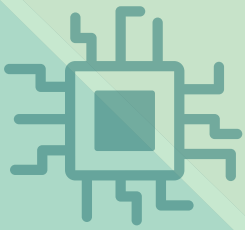
BANKALARARASI KART MERKEZİ

TÜBİTAK BİLGEM

BLOKZİNCİR Araştırma Laboratuvarı

BLOKZİNCİRLERDE GÜVENLİK VE MAHREMİYET

NİSAN 2020



HAZIRLAYANLAR

Nevzat Özcandan
Araştırmacı

Öznur Kalkar
Uzman Araştırmacı

Dr. Muhammed Ali Bingöl
Başuzman Araştırmacı

Dr. İsa Sertaya
Başuzman Araştırmacı

Taner Dursun
Başuzman Araştırmacı

Okan Yıldız
BKM İş Geliştirme Müdürü

Enes Türk
BKM İş Geliştirme Mühendisi

KONTROL

Fatih Birinci
TÜBİTAK BİLGEM UEKAE Müdür Yardımcısı

Özge Çelik
BKM İş Geliştirme Direktörü

ONAY

Erdal Bayram
TÜBİTAK BİLGEM UEKAE Müdürü

Celal Cündoğlu
BKM Ödeme Platformaları ve İş Geliştirme Genel Müdür Yardımcısı

Bu Rapor, TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarı tarafından Bankalararası Kart Merkezi (BKM) için hazırlanmıştır.

Tasarım ve Grafik Uygulama
TERMİNAL MEDYA LTD. ŞTİ.
Maslak Mah. Bilim Sokak No:5 SUN Plaza Kat:13 Sarıyer/İSTANBUL
0(212) 367 4988 ve 0(532)643 6959

Editör
ÖZLEM ÖZKAN

Grafik Uygulama
GÜLİSTAN ŞENOL

Baskı
SET POZİTİF MATBAA
Maslak Mahallesi Ahi Evran Caddesi
Rentaş İş Merkezi A Blok No: 62 Sarıyer/İSTANBUL
0(212) 286 4933

İÇİNDEKİLER

SUNUŞ

Celal Cündoğlu
BKM
Genel Müdür Yardımcısı

DİJİTALLEŞEN dünyada her kurumun iş modellerini yeniden yorumlaması bir opsiyondan çıkıp zorunluluğa dönüşüyor. Şirketlerin geleneksel düşünce yapılarını geride bırakmaları, inovasyona ağırlık vermeleri, değişimi ve dönüşümü içselleştirecek bilince sahip olmaları gerekiyor. Blokzincir teknolojisi ise bu dönüşümün ana bileşenlerinden biri olarak karşımızda duruyor. Temelinde merkeziyetsizlik, şeffaflık ve güven olgularını barındıran blokzincir, geleneksel iş yapış biçimlerini köklü değişime uğratmanın yanı sıra veri gizliliği ve mahremiyet başlıklarında çağın gereksinimlerine uygun yapılar sunma potansiyeliyle dikkat çekiyor.

Kurumumuz bünyesinde farklı platformlarda deneme çalışmaları gerçekleştirdiğimiz blokzincirde her gün yeni şeyler öğreniyoruz. Ödemeler alanında hizmet veren bir kurum olarak blokzincirin değer öne-

Fatih Birinci
TÜBİTAK BİLGEM UEKAE
Enstitü Müdür Yardımcısı

YÜZ YÜZE ve kağıt para ile alışveriş yaptığımız günlerde mahremiyet sorunlarımız yoktu. Mahremiyet problemi daha çok ünlülerin özel yaşamı ve onları takip eden gazetecilerin sorunuydu. Dijitalleşme ile birlikte mahremiyet kavramı daha fazla gündemimize gelmeye ve tartışılmaya başlandı. Mahremiyetin dijital dünyada gerekli olmadığını savunanlar "Saklayacak bir şeyiniz yoksa kaygılanacak bir şeyiniz de yoktur" derler. Dijital dünyada saklayacak bir şeylerimiz olabilir mi veya sadece suçluların mı gizlenmeye ihtiyaçları vardır?

Dijitalleşen dünyada sağlık, sigorta, alışveriş gibi işlerimizi elektronik ortamda kaydediyor veya yapıyoruz. Buna bağlı olarak finansal bilgilerimiz, hastalık bilgilerimiz, alışkanlıklarımız, ziyaret ettiğimiz yerler gibi bilgileri üçüncü taraflarla paylaşmak durumunda kalıyoruz. Bu paylaşım bazen kontrolümüzde bazen de kontrolümüz dışında gerçekleşiyor. Saklamak insani bir davranış olduğundan açığa vurmak istemediğimiz şeylerin olması doğaldır. Fakat zorunlu olarak ve isteğimizin dışında paylaşmamız gereken veriler de olabilir. Örneğin acil bir durumda, acil sağlık bilgilerimize (kan grubumuz, ilaçlara alerjilerimiz vb.) ilgililer tarafından erişilmesi gerekir. Buna karşın, otoriteler dahil olmak üzere kişisel bilgiler hakkında yapılan tüm işlemlerin değiştirilemez bir şekilde kayıt altına almasının önemi tartışılmaz bir gerçektir. Dünyada ve ülkemizdeki mevzuatlarla (GDPR ve KVKK) farkındalığımızın ve mahremiyetimizin artırılması için yapılan çalışmalar güzel gelişmelerdir. Bunu sağlamak için teknolojik gelişmelere de ihtiyaç vardır.

rileri arasında en fazla odaklandığımız alanlardan biri, verinin gizliliği ve güvenliği oluyor. BKM bünyesinde gerçekleştirdiğimiz çalışmalara ek olarak ekosistemi aydınlatmaya ve doğru yönlendirmeye yönelik çalışmalar yapan Blockchain Türkiye Platformu (BCTR) çatısı altında finans, hukuk, teknoloji, tedarik zinciri gibi alanlarda teknolojinin potansiyelini keşfedip kullanım alanlarını belirlemeye çalışıyoruz.

BCTR çalışma gruplarında birlikte çalışmaktan mutluluk duyduğumuz ve bu noktada gerek Blockchain Türkiye gerekse BKM bünyesinde ortak çalışmalar yürütmekten büyük keyif aldığımız TÜBİTAK BİLGEM ile blokzincir teknolojisinin güvenlik ve mahremiyet özelliklerini, günümüzdeki blokzincir uygulamalarının temellerini ve blokzincirin yeni nesil teknolojileri başlıklarını inceleyerek bir rapor haline getirdik.

Raporumuzun bu konular hakkında detaylı bilgi sahibi olmak isteyen değerli okuyucularına faydalı olmasını dileriz.

