini vurgular.

4.2 Tartışma

Önceki kısımlarda defaatle bahsedildiği üzere Bitcoin her ne kadar ilk çıktığında anonim olduğu düşünülse de hiçbir şekilde anonim olmadığı zaman içerisinde anlaşılmış ve anonimlik için çeşitli yöntemler geliştirilmiştir. Bu yöntemler de istenildiği anonimliği sağlamayınca anonim kriptoparalar çıkartılmıştır.

Anonim kriptoparalar teoride tamamıyla yahut büyük ölçüde anonimlik sağladıklarını iddia ederler. Zcash anonimliği sağlamak için kayıt defterinde görünmeyen ve ZEC'lerin toplandığı ikinci bir havuz olan korumalı havuza ZEC tranferi yapan EkleBöl işlemlerini kullanır, bu işlemlerdeki miktar ve adresleri doğrulamak için zk-SNAKRs'ı kullanır. Dash CoinJoin'den türetilmiş ve AnaUçlar tarafından yönetilen ÖzelGönderim işlemlerini kullanarak karıştırma yapar. Monero halka algoritmalarını kullanarak girdi olarak hangi adresin kullanıldığı bilgisini gizlerken bir yandan da çıktı için gizli adresleri kullanır ve gönderilen ve alınan XMR miktarını gizler. Verge ise yapılan işlemlerin IP adreslerini gizlemek için ToR mekanizmasını kullanır. PIVX anonim kriptoparası ise hem AnaUçları hem de Zerocash protokolünü kullanarak çok daha güçlü bir anonimleştirme makenizması kurduğunu belirtir.

Bahsedilen tüm bu anonim kriptoparalar gerçekten de bahsettikleri şekillerde güçlü bir anonimleştirme mekanizması sağlarlar. Ancak işlemlerin yapılması için gerekli olan kriptosistem sadece blokzincir altyapısından ibaret değildir. Anlatılmak istenen mesele şudur; gerçek dünyada bir karşılığı olan yani artık tüm dünya tarafından o ya da bu şekilde "gerçek para" olarak atfedilen kriptoparaların "kriptosistemleri" sadece blokzincir altyapısından oluşmazlar. Her ne kadar blokzincir altyapısı kriptosistem için en önemli yapıtaşı olsa da, ve çoğu zaman ikisinin de aynı şey olduğu düşünülse bile aslında kriptosistemlerin kullanıcı profilleri, ağ yapıları, madenciler, kullanılan yöntemler ve yardımcı uygulamalar gibi farklı öğeleri de bulunmaktadır. Anonimlik sadece blokzincir için düşünülüp buradaki açıklar üzerinde fazla düşünülmediği takdirde gizliliğin ve mahremiyetin ihlal edildiği durumlarla karşılaşılmaktadır. Buna en güzel örnek Birkuyov'un [33] ve [35] makaleleri gösterilebilir. Makalelerin sonucunda kriptosistem ağlarında ve kullanılan mobil cüzdanlarda anonim kriptoparaların Bitcoin'den çok da bir farkı olmadığı belirtilmektedir.

Anonim kriptoparalardaki "anonimlik ihlallerinin" belli başlı nedenleri aşağıdaki şekilde listelenebilir:

- Bilgi güvenliği ve siber güvenlik konulu çeşitli kurslarda, toplantılarda, seminelerde ve derslerde sürekli olarak bir güvenlik altyapısının en zayıf halkasının "insan" olduğu özellikle defalarca vurgulanır. Kriptoparalarda da bu durum maalesef farklı değildir. Zcash ve Dash analizi yapılırken normal kullanıcıların anonim işlemleri

yaparken dikkat etmemeleri; misal vermek gerekirse t_1 zamanında yapmış olduğu X_1 işlemini anonimliği sağlayan mekanizmaya soktuktan sadece saatler sonra t_1+t_i zamanında X_2 işlemini yaparak aynı değerle anonim sistemden 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 görevi üstlenirler; sürekli olarak blokzincire eklenmesi için yeni blok üretirler. Yapılan bu işlem için ilgili kriptopara, bloğunu üreten madenciye önceden belirlenmiş bir ödül (yahut ödülden pay) verir. Bu da gerçek dünyada bir çeşit "kolay para kazanma" yöntemi olarak düşünülmeye başlanmıştır. Zamanla madenciler madenci havuzlarına evrilmiş ve madenci havuzları aldıkları ödülü madencilere paylaştırmaya başlamışlardır. Sonuç olarak madenci ve madenci havuzlarının yaptıkları işlemler blokzincirde ciddi orana sahip olmaya başlamış; bu da madenci havuzları ve madenciler için hususi olarak yapılan anonimsezliştirme yöntemlerinin doğmasına sebep olmuştur. Gerçekten de madenci havuzlar Zcash kriptoparasında olduğu gibi sürekli olarak benzer şekilde madencilere ödeme yaparlar. Sonuç olarak madenci havuzlarının yaptığı işlemler daha kolay analiz edilebilir ve 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 edilememzliğin, dolayısıyla anonimliğin mahremiyetin sağlanması için yeterli olmaz. İşlemlerin bir şekilde korumalı havuzda hiçbir şekilde birleştirilemeyecek şekilde parçalanması gerekmektedir.

- 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.