Elektronik ihale ve oylama sistemlerini incelemeye başladığımızda, internet bankacılığı gibi hayatımıza girmiş teknolojilerde kullanılan kriptografik yapılardan farklı olarak grup imzalama, homomorfik şifreleme ve taahhüt şemaları gibi daha karmaşık yapılara ihtiyaç olduğunu gördük. Bu tip ileri kriptografik yapılar, ihale ve oylamada son derece önemli olan mahremiyeti sağlamak için gereklidir. Blokzincirlerde de mahremiyet teknolojilerine ihtiyaç var mıdır?

Bitcoin ile başlayan blokzincir teknolojisi gün geçtikçe gelişimine devam ediyor ve daha fazla alanda kullanım imkanı bulabileceğini gösteriyor. Blokzincirler, üzerlerinde birçok uygulamanın geliştirilebileceği platformlar haline dönüşüyor. Ethereum, Hyperledger Fabric ve Corda platformlarını örnek olarak gösterebiliriz. Bu platformların, üzerlerinde geliştirilecek uygulamaların ihtiyaçlarını karşılayabilecek kabiliyette olması beklenir. Bu kabiliyetlerden bir tanesi de mahremiyet sağlama teknolojileridir. Blokzincirin kullanım alanlarının genişliği düşünüldüğünde elektronik ihale ve oylama sistemlerinden daha ileri kriptografik yapıtaşlarına ihtiyaç duyulacağı anlaşılabilir. Yönetim ve mutabakat sağlama işlemleri gibi blokzincirin iç işleyiş mekanizmalarında da bu tür mahremiyet sağlama teknolojileri kullanılıyor.

Ülkemizde blokzincir konusunda araştırma ve geliştirme çalışmaları gün geçtikçe artıyor. Mahremiyeti sağlamak için ihtiyaç duyulacak karmaşık ve anlaşılması zor ileri düzey kriptografik yapıtaşlarını bir arada anlatan bir kaynak blokzincirle ilgilenenler için çok faydalı olacak. Bu konuda çalışan/çalışacak araştırmacı ve geliştiricilere kaynak olacak böyle bir raporun anadilimizde hazırlanması çok yerinde ve isabetli oldu. Bu çalışmanın ülkemize kazandırılmasına öncülük ettiği için Bankalararası Kart Merkezine teşekkür ederiz.

“Her yönüyle mükemmel hiçbir teknoloji olmadığı gibi blokzincirin de özellikle mahremiyet ve güvenlik konularında ilave tekniklere ihtiyaç duyduğu durumlar olabilmektedir. Önemli olan, hayal ettiğimiz yeni blokzincir tabanlı iş modellerini uygun tekniklerle desteklemek ve mükemmelleştirmektir.”

Dr. Soner CANKO
BKM Genel Müdürü

“Dijitalleşen dünyamızda güvenlik ve mahremiyetin önemiyle birlikte bu konudaki toplum bilinci de giderek artırmaya başlamıştır. TÜBİTAK BİLGEM Ulusal Elektronik ve Araştırma Enstitüsü, güvenlik ve mahremiyet konularında ülkemizin en eski ve öncü kuruluşudur. Enstitümüz bünyesinde yer alan Blokzincir Araştırma Laboratuvarı’nda, gelişmekte olan ve geniş kullanım potansiyeline sahip blokzincir teknolojisi ile bu teknolojinin güvenlik ve mahremiyeti konularında Ar-Ge çalışmaları yapıyoruz. Laboratuvarımızda, hem yeni çözümler üretiyor hem de blokzincir konusunda faaliyet gösteren kurum ve kuruluşlarla ortak çalışmalarda bulunuyoruz.”

Erdal BAYRAM
TÜBİTAK BİLGEM UEKAE Müdürü

YÖNETİCİ ÖZETİ

Blokzincir, en genel ifadesiyle veri erişiminin herkese açık ya da izne tâbi olarak tutulduğu ve üçüncü taraf bir güven otoritesine gerek duymayan, merkezi olmayan bir sistemdir. Blokzincir, her ne kadar dijital para birimi Bitcoin ile birlikte ortaya çıkmış olsa da, aslında her türlü veri ya da değer atfedilen dijital varlık transferinde kullanılabilmektedir. Blokzincir son yıllarda olgunlaşmış ve tedarik zinciri, kaynak, uyumluluk, gıda güvenliği ve dijital kimlik gibi çeşitli alanlarda değer üretmeye başlamıştır.

Blokzincirlerin, kullanıldıkları senaryoya bağlı olarak, kendi güvenliğini sağlamanın yanı sıra, kullanıcıların mahremiyetini sağlama ihtiyacı da bulunabilir. Mahremiyet kapsamında, işlemlerin kaynaklarının ve hedeflerinin gerçek kimliklerle bağdaştırılamaması ve birbiri ile ilişkilendirilememesi (anonymity ve untraceability), işlemlerdeki içeriklerin gizlenmesi, durum verilerinin gizlenmesi gibi alt işlevsellikler sağlanmalıdır. Blokzincirin doğası gereği, verilerin kopyasının bütün düğümlerde bulunması ve işlenmesi gerektiği göz önüne alındığında, mahremiyet hedeflerini sağlamanın güçlüğü daha kolay anlaşılabilir.

Mahremiyetin sağlanabilmesi için, gizlilik ve bütünlük isterlerini karşılamak için kullanılan temel kriptografik yapıtaşlarına ek olarak, sıfır bilgi ispatları gibi ileri kriptografik yapıtaşlarına da ihtiyaç duyulmaktadır. Sıfır bilgi ispatı, bir bilgiye sahip olunduğunun, o bilgi açık edilmeden, ispat edilmesine olanak sağlar. Ayrıca; taahhüt, akümülatör, simetrik şifreleme ve homomorfik şifreleme teknikleri verilerin kendisi yerine, gizlenmiş hallerinin kullanılarak işlem yapılmasına olanak verir. Özel imzalama yöntemleri ise işlemi başlatan kişinin kimliğinin gizlenmesi, işlemlerle kişilerin ilişkilendirilememesi ve imzalanan verinin gizlenmesi vb. mahremiyet artırıcı amaçlarla kullanılır. Bu yöntemler yeni olmasalar da kripto para sistemleri ve güncel teknolojik gelişmeler ışığında nispeten uygulanabilir duruma gelmişlerdir.

Bu raporda, blokzincir platformlarından beklenen temel güvenlik ve mahremiyet özellikleri açıklanmıştır. Bu özellikleri sağlamak üzere kullanılan ve/veya kullanılabilecek kriptografik olan ve kriptografik olmayan teknikler özetlenmiştir. Mevcut blokzincir platformlarının güvenlik ve mahremiyet açısından durumuna ise kriptopara blokzincirleri ve genel amaçlı blokzincirleri grupları altında bakılmıştır. Ek olarak, GDPR ve KVKK bağlamında mahremiyet sorunları tanımlanmış ve blokzincir projelerinde uygulanması için fırsatlar ve zorluklar gösterilmiştir. Blokzincir sistemlerinin ölçeklenebilirliğini artırmak için önerilen teknolojiler ve bunların güvenlik seviyeleri irdelenmiştir. Farklı blokzincir platformları ve dağıtık kayıt teknolojileri arasındaki birlikte çalışabilirlik konularına odaklanan blokzincir projelerine kısa bir bakış sunulmuştur.