Yukarıdaki anonimliğin ihlaline sebep olan nedenler bu tez çalışmasında yapılan analize binaen çıkan sonuçlardan yola çıkarak gözlemlenmiş nedenlerdir. Bunun haricinde yukarıdaki diğer analiz çalışmalarında anonimliğin ihlaline neden olan/olabilecek sebepler şu şekilde listelenebilir:

- Monero kriptoparasında özellikle 2017 öncesi 0-karıştırıcılı işlemler 2 yahut daha fazla karıştırıcıya sahip işlemlerin çok daha kolay analiz edilmesine neden olmaktadırlar. Neyse ki Monero bu açığı Şubat 2017'de karıştırma sayısını asgari sayı getirerek önüne geçmiştir. Mevcut durumda bu halka imzalayıcı sayısı 11'dir.

- [47] makalesine göre anonim kriptoparalar olması gerektiğinden pahalıdır. Bu da kullanıcıların çok fazla tercih etmemesine sebep olmaktadır. Ayrıca kullanılması normal işlemlere göre (mecburen) "normal kullanıcılar" için daha zordur.

- Kriptosistemdeki ağın kendisi ve ağ trafiği analiz edilebilmektedir. Özellikle yapılan işlemler için kripto-ağa gönderilen istek ve çağrılar çeşitli şekillerde bilgi sızdırabilmektedirler.

- Kullanıcıların kullandığı özellikle mobil cüzdanlar çeşitli şekillerde bilgi sızdırabilmektedirler.

- Kriptosistemde bulunan öğelerin işlem logları bilgi sızdırabilmektedirler. Misal olarak, Dash kriptoparasındaki AnaUçların işlem loglarından yola çıkılarak Özel-Gönderim işlemleri takip edilebildiği belirtilmiştir [2].

- Kötü niyetli düğümlerin çoğunluğu yani konsensusu ele geçirmesi ilgili kriptoparanın tamamıyla ele geçirilmesine sebep olacaktır. Bu saldırıya %51 saldırısı yahut Sybil saldırısı denir. Her ne kadar özellikle büyük kriptoparalar için gerçekleştirmesi oldukça maliyetli bir saldırı olsa da henüz kriptoparalar buna bir çare bulamamışlardır. Misal olarak Zcash için "poolin.com" madenci havuzu bilinen özetleme oranının %35.2'sine sahiptir[3]. %50.1 oranını geçtikten sonra poolin.com madenci havuzunun kötü niyetli bir madenci havuza dönmesi durumunda Zcash için çok tehlikeli sonuçları olabileceği kolaylıkla anlaşılacaktır.

- AnaUç ve mobil cüzdanlar örneklerinde olduğu gibi kriptosistemdeki öğelerindeki gereksiz loglamalar, iletişimde verilen gereksiz bilgiler, uygulama açıkları yahut göz ardı edilmiş açıklar çeşitli kötü niyetli kişiler tarafından ilgili kriptoparanın ciddi saldırılara maruz kalmasına sebep olmaktadır. Örnek olarak Monero geliştirme takımı yaptıkları araştırmada web sayfaları https://web.getmonero.org/ sayfasının hacklendiğini doğrulamış ve 18 Kasım 2019 UTC 02:30 ile 04:30 saatları arasında CLI cüzdanını indirilenlerin muhtemelen etkilendiğini belirtmişlerdir[4]. Bu durumun anonimsizleştirmeye nasıl katkı sağlayacağı şu şekilde açıklanabilir; kötü niyetki kişiler ele geçirdikleri kişilerin cüzdanlarını da ele geçirmişlerse bu durumda bu cüzdanlar vasıtasıyla yapılan tüm işlemleri de tespit edebileceklerdir. Bu da bu cüzdanlarda üretilen çıktıların başka halka imzalarda girdi olarak kullanıldığında "sahte imzalayıcı" olarak işaretlenebilmesine ve nihayet bu işlemlerin bir adım daha hızlı analiz edilebilmesine yol açacaktır.

[2] https://www.reddit.com sayfasında Dash AnaUçlarının anonimsizleştirmeye olan katkısı hakkında bir forum tartışması yapılmıştır.

[3] https://miningpoolstats.stream/zcash sitesindeki 5 Temmuz 2020 verilerine göre hesaplanmıştır.

[4] https://securityboulevard.com/2020/01/how-the-november-2019-monero-supply-chain-hack-was-discoveredand-what-it-takes-to-block-these-kinds-of-attacks/ sayfasında bu konudan detaylıca bahseder.

- Kullanıcı gruplarından borsalar (exchanges) yani kriptopara coinlerinin alınıp satıldığı yerler ve bunların kullandığı adresler de yine risk grubundadır.

Bahsedilen tüm bu nedenlerden de anlaşılacağı gibi anonim kriptoparalar pratikte düşünüldüğü kadar anonim değillerdir. Ancak bu durum bu kriptoparaların yaptıkları işten tamamıyla vaz geçip büyük zahtmetlerle ürettikleri kriptopara sistemlerini kapatmaları gerektiği anlamına gelmez. Anonim kriptoparalar da başka herşeyde olduğu gelişen ve ilerleyen bir konudur. Önemli olan Monero'nun Şubat 2017'de 0-karıştırmalı işlemler örneğinde yaptığı gibi kriptosistemin herhangi bir üyesinde yahut kullanıcı grubunda oluşabilecek sızmaları ve açıkları fark edip bu açıklar için tedbir almalarıdır. Çünkü kriptoparaları kullanan kullanıcılar ne kadar insan ise bu kriptoparaları geliştiren geliştiriciler de o kadar insandır; yani hata yapmamaları imkansızdır. Önemli olan yapılan hatadan ders çıkartabilmektir. Bu nedenle bir sonraki kısım olan 4.3 kısmında kriptoparaların geliştiricileri ve kullanıcıları için naçizane tavsiyelerden bahsedilecektir.