GÖSTERİMLER

Bit	İkili sayı, 0 veya 1.
Bayt	8 bit uzunluğunda bit katarıdır.
SHA	NIST tarafından onaylanan güvenli özet fonksiyonlarını belirtir.
EC	Eliptik eğri
ECDSA	Eliptik eğri sayısal imzalama algoritmasının kısaltmasıdır.
$\in$	Küme elemanlığını belirtir.

$\cup$ ——— Küme birleşim operasyonudur.

$O(.)$ ——— Karmaşıklık üst sınırını belirten “Büyük O” operasyonudur.

$Com(.)$ ——— Taahhüt Fonksiyonudur.

$||$ ——— Bayt katarı birleştirme operatörüdür.

V ——— Veya operatörüdür.

$\oplus$ ——— XOR operatörüdür.

$\lceil . \rceil$ ——— Tavan fonksiyonudur. Örneğin; $\lceil 3.541 \rceil = 4$ veya $\lceil -1.034 \rceil = -1$

GİRİŞ

Toplumların para kavramını kullanmaya başlamalarının tarihsel kökenini tam olarak tespit etmek zordur. Ancak, ilk başlarda gerçek değere sahip emtia para kullanılırken, zaman içerisinde özellikle kolay taşınabilirlik amacıyla, "meta destekli" yani temel emtiayı temsil eden ve aslında öz değeri bulunmayan paralar kullanılmaya başlandı. Günümüzde ise, ekonomiler merkezi bir otorite tarafından basılan ve yasal güvence ile taahhüt altına alınan fiyat para temelli bir yapıya dönüşmüştür. Merkezi otoriteye duyulan güvenden hareketle; toplum alışverişlerinde bu parayı kullanmakta ve temelde güven ilişkisi bu sistemi ayakta tutmaktadır [Ser20]. Gelenekselleşmiş otoriteler, arabulucular ve benzeri üçüncü kişilerin tesis etmekte olduğu "güven" olgusunun; merkeziyetsiz ya da dağıtık güven yapısı modelini içeren dağıtık kayıt defteri teknolojileri ile oluşturulması için ciddi çalışmalar yapılmaktadır.

Blokzincirin ana özellikleri şöyle özetlenebilir: Kayıt defterindeki verilerin doğruluğuna güven, dağıtık güç, erişilebilirlik, anonimlik ve değiştirilemezlik. Blokzincir teknolojisi nesnelerin interneti, bulut bilişim gibi diğer popüler teknolojilere benzer şekilde, doğasında siber güvenlik riskleri ve olumsuz yönler barındırır. Hız ve depolama açısından ölçeklenebilirliğinin zor olması, ilgili yasal düzenlemelerinin eksikliği, mevcut boyut ve bant genişliği kapasitesini zorlaması, mahremiyet ve güvenlik riskleri bu yönlerin başında gelmektedir. Blokzincir teknolojisinin yönetimine ilişkin düzenleyici standartlar ve yönetişim organları yetersizdir; bundan dolayı teknolojinin sunduğu olanaklardan faydalanmak isteyen kurumlar uygun güvenlik çerçevesini ve protokollerini belirlemeye çalışmalıdır. Blokzincir teknolojisinin kriptografik ve değiştirilemez yapısıyla ilgili göz önünde bulundurulması gereken güvenlik hususları; anahtar yönetimi, ağ ve erişim yönetimi, akıllı sözleşme yazılım geliştirme yaşam döngüsü ile veri gizliliği ve mahremiyetidir. Blokzincir teknolojisinin esaslarından olan mutabakat protokolleri, verilerin güvenliği konusunda kurumlara daha fazla güvence sağlamaktadır; çünkü bir işlemin zincirin sonuna eklenebilmesi için genellikle açık ve özel blokzincir kullanıcılarının en az %51'inin söz konusu işlemin geçerli olduğunu kabul etmesi gerekir. Kurumlar, belirli süreçlerinde blokzincir teknolojilerinden faydalanırken, bu ve benzeri senaryolarda ağ sorunlarının çözümüne odaklanmalıdır. Blokzincir teknolojisi, iş modellerini, insan tabanlı bir güven modelinden; daha önce karşılaşılmayan riskleri barındırabilecek, algoritmaya dayalı güven modeline dönüştürmektedir.

Kurumlar; roller, süreçler, hesap verebilirlik ölçütleri, performans ölçütleri iyi tanımlanmış yönetimsel bir çerçeve oluşturmalı ve söz konusu güvenlik risklerini düzgün bir şekilde yönetebilmek için genel bir güvenlik protokolü uygulamalıdır.

Blokzincir teknolojileri dağıtık veri saklama ve değer değişimi için gerek şart olan güven ortamını, temelde, kriptografik yapıtaşları ile sağlamaktadır. Kriptografi, blokzincir teknolojilerinden bağımsız olarak, çok eskilerden beridir, güvenli bilgi paylaşımı, veri bütünlüğünün korunması gibi gizlilik ve mahremiyet problemlerini çözmeyi hedefleyen bir bilim dalıdır. Blokzincirde ağırlıklı olarak kriptografik özet fonksiyonları ve sayısal imzalama yöntemleri kullanılmaktadır.

Mevcut blokzincir platformları, mahremiyet ve gizlilik içeren kullanım senaryolarını desteklemek için, çeşitli kriptografik teknikler ve bileşenler içermektedir. Halihazırda kullanılan bu bileşenlerin hepsinin kendi içinde avantajları ve dezavantajları bulunmaktadır. Blokzincir, değer zincirinde yer alan katılımcılar için mahremiyet ve gizliliği korurken, hesap verebilirlik ve şeffaflık sağlar. Bununla birlikte, kişisel veriler de ağ üzerinde tutulduğu için, blokzincirin kişisel verilerin korunması mevzuatına uygunluğu konusunda çalışmalar yapılmaktadır.

Kişisel verilerin korunmasına dair düzenlemeler, kişisel veri sahiplerinin yasal mevzuat kapsamında kendilerine tanınmış haklarına ilişkin başvurularını yöneltebilecekleri ve kişisel veri işleme faaliyetlerini mevzuat ile uyumlu şekilde gerçekleştirmekle yükümlü veri sorumlularının mevcudiyeti varsayımına dayanır. Blokzincir teknolojisinin merkezi olmayan yapısının veri sorumlusu gibi ara aktörleri ortadan kaldırması, merkeziyetçi bir yapı üzerine inşa edilmiş olan bu yasal düzenlemelerin uygulanmasını zorlaştırmaktadır. Temelde yaşanan bu zıtlık, blokzincir teknolojisi ile kişisel verilerin korunmasına dair düzenlemeler konularındaki tartışmaları yükseltmektedir. Blokzincir teknolojisinin kişisel verileri koruma kanunları ile tam uyumlu olduğu söylenemez. Bununla birlikte, söz konusu uyumsuzlukların giderilmesi için her geçen gün yeni öneriler ortaya çıkmaktadır. Her şeye rağmen blokzincir teknolojisinin, kişisel verilerin korunması kanunlarındaki yükümlülüklerin daha sağlıklı ve kolay şekilde yerine getirilmesine hizmet edecek pek çok özelliği olabileceği de dikkate alınmalıdır. Bu yönüyle blokzincir kişisel verilerin kullanımını kontrol etmeye yardımcı olan bir mekanizma olarak kabul edilebilir.

Kişisel verilerin korunması, teknolojiden çok teknolojinin nasıl kullanıldığıyla ilişkilidir. Dolayısıyla, tartışmaların sürdüğü ve blokzincir platformlarının bu tartışmalar ışığında olgunlaştığı bu geçiş döneminde; blokzincir teknolojisinin kullanılması zorunlu ise, kullanılacak alana uygun olan blokzincir türü seçilmeli, kullanım senaryoları ise mevcut düzenlemelerle azami uyumlu olacak şekilde tasarlanmalıdır.

Kapalı ve izin gerektiren blokzincir ağları, açık ve izin gerektirmeyen blokzincir ağlarına göre, kişisel verileri koruma kanunlarına daha uyumludur. Ancak kapalı ve izin gerektiren blokzincir altyapısı tercih edilse dahi, düzeltme ve silme haklarına ilişkin problem çözülemeyebilir. Bu nedenlerle, blokzincir üzerinde kişisel verilerin açık şekilde saklanmasından kaçınılmalı ve kişisel verilerin anonim bir şekilde saklanması için veri karıştırma, şifreleme, birleştirme teknikleri kullanılmalıdır.

Blokzincir teknolojisinin kitlesel olarak benimsenmesi için çözülmesi gereken bir diğer problem ölçeklenebilirliktir. İşlemlerin daha hızlı ve daha az maliyetle yapılabilmesi için birçok çözüm önerilmiştir. Bu sorunun protokol düzeyinde çözülüp çözülemeyeceği ve ademi merkeziyetçilikten taviz vermenin gerekip gerekmediği konusunda çok fazla tartışma da bulunmaktadır. İşlem kapasitesini arttırabilmek için önerilen bazı alternatif mutabakat mekanizmaları, güven garantilemek için bir tür izin katmanı oluşturulmasını önermektedir. Bu durum, belirli katılımcılara daha fazla güç verilmesini gerektirdiği için

ademi merkeziyetçilikten uzaklaşılmasına neden olacaktır. Kayıt defterinin daha küçük parçalara bölünmesi veya farklı kriptografik protokollerin kullanılması ölçeklenebilirlik sorununu çözmenin diğer yollarıdır. Yanzincirler (Sidechains) ve durum kanalları (State Channels), ölçeklenebilirlik problemlerini ortadan kaldırmak için önerilen başka yöntemlerdir. Bu durumlarda, kullanıcı etkileşimi blokzincirden farklı ikinci bir katmana taşınırken, katılımcılar arasında risksiz P2P işlemlerine izin verilmesi öngörülmektedir.

Durum kanalı ve yanzincir kavramları, sıklıkla birbirlerinin yerine kullanılan ve bu nedenle kitlesel karışıklığa neden olan iki terimdir. Yanzincirler, bir blokzincirde bulunan dijital varlıkların, farklı bir blokzincirde güvenli bir şekilde kullanılmasını ve gerekirse orjinal blokzincire geri taşınmasını sağlarlar. Yanzincirler, mevcut blokzincir yetkinliklerini geliştirmek için önemli bir potansiyele sahiptir. Durum kanalları ise, kullanıcıların normal şartlarda zincirde gerçekleşen işlemlerinin, zincir dışında yapılmasına olanak sağlayan, blokzincir üstü ikinci bir katman sunar. Bu katman, blokzincir platformlarının kendi aralarında ve diğer sistemlerle entegrasyonu için bir seçenek sağlar. Mevcut blokzincirleri birbirine bağlamak kolay bir iş olmamakla birlikte, farklı yaklaşımlar üzerinden bu sorunu çözmeye çalışan bir dizi blokzincir projesi bulunmaktadır.

Durum kanalları, mahremiyet açısından başvurulabilecek araçlardandır. Durum kanallarının aksine, bir yanzincir üzerindeki işlemler mahrem değildir. Yanzincir üzerinde yayınlanırlar ve böylece yanzincir üzerindeki her katılımcı tarafından görülebilirler.

Hayatımızdaki süreçler gün geçtikçe hızlanan bir şekilde sanal ortama taşınmaktadır. Bununla birlikte bazı süreçler hala sanallaştırılamamış veya kısmen sanallaştırılabilmiştir. Bunun başlıca nedenlerinden birisi, artan siber tehditlerden dolayı, bireyler lehine gelişen kişisel veri koruma kanunlarının gereklerini yerine getirmede yaşanan zorluklardır. Bir diğer neden ise, süreçlerin alt parçalarının çalıştığı, farklı otoritelere ait bilgi işlem sistemlerinin birbiri ile çevrim içi olarak bağlantılandırılmasına, sahipleri arasındaki güven eksikliği nedeniyle, zorunlu olmadıkça sıcak bakılmamasıdır. Çünkü bu sistemleri, mahremiyet, güvenlik, güven ihtiyaçlarını karşılayacak şekilde birleştirebilecek teknolojiler henüz olgunlaşmamıştır.

Bitcoin, bir otoritenin sahipliğine ihtiyaç duymadan yaşayan, hiçbir merkezi sisteme bağlı olmadan çalışabilen, birbirine güven sorunu olan tarafların bile birlikte sorunsuzca kullanabileceği, manipülasyonlara karşı önlemler içeren ilk sistemdir. Bitcoin ile beraber kriptopara ve blokzincir kavramları doğdu ve hızla gelişerek, küresel ölçüde kabul gören teknolojik kavramlara dönüştüler.

Bitcoin ve diğer kriptoparaların gösterdiği dayanıklılık, gereksiz aracıların süreçlerin içinden çıkması ile güvenlik, mahremiyet, hız ve maliyet avantajlarının uygulanabilir olduğu görüşünü yaygınlaştırdı. Blokzincir teknolojisi ile kriptopara dışındaki alanlarda, benzer ihtiyaçları karşılamak üzere harekete geçilmesi uzun sürmemiştir.

Mahremiyet (privacy), istenmeyen gözetlemeden uzak kalma ve kişisel/kurumsal bilgilerin paylaşılıp paylaşılmayacağına, paylaşılacaksa da kiminle ne zaman ve nasıl paylaşılacağına karar verme hakkı olarak tanımlanabilir. Gizlilik (confidentiality) ise, özel

bilginin gizli olarak kalmasıdır. Raporun odağı gizlilikten ziyade, verilerin istendiğinde paylaşımı ile ilgili konuları da içeren "blokzincir sistemlerinde mahremiyet" olacaktır.