4.3 Öneriler

Anonim kriptoparaların en önemli özelliği isimlerinden de anlaşılacağı gibi anonim ve mahremiyet sağlamalarıdır. 4.2. kısımda da bahsedildiği gibi teoride anonimken pratikte istenildiği ölçüde anonimliği yakalayamamaktadırlar. Ancak bu durumu engellemek için de bazı yöntemler mevcuttur. Bu yöntemleri aşağıdaki gibi listelenmiştir:

- Öncelikle kriptosistemde bulunan açıkların kapatılması gerekir. Çeşitli kriptoparaların geliştiricileri blokzincirin kendisinde zaman içerisinde detaylı bir şekilde dokümante ettikleri güncellemeler yapmışlardır. Ancak sadece blokzincirde değil kriptoparanın yaşam ve işlem döngüsünde kullanılan bütün öğelerin ilgili güvenlik güncellemelerinin yapıldığı denetlenmelidir. Kriptoparalarda çeşitli işlemlerin yapılması için kullanılan bazı cüzdanlar gibi kriptosistemin çeşitli öğeleri doğrudan geliştiricilerin müdahele edebileceği öğeler değildir, daha çok üçüncü şahısları geliştirmiş olduğu sistemlerdir. Ancak ilgili kriptoparayı kullandıkları için geliştiricilerin buralarda oluşabilecek bilgi sızmalarını ve açıkları da bir nebze de olsa denetlemeleleri onlar için daha güvenilir olacaktır. Detaylı olarak kriptopara ağları yahut kullanılan cüzdanlar için öneriler anlatılmayacaktır. Bu öneriler Kısım 4.1'de bahsedilen makalelerde zaten detaylı bir şekilde anlatılmışlardır.

- Anonim kriptopara geliştiricileri kullanıcıları "anonim özelliklerinin nasıl kullanılması" gerektiğiyle alakalı bilgilendirme yapmaları gerekmektedir. Örneğin en iyi pratikler (best practices) şeklinde bir yazı yazılıp kullanıcılar için en doğru bir

şekilde nasıl korumalı işlem yahut ÖzelGönderim işlemi yapabilecekleri basitçe bilgilendirilir.

- 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 tavsiye olunur. Bunun yerine kullanıcılar sadece ihtiyacı olan miktarı korumalı havuzdan çıkarmaları daha doğru olacaktır.

- Yine Zcash kullanıcılarının JS-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 edilemezlik sağlayacaktır.

- Zcash kullanıcıları son olarak işlem yaparken Zatoshi cinsinden 10.000'in (varsayılan işlem bedeli) katsayısı olacak yuvarlak değerler üzerinden işlem yapmaktan kaçınmalıdırlar. Bu durumda kötü niyetli kişilerin yaptığı saldırılarla yahut bu tezdeki analiz çalışmasında olduğu gibi yapılan araştırmalarla göz ardı edilen değerler kullanılarak işlem geçmişini takip edilemeyecektir.

- Zcash madenci havuzları bünyesinde bulundurdukları madencilere ödemeleri hep aynı adres üzerinden yapmaktan kaçınmalıdırlar. Yapılan analizde bazı madenci havuzlarının en azından 6-7 farklı adres kullandıkları tespit edilmiştir, ki bu iyiye işarettir. Ayrıca madenci havuzlarının TMadenci yahut ZMadenci kategorilerine girmekten kaçınmaları için madencilerine ödemeleri doğrudan z-z korumalı işlemler üzerinden yapmaları tavsiye edilir. Örnek olarak SlushPool, Bitfly ve Luxor Mining isimli madenci havuzlarının doğrudan z-adrese sahip madencilere ödeme yapmaya imkan sunduklarını belirtilmiştir[5].

- 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 aynı ya da benzeri olmaması gerekir.

[5]https://www.zcashcommunity.com/mining/mining-pools/ web sayfasında "Pools that payout to Private Z_addresses " başlığı altındaki madenci havuzlarıdır.

- 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. Ne var ki, 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 için doğrudan analiz çalışması yapılmadığından bu anonim kriptoparada doğrudan bir öneri açıklaması yapılmayacaktır. Ancak anonim yahut anonim değil tüm kriptopara kullanıcılarının (doğal olarak) şahsi adreslerini gerekmeyen hiçbir yerde açıklamamaları tavsiye edilir. Ayrıca kriptopara geliştiricilerinin bunu ihlal eden Online marketler yahut forumları izlemeleri önerilir.

- Son olarak, Zcash ve Dash geliştiricilerinin (aslında bu durum tüm anonim/anonim olmayan kriptoparalar için geçerlidir) kullanıcı gruplarının genel olarak yapmış olduğu hataları gruplandırmaları önerilir. Böylece her yapılan yanlışı engellemek imkansız olsa da kullanıcıların en çok yaptığı yanlışlar için düzeltmeler, güncellemeler yahut alternatif yöntemler geliştirmek mümkün olacaktır.

Bölüm 5

Netice

2008 yılının Ekim ayında Satoshi Nakamoto'nun çıkarmış olduğu makalede sunduğu blokzincir teknolojisi ve kriptopara mantığıyla 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 teknolojisi ve kriptoparalar önemini artarak korumuştur.

Bitcoin, ilk çıktığı yıllarda her ne kadar tümüyle anonim olduğu düşünülse de yapılan çalışmalar, yaşanılan çeşitli olaylar ve gerçekleştirilen kötü niyetli saldırılar neticesinde hiçbir şekilde anonim olmadığı anlaşılmıştır. Bu nedenle zamanla Bitcoin için anonimliği sağlaması adına çeşitli yöntemler geliştirilmiştir.

Ancak bu yöntemlerin de istenilen anonimlik ve mahremiyeti sağlayamadığı kolaylıkla analiz edilebilmiştir. Bunun yanında ayrıca bazı yöntemlerin de uygun maliyetli (cost-effective) olmadığı gözlemlenmiştir. Bu durumda çeşitli geliştiriciler farklı zamanlarda Bitcoin'e alternatif "anonim kriptoparalar" denilen ve tamamıyla anonimliğe odaklanan kriptoparalar geliştirmişlerdir.

Bu kriptoparalar teoride gerçekten de ciddi anlamda anonimlik ve mahremiyet sağlar. Zcash ve Monero kriptografik yöntemler kullanarak sağlarken Dash ve PIVX masternodelar ve CoinJoin tabanlı karıştırma mekanizmaları kullanarak yapar. Verge ise ToR altyapısını kullanarak IP adreslerini gizlemeye odaklanır. Ancak pratikte bu kriptoparaların düşünüldüğü kadar anonimlik sağlamadığını yapılan analizler neticesinde anlaşılmıştır.

Zcash ve Dash için bu tez içerisinde işlem miktarı (ve Dash için toplam adres sayısı) bakımından analiz çalışması yapılmıştır. Analiz sonucunda önemli oranda anonim işlemin takip edilebileceği sonucuna varılmıştır. İlgili kriptoparaların anonimlik seviyesinin

artırılması için hem kullanıcılarına hem de geliştiricilerine çeşitli görevler düşmektedir. Yazılan tezde her iki grup için çeşitli önerilerden bahsedilmiştir.

Kriptosistemdeki açıklar, kriptopara ağından bilgi sızdırabilme, kötü niyetli madenciler, borsacılar, düğümler ve masternodelar, bilgi sızdıran mobil cüzdanlar gibi birçok anonimlik ve mahremiyeti tehdit eden unsur tüm anonim kriptoparalar için canlılığını koruyan tehlikelerdir. Yapılan güncellemeler ve engellemelerle ilgili kriptoparaların geliştiricileri bu tehlikeleri bertaraf etmek için çalışma yapmış ve yapmaya devam etmektedirler. Her ne kadar bu tehlikeler için tavsiye edilen öneriler detaylı bir şekilde tez içerisinde anlatılmamış olsa bile tehlikelerin anlatıldığı ilgili makalelerde alınması gereken önerilerden detaylıca bahsedilmiştir.

Sonuç olarak şu söylenebilir, anonim kriptoparalar ve bunların bütün unsurları her geçen gün gelişen ve değişen bilişim teknolojilerinin bir parçasıdır. Özellikle bilgi güvenliğinin ve mahremiyetin olması gerektiği "para" odaklı sistemlerde gizlilik ve mahremiyetin ihlalinin daha çok yaşanması beklenen bir durumdur. Özellikle hiçbir şekilde güven odaklı olmayan kriptoparalar ve blokzincir için bu tehlike daha da önemli bir ölçüde canlılığını korumaktadır. Örnek olarak kötü niyetli bir düğüm yahut düğüm grubunun %51 doğrulama oranını yakalaması durumunda kriptoparayı ciddi tehlikeler beklemektedir. Ayrıca güvenlik mekanizmalarının sürekli gelişip iyileştiği gibi güvelik ve mahremiyeti ihlal eden mekanizmalar da sürekli olarak daha tehlikeli bir şekilde gelişip kullanıcıların ve geliştiricilerin karşısına çıkmaktadırlar. Burada önemli olan nokta kriptopara geliştiricilerinin güvenlik ihlallerinin anlaşılmasının ardından hızlı bir şekilde müdahele edip yapılan yanlışlardan ve ihlallerden ders çıkartabilmesidir. Yapılan bu tez çalışmasında da Zcash ve Dash kriptoparaları için anonimliğin analiz edilebileceği gösterilmiş; bunun yanında analiz yapılmasını engellemek yahut çıkan sonuçları daha kabul edilebilir hale getirebilmek için çeşitli tavsiyeler verilmiştir.