Blokzincir teknolojisi, ademi merkeziyetçi bir ortamda gizlilik kaygılarını gidermek için yeni tekniklere ilham vermiştir. Farklı blokzincir sistemleri, farklı gizlilik özellikleri ve modelleri içerdiğinden; sistemlerde kullanılacak olan yaklaşım veya blokzincir teknolojisi kullanım senaryolarına özel olarak belirlenmelidir.

Bitcoin gibi açık (izinsiz) blokzincir sistemlerinde, katılım ve kayıt defteri herkese açıktır. Kullanıcı kimlikleri, kullanıcıların işlemlerinde kendilerini temsil etmek için ürettikleri sanal takma adların (veya "adreslerin") arkasında korunur. Öte yandan, işlem ayrıntıları sistemin kayıt defterinde açık olarak bulunmaktadır. Bu durumun yarattığı mahremiyet problemlerini azaltmak için; sisteme dahil olabilecek olan kullanıcıların sistemi işletenler tarafından belirlenebildiği, izinli blokzincirler ortaya çıkmıştır. İzinli blokzincirlerde, kayıt defterine erişebilecek olan ve işlem yapabilecek olan kişiler sınırlandırılmıştır. Tasarlanacak olan sistemin isterlerine göre, kullanılması gereken blokzincir türü de değişecektir.

Bu rapor, blokzincir güvenliğine ve mahremiyetine kapsamlı bir bakış sunmak amacıyla hazırlanmıştır. Okuyucunun, blokzincir alanındaki güvenlik ve mahremiyet konularındaki terminolojiyi anlaması ve mevcut kazanımlar hakkında bilgi sahibi olması hedeflenmiştir. Blokzincir teknolojisinin kendisi yeni ve anlaşılması yeterince güç olan bir teknoloji olduğu için, "Blokzincir ve Mahremiyet" konularının birlikte ele alındığı bir raporu anlamak okuyucu açısından kolay olmayacaktır. Bu nedenle, rapor hazırlanırken, blokzincir teknolojisinin mahremiyet özelliklerinin daha kolay anlaşılabilmesi için gerekli olan bilgilerin verilmesine dikkat edilmiştir. Blokzincir teknolojisine ait temel bilgiler, artık yaygın şekilde bilinir hale geldiği için raporun kapsamına alınmamıştır.

Raporun Yapısı

Bu raporun bir sonraki bölümünde, blokzincir platformlarından beklenen temel güvenlik ve mahremiyet özellikleri açıklanmaktadır. Bölüm 3'te, temel kriptografi ilkeleri, gelişmiş güvenlik yapı taşları ve algoritmaları ve blokzincir tabanlı uygulamalarda kullanılan bazı kriptografi dışı teknikler özetlenmiştir. 4. bölümde, mahremiyet sağlayan kriptopara sistemleri ve geleneksel bankacılık sistemleriyle uyumlu olan banka aracılı sistemler kısaca açıklanmıştır. Daha sonra, mahremiyet odaklı blokzincir platformları tanıtılarak güvenlik ve mahremiyet özellikleri değerlendirilmiştir. Ek olarak, GDPR ve KVKK bağlamında mahremiyet sorunları tanımlanmış ve blokzincir projelerinde uygulanması için fırsat ve zorluklar gösterilmiştir. Bölüm 5, blokzincir sistemlerinin daha ölçeklendirilebilir hale gelmesi ve kitlesel olarak benimsenmesi için önerilen yanzincir ve durum kanalı mekanizmalarını kapsamaktadır. Ek olarak, farklı blokzincir platformları ve dağıtık kayıt teknolojileri arasındaki birlikte işlerlik konularına odaklanan blokzincir projelerine kısa bir bakış sunulmuştur.

BLOKZİNCİRDE GÜVENLİK VE MAHREMİYET ÖZELLİKLERİ

Bu bölümde, blokzincir teknolojisinde bahsi geçen güvenlik ve mahremiyet yetenekleri açıklanmaktadır.

2.1 Güvenlik Özellikleri

Öncelikle çevrim içi işlemlerin açıklarını hedef alan güvenlik gereksinimleri tartışılmaktadır. Daha sonra, blokzincirin ilk uygulaması olan Bitcoin temel alınarak, blokzincirin temel ve doğal güvenlik özellikleri açıklanmıştır. Son olarak, bazı blokzincir sistemlerinde bulunan veya birçok blokzincir uygulaması tarafından ihtiyaç duyulan önemli ek güvenlik özellikleri sunulmaktadır.

2.1.1 Çevrim İçi İşlemlerin Güvenlik Gereksinimleri

Çevrim içi işlemlerde güvenlik gereksinimleri genel olarak aşağıdaki başlıklarda sınıflandırılır.

İşlemlerin Bütünlüğü

Yatırım ve varlık yönetimi için çevrim içi işlemler kullanılırken öz kaynaklar, tahviller, notlar, gelir kuponları, depo makbuzları ve diğer varlıklar farklı aracılar tarafından yönetilmektedir. Bu durum yalnızca işlem maliyetlerini artırmakla kalmaz, sertifikaların kasıtlı olarak tahrif edilmesi veya sahtekarlık risklerini de beraberinde getirir. Bu nedenle sistem, işlemlerin bütünlüğünü garanti etmeli ve tahrif edilmesini önlemelidir.

Erişim Denetimi

Blokzincirde tutulan dijital varlıklar üzerinde, sadece o varlık üzerinde yetkisi olan kişilerin, yetkisi olan işlemleri yapabilmesi sağlanmalıdır.

Sistem ve Verilerin Kullanılabilirliği

Çevrim içi bir sistemin kullanıcılarının işlem verilerine istedikleri zaman, istedikleri yerden erişebilmeleri gerekir. Sağlanması gereken kullanılabilirlik, hem sistem hem de işlemler için olmalıdır. Sistemin bir ağ saldırısı altında olmasına rağmen güvenilir bir şekilde çalışması beklenir. İşlem verileri, tutarsızlık ve bozulma olmadan yetkili kullanıcılar için erişilebilir olmalıdır.

Çifte Harcama Koruması

Merkezi olmayan bir ağda dijital para alım satımında önemli bir zorluk, çifte harcamaların, yani bir parayı birden fazla kez harcamanın önlenmesidir (Not: Aslında bu kavram,

yetkisinden çıkmış bir dijital varlık üzerinde, yetkisi varmış gibi tekrar aynı işlemi yapmaya çalışma olarak bütün blokzincir türleri için genelleştirilebilir). Merkezi bir ortamda, dijital bir para biriminin iki kez harcanmış olup olmadığının doğrulanmasından güvenilir bir merkezi üçüncü taraf sorumludur. Merkezi olmayan bir ağ ortamında ise; çifte harcamayı önlemek için sağlam güvenlik ve mutabakat mekanizmalarına ve önlemlere ihtiyaç vardır.