Ek A

Ek-A

Algorithm 1 TMadencilerin Bulunmasi

```
1: procedure TMadencileriBul(blokZincir)
2:     blokListesi[] ← blokZincir[-25000]
3:     islemListesi[] ← blockList.adreses
4:     muhtemelTMadenciListesi[] ← ∅
5:     korumaliHavuzdanCoinAlanListesi[] ← ∅
6:     korumaliHavuzdanCoinAlanGruplanmisListesi ← ∅
7:     for islem ∈ islemListesi do
8:         if islem.ciktiSayisi>30 & islem.korumaliMi == false then
9:             muhtemelTMadenciListesi ← islem.GirdiAdresi
10:        else if islem.korumaliMi == true then
11:            korumaliHavuzdanCoinAlanListesi ← islem.ciktiAdresi
12:        end if
13:    end for
14:    muhtemelTMadenciListesi ← muhtemelTMadenciListesi ∈ muhtemelTMadenciListesi.adres = korumaliHavuzdanCoinAlanListesi.adres
15:    korumaliHavuzdanCoinAlanListesi ← korumaliHavuzdanCoinAlanListesi ∈ korumaliHavuzdanCoinAlanListesi.adres = muhtemelTMadenciListesi.adres
16:    odemeYapilanMadenciListesi ← blokListesi.islem.ciktiAdresi ∈ blokListesi.islem = muhtemelTMadenciListesi.islem
17:    for muhtemelTMadenci ∈ muhtemelTMadenciListesi do
18:        TMadencileriGrupla(muhtemelTMadenciListesi, muhtemelTMadenci, odemeYapilanMadenciListesi, korumaliHavuzdanCoinAlanGruplanmisListesi)
19:    end forreturn korumaliHavuzdanCoinAlanGruplanmisListesi
20: end procedure
21: procedure TMadencileriGrupla(muhtemelTMadenciListesi, muhtemelTMadenci, odemeYapilanMadenciListesi, korumaliHavuzdanCoinAlanGruplanmisListesi)
22:    mevcutHavuzunMadenciAdresleri ← odemeYapilanMadenciListesi ∈ odemeYapilanMadenciListesi.islem = muhtemelTMadenci.islem
23:    for girdi ∈ muhtemelTMadenciListesi do
24:        girdiIslemMiners ← odemeYapilanMadenciListesi ∈ odemeYapilanMadenciListesi.islem = girdi.islem
25:        if ∃ girdiIslemMiners ∈ mevcutHavuzunMadenciAdresleri then
26:            korumaliHavuzdanCoinAlanGruplanmisListesi ← korumaliHavuzdanCoinAlanListesi ∈ korumaliHavuzdanCoinAlanListesi.adres = girdi.adres
27:        end if
28:    end for
29: end procedure
```

Ek B

Ek-B

Algorithm 2 ZMadenci Havuzlarının Bulunması

```
1: procedure ZMadencileriBul(blokZincir)
2:     blokListesi[] ← blokZincir[-25000]
3:     muhtemelZMadenciler[] ← ∅
4:     for blok ∈ blokZincir do
5:         if blok.islem.ciktiSayisi > 30 & blok.islem.korumaliIslemMi then
6:             muhtemelZMadenciler ← blok.islem
7:         end if
8:     end for
9:     odemeYapilanMadenciListesi ← blokListesi.islem.ciktiAdresi ∈ blokListesi.islem
   = muhtemelZMadenciler.islem
10:    for zMadenciİslemi ∅ muhtemelZMadenciler do
11:        ZMadencileriGrupla(muhtemelZMadenciler, zMadenciİslemi, odemeYapilan-
MadenciListesi)
12:    end forreturn gruplanmisZMadenciListesi
13: end procedure
14: procedure ZMadencileriGrupla(muhtemelZMadencilerList, mevcutIslem, ode-
meYapilanMadenciListesi)
15:    eskiAdresListesi[] ← ∅
16:    mevcutIslemAdresListesi[] ← odemeYapilanMadenciListesi ∅ odemeYapilanMaden-
ciListesi.islem = mevcutIslem
17:    while eskiAdresListesi != mevcutIslemAdresListesi do
18:        eskiAdresListesi = mevcutIslemAdresListesi
19:        for zMadenciIslemi in muhtemelZMadencilerList do
20:            zMadenciIslemiAdresListesi[] ← odemeYapilanMadenciListesi ∅ odemeYapi-
lanMadenciListesi.islem = zMadenciIslemi
21:            if ∃ zMadenciIslemiAdresListesi ∅ mevcutIslemAdresListesi then
22:                mevcutIslemAdresListesi ← mevcutIslemAdresListesi + zMadenciIslemi-
AdresListesi
23:                gruplanmisZMadenciListesi ← mevcutIslem, zMadenciIslemi
24:            end if
25:        end for
26:    end while
27: end procedure
```

Kaynaklar

[1] Blokzincir. https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html. Accessed: 2020-03-27.

[2] Bitcoin'e başlarken. https://bitcoin.org/tr/. Accessed: 2020-03-27.

[3] Dash documentation. https://docs.dash.org/en/stable/, . Accessed: 2020-07-01.

[4] Dash features. https://docs.dash.org/en/stable/introduction/features.html, . Accessed: 2020-07-01.

[5] Dash (cryptocurrency). https://en.wikipedia.org/wiki/Dash_(cryptocurrency)#:~:text=Dash%20is%20an%20open%20source,transactions%20that%20can%20be%20untraceable., . Accessed: 2020-07-01.

[6] Address. https://monerodocs.org/public-address/standard-address/, . Accessed: 2020-07-04.

[7] Ring signature. https://web.getmonero.org/resources/moneropedia/ringsignatures.html, . Accessed: 2020-07-04.

[8] Monero technical specs. https://monerodocs.org/technical-specs/, . Accessed: 2020-07-04.

[9] Monero (cryptocurrency). https://en.wikipedia.org/wiki/Monero_(cryptocurrency), . Accessed: 2020-07-04.

[10] Zcash documentation, what is zcash? https://zcash.readthedocs.io/en/latest/, . Accessed: 2020-03-28.

[11] Glossary. https://zcash.readthedocs.io/en/latest/rtd_pages/glossary.html#zecGlossary, . Accessed: 2020-06-30.

[12] Pool distribution (calulate by blocks). https://btc.com/stats/pool?pool_mode=year, . Accessed: 2020-06-06.