2.1.2 Blokzincirde Temel Güvenlik Özellikleri

Blokzincirin temel güvenlik özellikleri, hem kriptografideki gelişmeler hem de Bitcoin'in tasarım ve gerçeklemesi üzerine şekillenmiştir. Blokzincir, kurcalamaya karşı direnç, Dağıtık Hizmet Engelleme (DDoS) saldırısına direnç, takma adlılık ve çift harcama saldırısına karşı direnç gibi bir dizi doğal güvenlik özelliğini sağlayacak şekilde geliştirilmiştir. Ancak, güvenli dağıtılmış depolama amacıyla blokzincir kullanmak için ek güvenlik ve mahremiyet özellikleri gereklidir. Takip eden bölümde, temel güvenlik özellikleri irdelenmiştir.

Kurcalamaya Direnç

Kurcalama direnci, bir sistem, ürün veya mantıksal/fiziksel nesnenin, kendi kullanıcılarının veya erişim sağlamış kötü niyetli kişilerin kasıtlı kurcalamasına karşı direnci anlamına gelir. Blokzincirde kurcalama direnci, blokzincirde depolanan herhangi bir işlem bilgisinin blok oluşturma sırasında ve sonrasında değiştirilememesidir. Örneğin, Bitcoin'de işlem bilgilerinin tahrif edilmesinin iki olası yolu vardır:

1. Madencilerin kullanıcıların gönderdiği işlem bilgisine (alıcı, miktar gibi) müdahale etmesi,

2. Saldırganların blokzincirde saklanan bilgileri değiştirmesi.

Bu tür kurcalama girişimleri, Bitcoin protokolleri tarafından şu şekilde önlenmektedir.

Bitcoinde her bir transfer göndericisi tarafından ECDSA gibi güvenli bir imza algoritması kullanarak imzalanır, madencilik yoluyla doğrulama ve onay için tüm ağa gönderilir, ağdaki birden fazla madenci bu transferi alır ve işler. Bir madenci işlemle ilgili herhangi bir bilgiyi değiştirirse, diğer madencilerin imza denetiminde ortaya çıkacaktır. Çünkü madenci, değiştirdiği bilgiler üzerine, transferi gönderenin gizli anahtarı olmadan geçerli bir imza atamaz. İlk tür kurcalamaya karşı direnç, taklit edilemez güvenli imza algoritmaları kullanılarak garanti edilir.

İkinci tür kurcalamada bir saldırgan, blokzincirinde saklanan geçmiş verileri değiştirmeye çalışır. Bu durumu önlemek için Bitcoin iki koruma tekniğinden faydalanır: özet işaretçisi (hash pointer) uygulaması ve blokzincirin hem depolanması hem de doğrulanması için ağ geneline yayılmış destek mekanizması. Saldırgan bir bloktaki verileri değiştirirse, karşılaşacağı ilk zorluk uyumsuzluk problemidir. Bir blok değiştirildiğinde, o blokun özet değeri de değişmiş olur. Bitcoinde, her bir blokta, kendisinden önce gelen blokun özet değeri bulunduğu için; bu durum sadece o bloku değil, kendisinden sonra gelen bütün blokları da etkiler. Burada, blok kurcalanmış olsa bile aynı özet değerine

sahip olabilir mi sorusu akla gelebilir. Bu durum, çakışma direncine sahip bir özet fonksiyonu kullanılarak önlenir. (Özet fonksiyonları için Bknz. Bölüm 3.1.1). Dahası, Bitcoin'in kayıt defterinin kopyası ağda bulunan herkeste vardır. Kısacası, Bitcoin'deki her bir işlem imzalanıp, ağın tüm düğümleri arasında dağıtıldığı için, ağın haberi olmadan işlem verilerini kurcalamak pratik olarak imkansızdır. Bu, kayıt defterinin depolanması ve dağıtımında görev alan topluluğun gücünü gösterir. Bu özellik birçok uygulama alanı için istenen bir özelliktir. Örneğin; sağlık hizmetlerinde, blokzincir, değişmez denetim delilleri oluşturmaya, sağlık kayıtlarının güvenilirliğini sürdürmeye ve hasta verilerinin bütünlüğünün korunmasına yardımcı olabilir.

DDoS Saldırılarına Karşı Direnç

Dağıtık Hizmet Engelleme Saldırısı(DOS), hedef makineyi veya üzerindeki servisleri, kullanıcıları tarafından kullanılamaz duruma getirerek, verilen İnternet hizmetlerini kesintiye uğratan bir siber saldırı türüdür. DoS saldırıları, ana bilgisayarı gereksiz isteklere boğarak, meşru hizmetlerin yerine getirilmesini durdurmaya, ana bilgisayar sistemini veya ana bilgisayar ağ kaynağını aşırı yüklemeye çalışır [McD13]. DDoS saldırısı "dağıtılmış" bir DoS saldırısı anlamına gelir, yani bir kurbana gelen istekler, İnternet üzerine dağılmış birçok farklı kaynaktan oluşturulmuş olabilir. Bir DDoS saldırganı, güvenlik açıkları veya zayıflıklarından yararlanarak bazı kişisel bilgisayarları başka bir bilgisayara saldırmak için ele geçirip kullanabilir. Bir DDoS saldırganı, bu şekilde ele geçirdiği bir bilgisayar kümesini kullanarak bir web sitesine büyük miktarda veri gönderebilir veya belirli e-posta adreslerine çöp mesajlar gönderebilir [McD13]. Bu durum, bilgisayarları tek tek engelleyerek saldırıyı önlemeyi çok zorlaştırır. Bir blokzincire yapılan DDoS saldırısındaki ciddi endişe, DDoS saldırganlarının blokzincirin bir parçasını veya tamamını çökerterek, blokzinciri erişilemez duruma getirmesi ihtimalidir. Bu ihtimal, blokzincir sistemlerinin merkezi olmayan mimarisi ve işleyişi ile blok üretimi ve üretilen bloğun blokzincire eklenmesi için mutabakat protokolü kullanılması sayesinde önlenir. Blokzincir işlemleri, birkaç düğümün çevrim dışı olmasına rağmen devam edebilir. Bir siber saldırganın blokzinciri çevrim dışı bırakmayı başarabilmesi için, blokzincir ağındaki düğümlerin ezici bir bölümünü tehlikeye atmaya yetecek kadar hesaplama kaynağı toplaması gerekir.