[13] Bitcoin (btc) nedir? https://www.btcturk.com/bilgi-platformu/bitcoin-nedir?gclid=CjwKCAjwt-L2BRA_EiwAacX32SDlg8Iv0AHilPasxPeh6O1b16jYNIlz-a6dY2LKbnHBYDyyRoZMkRoC33UQAvD_BwE, . Accessed: 2020-06-06.

[14] Proof of reputation as liquid democracy for blockchain. https://steemit.com/blockchain/@aigents/proof-of-reputation-as-liquid-democracy-for-blockchain. Accessed: 2020-06-08.

[15] What is blockchain? https://lisk.io/what-is-blockchain. Accessed: 2020-06-08.

[16] Bitcoin'in yasal mevzuat karşisindaki durumu. https://www.mondaq.com/turkey/fin-tech/697860/bitcoin39in-yasal-mevzuat-kar351isindaki-durumu. Accessed: 2020-06-08.

[17] Btc
usd grafiği. https://tr.tradingview.com/chart/?symbol=BITSTAMPABTCUSD. Accessed: 2020-06-05.

[18] Bitcoin. https://en.wikipedia.org/wiki/Bitcoin, 2020. Accessed: 2020-06-06.

[19] Blockchain. https://en.wikipedia.org/wiki/Blockchain, 2020. Accessed: 2020-06-06.

[20] Consensus mechanism (cryptocurrency). https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp#:~:text=What%20Is%20a%20Consensus%20Mechanism,systems%2C%20such%20as%20with%20cryptocurrencies., 2020. Accessed: 2020-06-07.

[21] Consensus. https://en.wikipedia.org/wiki/Consensus_(computer_science), 2020. Accessed: 2020-06-07.

[22] Dash cryptocurrency: Complete dash coin guide. https://www.bitdegree.org/tutorials/dash-cryptocurrency/, 2020. Accessed: 2020-05-05.

[23] Lydians. https://en.wikipedia.org/wiki/Lydians, 2020. Accessed: 2020-05-31.

[24] Merkle tree. https://en.wikipedia.org/wiki/Merkle_tree, 2020. Accessed: 2020-06-07.

[25] Silk road (marketplace). https://en.wikipedia.org/wiki/Silk_Road_(marketplace), 2020. Accessed: 2020-06-21.

[26] Virtual currency law in the united states. https://en.wikipedia.org/wiki/Virtual_currency_law_in_the_United_States, 2020. Accessed: 2020-05-31.

[27] Y. v. E. A. v. A. S. M. Al Jawaheri, Husam ve Boshmaf. Deanonymizing tor hidden service users through bitcoin transactions analysis. pages 1–11. Qatar University, Jul 2019. URL https://orbilu.uni.lu/bitstream/10993/39996/1/Zcash_Miner_Linking%20(2).pdf.

[28] B. Alex and F. Daniel. Deanonymization of hidden transactions in zcash. pages 1–15, University of Luxembourg, May 2018. URL https://cryptolux.org/images/d/d9/Zcash.pdf.

[29] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating user privacy in bitcoin. In *Lecture Notes in Computer Science*, pages 1–18, ETH Zurich, 8092 Zuerich, Switzerland and NEC Laboratories Europe, 69115 Heidelberg, Germany, 2013. ISBN 978-3-6423-9883-4. URL https://eprint.iacr.org/2012/596.pdf.

[30] K. Atlas. An analysis of darkcoin's blockchain privacy via darksend+. pages 1–25, Sep 2014. URL http://cdn.anonymousbitcoinbook.com/darkcoin/darksend-paper/Atlas_Darksend-Analysis-v001.pdf.

[31] A. Biryukov and D. Feher. Privacy and linkability of mining in zcash. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 1–6, University of Luxembourg, Esch-sur-Alzette, Luxemburg, Jun 2019. IEEE. ISBN 978-1-5386-7117-7. URL https://orbilu.uni.lu/bitstream/10993/39996/1/Zcash_Miner_Linking%20(2).pdf.

[32] A. Biryukov and S. Tikhomirov. Transaction clustering using network traffic analysis for bitcoin and derived blockchains. In *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019, April 2019, :204-209*, pages 1–6, University of Luxembourg, Esch-sur-Alzette, Luxemburg, April 2019. IEEE. ISBN 978-1-7281-1878-9. URL https://orbilu.uni.lu/bitstream/10993/39729/1/biryukov-tikhomirov-mobile-wallets.pdf.

[33] A. Biryukov and S. Tikhomirov. Deanonymization and linkability of cryptocurrency transactions based on network analysis. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 1–13, University of Luxembourg, Esch-sur-Alzette, Luxemburg, Jun 2019. IEEE. ISBN 978-1-7281-1148-3, 978-1-7281-1147-6. URL https://orbilu.uni.lu/bitstream/10993/39996/1/Zcash_Miner_Linking%20(2).pdf.

[34] A. Biryukov and S. Tikhomirov. Portrait of a miner in a landscape. pages 1–6, Paris, France, France, May 2019. IEEE. ISBN 978-1-7281-1879-6. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8822516.

[35] A. Biryukov and S. Tikhomirov. Security and privacy of mobile wallet users in bitcoin, dash, monero, and zcash. pages 1–11, University of Luxembourg, Esch-sur-Alzette, Luxemburg, Jun 2019. Elsevier. URL https://orbilu.uni.lu/bitstream/10993/39729/1/biryukov-tikhomirov-mobile-wallets.pdf.