Çifte Harcama Saldırısına Karşı Direnç

Bitcoin blokzinciri bağlamındaki çifte harcama saldırısı, dijital para birimi işlemlerine özgü belirli bir soruna işaret eder. Çifte harcama saldırısı, dijital bilgilerin nispeten kolayca yeniden üretilebilmesi nedeniyle genel bir güvenlik kaygısı olarak değerlendirilir. Spesifik olarak, elektronik para birimi gibi dijital jeton alışverişinde bulunan işlemlerde, sahibinin dijital jetonu çoğaltması ve birden fazla alıcıya aynı jetonu göndermesi riski vardır. Çifte harcamaları önlemek için Bitcoin, bir uzlaşma protokolü ile blokzincirdeki işlem kayıtlarını kullanarak her bir işlemin doğruluğunu değerlendirir ve doğrular. Gerçekleşen bütün işlemler blokzincirde kayıtlı olduğu ve uzlaşma protokolü sayesinde bloklar global blokzincire dahil edilmeden önce ağdakiler tarafından kontrol edildiği

için, her bir işlemin göndericisinin yalnızca yasal olarak sahip olduğu bitcoinleri harcadığından emin olunur. Sayısal imzalarla imzalanan işlemlerin ve çoğunluk oyu ile yapılan işlemlerin halka açık olarak doğrulanması, blokzincirin çifte harcama saldırısına karşı dirençli olacağının garantisidir.

Çoğunluğa Direnç (%51) Mutabakat Saldırısı

Bu saldırı, mutabakat protokolündeki hile risklerini ifade eder. Bu tür risklerden biri, özellikle çifte harcama bağlamında, genellikle (%51) saldırısı olarak adlandırılır. (%51) saldırısı, kötü niyetli madencilerin varlığında ortaya çıkabilir. Bir madenci blokzincirde bulunan hesaplama gücünün %50'sinden fazlasını kontrol ederse işlemlerde oynamalar yaparak ağın doğruluğunu bozabilir. (%51) saldırısının bir başka örneği, bir grup madencinin doğrulama aşamasında oylar sayılırken komplo yapmak için işbirliği yapması durumunda ortaya çıkabilir. Güçlü bir kullanıcı veya bir grup kötü niyetle işbirliği yapan kullanıcı blokzinciri kontrol ederse, çeşitli güvenlik ve mahremiyet saldırıları başlatılabilir. Örneğin; çifte harcama yapmak, orijinal işlemleri asla gerçekleşmemiş gibi tersine çevirmek, bazı kullanıcıların işlemlerini engellemek gibi.

2.2 Blokzincirlerde Mahremiyet Özellikleri

Her ne kadar Bitcoin'deki blokzincir temel güvenlik özelliklerini sağlıyor olsa da (kurcalamaya ve DDoS saldırılarına karşı direnç), genel amaçlı bir blokzincir sistemi, dijital para birimi sistemleri ve dağıtılmış global defter hizmetleri için kritik olan bir dizi mahremiyet özelliğine de ihtiyaç duyabilir. Bu bölümde, bu tür ek özelliklerden bir kaçı [ZXL19]'dan özetlenmiştir.

2.2.1 Takma adlar

Takma adlandırma (Pseudonymity), gizlenmiş bir kimlik durumunu ifade eder. Bitcoin'de adresler, ağdaki bir düğümün ve/veya eşlerin (kullanıcı) açık anahtarlarının özet değerleridir. Kullanıcılar, gerçek isimlerini açıklamadan, açık anahtarlarının özet değerlerini takma kimlikleri olarak kullanarak sistemle etkileşime girebilirler. Böylece, bir kullanıcının kullandığı adres sahte bir kimlik olarak görülebilir. Sistemin takma adlar ile çalışması, kullanıcının gerçek kimliğini korumaya yarayan bir mahremiyet özelliği olarak görülebilir. Ek olarak, kullanıcılar, birden çok banka hesabı açmaya benzer şekilde istedikleri sayıda anahtar çifti (çoklu adres) oluşturabilirler. Açık anahtarların özet değerlerinin takma ad olarak kullanılması zayıf bir anonimlik sağlıyor gibi görünse de kullanıcıların kimlik bilgilerinin açığa çıkma riski devam etmektedir.

Kullanıcıların Kimliğinin Mahremiyeti

Kullanıcı verilerinin çeşitli finans kuruluşları arasında etkin ve güvenli bir şekilde paylaşılmasının zorluğu, kimlik doğrulama işlemlerinin tekrar tekrar yapılması ile maliyetleri arttırabilir.

Ayrıca, bazı aracılar tarafından kullanıcı kimliklerinin ifşa riskini de dolaylı olarak getirir. Ek olarak, işlemin paydaşları bazı durumlarda gerçek kimliklerini diğer tarafa bildirmek istemeyebilirler.

2.2.2 Bağlantısızlık

Bağlantısızlık (unlinkability), sistem içerisinde gözlenen iki öge arasındaki ilişkinin ifade edilememesi veya yüksek doğrulukla belirlenememesidir. Anonimlik ise kimliğin saklı olup belirlenememesi durumunu ifade eder. Her ne kadar Bitcoin benzeri blokzincirler, takma ad kullanımını desteklese de kullanıcının işlemlerinin bağlantısızlığını sağlamada başarısız olur. Bir kullanıcının tam anonimliği, ancak takma ad kullanımı ve bağlantısızlık beraber olursa korunabilir.

Bitcoin benzeri sistemlerde, bir kullanıcı birden fazla takma ada sahip olabilir. Fakat, bu kullanıcılar için mükemmel bir anonimlik sağlamaz; çünkü kaydedilen her işlemde göndericinin ve alıcının adresleri bulunur ve işlemler bu adresleri bilen herkes tarafından serbestçe izlenebilir. Dolayısıyla, Bitcoin transferlerinde kullanılan adreslerin basit istatistiksel analiziyle, bir kullanıcının transferleri ve takma adları birbirleriyle ilişkilendirilebilir. Örneğin, gönderenin hesabını analiz edilerek, bu hesaba giren/çıkan bitcoin sayısı ve toplam miktar kolayca öğrenilebilir. Aynı IP adresini kullanarak işlem gönderen/alan hesaplar birbirleri ile bağlantılandırılabilir. Bir kullanıcının kullandığı takma ad ile gerçek kimliği eşleştirilirse, o takma ad ile gerçekleştirilmiş olan bütün işlemlerin de gizliliği ve dolayısıyla mahremiyeti ortadan kalkar. Dolayısıyla Bitcoin, takma adlı olma özelliğini sağlar ancak bağlantısızlığı sağlayamaz. Bu nedenle tam bir anonimlik sağladığını söyleyemeyiz.

İşlemlerin Bağlantısızlığı

Bir kullanıcıyla ilgili tüm işlemler bağlantılandırılabildiğinde, kullanıcı hakkında hesap bakiyesi, işlem türü ve sıklığı gibi başka bilgilere ulaşmak kolaylaşır. İşlemler ve hesaplarla ilgili bu tür istatistiki verilerin meraklı veya kötü niyetli kişiler tarafından, kişi hakkındaki bazı geçmiş bilgilerle birlikte kullanılması, kullanıcının gerçek kimliğini yüksek ihtimal ile tahmin edilebilir hale getirir.