[36] A. Biryukov, D. Khovratovich, and I. Pustogarov. Deanonymisation of clients in bitcoin p2p network. In *Computer and Communications Security*, pages 1–13, University of Luxembourg, Esch-sur-Alzette, Luxemburg, 2014. New York, NY, USA: ACM, 2014. ISBN 978-1-4503-2957-6, 1-4503-2957-8. URL https://dl.acm.org/doi/pdf/10.1145/2660267.2660379.

[37] A. Biryukov, D. Feher, and G. Vitto. Privacy aspects and subliminal channels in zcash. In *ACM CCS 2019*, pages 1–17, University of Luxembourg, Esch-sur-Alzette, Luxemburg, Nov 2019. URL https://orbilu.uni.lu/bitstream/10993/41278/1/Post_sapling_ZC_paper.pdf.

[38] I. Biryukov, Alex ve Pustogarov. Bitcoin over tor isn't a good idea. In *2015 IEEE Symposium on Security and Privacy, SP 2015*, pages 1–13, University of Luxembourg, Esch-sur-Alzette, Luxemburg, Feb 2015. IEEE. ISBN 978-1-4673-6949-7. URL https://orbilu.uni.lu/bitstream/10993/39996/1/Zcash_Miner_Linking%20(2).pdf.

[39] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for bitcoin with accountable mixes. In *Financial Cryptography and Data Security : 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers. :486-504*, pages 1–18, Princeton University, University of Maryland and Concordia University, 2014 Nov. Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. ISBN 978-3-662-45472-5, 978-3-662-45471-8. URL http://www.jbonneau.com/doc/BNMCKF14-FC-mixcoin_proceedings.pdf.

[40] E. Daniel, E. Rohrer, and F. Tschorsch. Map-z: Exposing the zcash network in times of transition. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 1–8, Distributed Security Infrastructures, Technical University of Berlin, Jul 2019. Cornell University. URL https://arxiv.org/pdf/1907.09755.pdf.

[41] C. G. M. G. I. M. E. T. Eli Ben-Sasson, Alessandro Chiesa and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin (extended version). In *booktitle*, pages 459–474, IEEE 2014, month year. A condensed version appeared in Proceedings of the IEEE Symposium on Security and Privacy (Oakland) 2014. URL http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[42] K. George and P. Ania M. Extending the anonymity of zcash. pages 1–2, University College London, United Kingdom, Feb 2019. Cornell University. URL https://arxiv.org/pdf/1902.07337.pdf.

[43] K. George, Y. Haaroon, M. Mary, and M. Sarah. An empirical analysis of anonymity in zcash. In *27th USENIX Security Symposium (USENIX Security '18)*, pages 1–15, University College London, May 2018. Cornell University. URL https://arxiv.org/pdf/1805.03180.pdf.

[44] A. Hinteregger and B. Haslhofer. An empirical analysis of monero cross-chain traceability. In *Conference paper (http://fc19.ifca.ai/)*, pages 1–8, Austrian Institute of Technology and Vienna University of Technology, Jan 2019. URL http://arxiv.org/abs/1812.02808.

[45] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox. Zcash protocol specification. In *Zcash Protocol Specification*, pages 1–151. Zcash, Mar 2020. URL https://github.com/zcash/zips/raw/master/protocol/protocol.pdf.

[46] Q. Jeffre. On the linkability of zcash transactions. In *27th USENIX Security Symposium (USENIX Security '18)*, pages 1–5, Esch-sur-Alzette, Luxemburg, Dec 2017. Cornell University. URL https://arxiv.org/pdf/1712.01210.pdf.

[47] L. Jong-Hyouk. Rise of anonymous cryptocurrencies: Brief introduction. In *IEEE Consumer Electronics Magazine IEEE Consumer Electron. Mag. Consumer Electronics Magazine, IEEE. 8(5):20-25 Sep, 2019*, pages 1–6, Sangmyung Univ., Cheonan, South Korea, Sep 2019. USA: IEEE. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8822516.

[48] H. Kalodner, S. Goldfeder, A. Chator, M. Möser, and A. Narayanan. Blocksci: Design and applications of a blockchain analysis platform. pages 1–14, Princeton University, Sep 2017. URL http://arxiv.org/abs/1709.02489.

[49] P. Koshy, D. Koshy, and P. McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security FC 2014: Financial Cryptography and Data Security pp 469-485.* Berlin, Heidelberg : Springer Berlin Heidelberg, 2014., Nov 2014. ISBN 978-3-662-45472-5, 978-3-662-45471-8. URL https://link.springer.com/chapter/10.1007%2F978-3-662-45472-5_30.

[50] A. Kumar, C. FischerShruti, and T. Saxena. A traceability analysis of monero's blockchain. In *In: Computer Security – ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Proceedings. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, 10493 LNCS:153-173)*, National University of Singapore, Singapore, Singapore, Aug 2017. Cham : Springer International Publishing, 2017. ISBN 978-3-319-66399-9, 978-3-319-66398-2. URL https://link.springer.com/chapter/10.1007%2F978-3-319-66399-9_9.

[51] E. H. K. L. H. H. S. S. K. H. J. H. A. M. A. N. N. C. Malte Möser, Kyle Soska. An empirical analysis of traceability in the monero blockchain. In *Proceedings on Privacy Enhancing Technologies, Vol 2018, Iss 3, Pp 143-163 (2018)*, pages 1–22, Princeton University, Apr 2018. Sciendo, 2018. URL https://arxiv.org/pdf/1704.04299.pdf.

[52] S. Mastan, Indra Deep ve Paul. A new approach to deanonymization of unreachable bitcoin nodes. pages 1–22. Indian Institute of Technology Gandhinagar, Indian Institute of Technology Bhilai. URL https://eprint.iacr.org/2018/243.pdf.

[53] C. L. S. R. Mauro Conti, Sandeep Kumar E. A survey on security and privacy issues of bitcoin. In *EAS 499 Senior Capstone Thesis*, pages 1–36. IEEE, Dec 2017. URL https://arxiv.org/pdf/1706.00916.pdf.

[54] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A fistful of bitcoins: Characterizing payments among men with no names. In *Internet measurement conference. :127-140*, pages 1–13, University of California and San Diego George Mason University, 2013. New York, NY, USA: ACM, 2016. ISBN 978-1-4503-1953-9. URL https://dl.acm.org/doi/pdf/10.1145/2504730.2504747.

[55] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. pages 1–9, https://bitcoin.org/, Oct 2008. URL https://bitcoin.org/bitcoin.pdf.

[56] L. Y. v. G. K. Nathan Borggren, Hyoung-yoon Kim. Simulated blockchains for machine learning traceability and transaction values in the monero network. pages 1–10, Geometric Data Analytics, Inc., Durham, NC, 27701, Jan 2020.

[57] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust (PASSAT) / 2011 IEEE Third Int'l Conference on Social Computing (SocialCom)*, pages 1–30, Clique Research Cluster, Complex & Adaptive Systems Laboratory, University College Dublin, Ireland, May 2012. IEEE. ISBN 978-1-4577-1931-8, 978-0-7695-4578-3. URL https://arxiv.org/pdf/1107.4524.pdf.

[58] D. Ron and A. Shamir. Quantitative analysis of the full bitcoin transaction graph. In *Lecture Notes in Computer Science*, pages 1–19, Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel, 2013. ISBN 978-3-6423-9883-4. URL https://eprint.iacr.org/2012/584.pdf.

[59] M. Spagnuolo, F. Maggi, and S. Zanero. Bitiodine: Extracting intelligence from the bitcoin network. In *Financial Cryptography and Data Security : 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers. :457-468*, pages 1–12, Politecnico di Milano, Italy, 2014. Berlin, Heidelberg

: Springer Berlin Heidelberg, 2014. ISBN 978-3-662-45472-5, 978-3-662-45471-8. URL http://www.syssec-project.eu/m/page-media/3/spagnuolo_bitiodine_fc14.pdf.

[60] TCMB. Kâğıt paranın tarihçesi. In *Kâğıt Paranın Tarihçesi*, pages 1–5. Türkiye Cumhuriyeti Merkez Bankası, 2020. URL https://www.tcmb.gov.tr/wps/wcm/connect/d189b219-fe71-40bf-9754-6a5f7d0a65eb/KagitParaTarihce.pdf?MOD=AJPERES#:~:text=%C4%B0lk%20k%C3%A2%C4%9F%C4%B1t%20para%20ise%20M.S.,yine%20%C3%87in'de%20ortaya%20%C3%A7%C4%B1km%C4%B1%C5%9Ft%C4%B1r.&text=%C4%B0lk%20Osmanl%C4%B1%20banknotlar%C4%B1%20Abd%C3%BClmecit%20taraf%C4%B1ndan,bonosu%20niteli%C4%9Finde%20olmak%20%C3%BCzere%20%C3%A7%C4%B1kar%C4%B1lm%C4%B1%C5%9Ft%C4%B1r.

[61] W. Wu and B. Falk. Limitations of privacy guarantees in cryptocurrency. In *EAS 499 Senior Capstone Thesis*, pages 1–31, University of Pennsylvania, USA, Apr 2018. School of Engineering and Applied Science University of Pennsylvania. URL https://www.cis.upenn.edu/~fbrett/theses/wai_wu.pdf.

[62] D. A. ÇARKACIOĞLU. Krİpto-para bitcoin. In *KRİPTO-PARA BITCOIN ARAŞTIRMA RAPORU*, pages 1–84, SERMAYE PİYASASI KURULU, Dev 2016. SERMAYE PİYASASI KURULU Araştırma Dairesi. URL https://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130.

Özgeçmiş

Tezin yazarı Muhammet Ali ÖZTÜRK 11 Ekim 1991 Cuma günü Ordu'nun Gülyalı ilçesinde hataya gözlerini açtı. İlkokul ve orta okulu Varsak Şelale İ.Ö. Okulu'nda, liseyi Özel Envar Anadolu Lisesi'nde okudu. Daha sonra 2009 senesinde İstanbul Üniversitesi Bilgisayar Mühendisliği programına kayıt yaptıran yazar, 2014'ün Haziran ayında 3.00 puanıyla lisans eğitimini tamamladı. 2014 Ekim ayında Kuveyt Türk Katılım Bankası'nda işe başladıktan sonra 2017 Haziran ayında bu firmadan ayrılarak aynı yılın Temmuz ayında TÜBİTAK BİLGEM'de Yazılım Geliştirme Uzmanı olarak işe başladı. Halen de bu firmada aktif olarak çalışmaya devam etmektedir.

Genel olarak yazılım alanında çalışan yazar C#, çeşitli SQL dilleri (MSSQL, Oracle, PostgreSQL), Java, Önyüz programlama dilleri ve syntaxları (HTML, CSS, Javascript vb.) alanlarında uzmanlaşmıştır. Nesne tabanlı tasarım, planlama ve yazılım alanlarında yıllardır çalışan yazar, daima en yeni teknolojileri kullanarak çalışmaya odaklanır.