2.2.3 İşlemlerin Mahremiyeti ve Veri Gizliliği

Blokzincirde veri gizliliği, blokzincirin bütün veriler veya belirli hassas veriler için mahremiyet sağlamasını ifade eder. Her ne kadar blokzincirin ilk uygulama alanı kriptoparalar da olsa; akıllı sözleşmeleri yönetmek, telif hakkıyla korunan işleri, ticari veya kurumsal sicilleri dijitalleştirmek gibi pek çok alanda kullanılabilir. Bu sebeple, blokzincir uygulamalarının, işlem içeriği (örneğin, Bitcoin'deki işlem tutarları) ve adresler gibi işlem bilgilerinin mahremiyetini sağlanmasına ihtiyaç duyulur. Ne yazık ki bu güvenlik özelliği Bitcoin sistemlerinde desteklenmemektedir. Bitcoin'de gönderici ve alıcının gerçek kimliği yerine takma adları kullanılsa da işlemlerin içeriği ve adresler herkes tarafından görülebilir. İşlem içeriğinin gizli tutulması, takma adın gerçek kullanıcı kimliği ile ilişkilendirilmesi riskini azaltmaya yardımcı olur.

Ethereum gibi karmaşık işlemlerin gerçekleştirilmesi için akıllı sözleşmeler kullanan blokzincir sistemleri (1) sözleşmelerin verilerinin ve veriler üzerinde yürütülen kodların herkese açık olmasını ve (2) her sözleşmeyi her madencinin işletmesini de gerektirir. Bu durum, kullanıcı bilgilerinin sızmasına yol açabilir. Örneğin, bir saldırgan, belirli bir zamanda belirli bir miktarda kripto parayı aralarında değiştirdiklerini bildiği kullanıcıların kimliklerini blokzincir üzerinden bulabilir. Bu nedenle, akıllı sözleşmelerin gizliliğini korumak için daha güçlü koruma mekanizmaları tasarlamak ve uygulamak çok önemlidir.

İşlemlerin Mahremiyeti

Çevrim içi finansal işlemler gerçekleştiren kullanıcıların çoğu, yaptıkları işlemlerin ve hesap bilgilerinin en az düzeyde açığa çıkmasını ister. Bu en az seviye aşağıdakileri içerir:

- Kullanıcıların işlem bilgilerine yetkisiz herhangi bir kullanıcı tarafından erişilmemesi,
- Sistem yöneticisinin veya ağın katılımcılarının, hiçbir kullanıcının bilgisini izni olmadan başkalarına ifşa edememesi;
- Tüm kullanıcı verilerinin, beklenmeyen hatalar veya kötü niyetli siber saldırılar altında bile tutarlı ve güvenli bir şekilde saklanması ve erişilebilmesidir.

Bu seviyede bir mahremiyet finansal olmayan bir çok senaryoda da arzu edilir.

BLOKZİNCİR UYGULAMALARINDAKİ GÜVENLİK VE MAHREMİYET YAPI TAŞLARI

Bu bölümde, blokzincir platformlarında ve uygulamalarında kullanılan kriptografik yapıtaşları ve Mixcoin, Coinjoin gibi anonimleştirme yöntemleri özetlenmiştir. Bölümün içeriği, temel kriptografik algoritmalar, mahremiyet amaçlı kriptografik yapı taşları ve kriptografik olmayan yapıtaşları olmak üzere üç alt bölümden oluşur.

3.1 Temel Kriptografik Algoritmalar

3.1.1 Özet Fonksiyonları

Kriptografik *özet fonksiyonları*, rastgele boyuttaki verileri sabit bir boyut dizesine eşleyen bir algoritma olarak tanımlanmaktadır. Özet fonksiyonlarının genellikle tek yönlülük ve çakışma direnci adlı iki güvenlik gereksinimini karşılaması beklenir. İlki, özet fonksiyonunun tersine çevrilememesini sağlarken, ikincisi aynı özet değerine sahip iki farklı mesaj bulmanın kolay olmadığını gösterir. Çıktı boyu η-bit olan bir özet fonksiyonu için, tek yönlülüğü kaba kuvvet saldırısı ile kırma karmaşıklığı $O(2^2)$ iken doğum günü saldırısı ile çakışma bulma karmaşıklığı $O(2^n)$ ile sınırlıdır. Bu nedenle, 80-bit güvenlik sağlamak için özet fonksiyonun çıktı uzunluğu en az 160-bit olmalıdır.

Blokzincirlerde kullanılan en popüler özet fonksiyonu, SHA (Secure Hash Algorithms) adlı bir özet fonksiyonu ailesinin algoritmalarından biri olan SHA256'dır. SHA algoritmaları, ABD Federal Bilgi İşleme Standardıdır ve ilk versiyonu olan SHA0 adı ile 1993'te yayınlanmıştır. Daha sonra SHA1 (1995'te yayınlandı), SHA2 (2001'de yayınlandı) dahil olmak üzere bu ailedeki algoritmaların çoğu Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (NSA) tarafından tasarlanmıştır. 2014 yılında yayınlanan SHA3 algoritması orijinal ismi ile Keccak algoritmasından, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yalnızca dolgu yöntemi değiştirilerek standartlaştırılmıştır. Keccak, 2008 yılında NIST tarafından başlatılan ve 2012'de sona eren NIST özet fonksiyon yarışmasının galibi oldu. Mevcut güvenlik gereksinimlerini karşılamak için, blokzincirler ve kripto para birimlerinde SHA2 [Rad12] ve SHA3 [Dwo15] kullanılması tavsiye edilmiştir.

Kabaca, özet fonksiyonlarının blokzincirlerde kullanımlarını aşağıdaki altı kategoriye ayırabiliriz:

- Emek ispatı (ing. proof-of-work (a.k.a., coin mining) (PoW)),
- Adres oluşturma (address (Addr) generation),
- Blok oluşturma (Merkle-ağacı (MKT) paradigmasının bir parçası olarak),
- İmzalardaki mesaj özeti (ing. message digest in signatures (MDS)),
- Sanki rassal sayı üretimi (ing. pseudorandom number generation (PNG)),
- Köprü yapıları (ing. bridge components) (Fiat-Shamir mekanizmasında olduğu gibi).

Son dört kullanım blokzincirinin ortaya çıkmasından önce bile oldukça yaygın kullanılırken, ilk ikisi kripto paralar ve blokzincirler ile birlikte son zamanlarda kullanılmaya başlandı.

Madencilik teknikleri ve yeni özet fonksiyonların tasarımları arasında ilginç bir çekişme başlamıştır. Madencilik tekniklerinin gelişimi madenciler için heyecan verici bir şey olsa da, blokzincirin kendisi için kötü bir haber olabilir. Özellikle, gelişmiş madencilik teknikleri bazı işletmelerin diğerlerinden daha yüksek madencilik hızına sahip olmasını sağlar ve kötüye kullanılırsa, iyi bilinen %51 saldırısı daha yüksek bir olasılıkla gerçekleşme riskini artırır.

Madencilik tekniklerinin gelişimi ile ortaya çıkan problemlerle mücadele etmek için, Ethash gibi birçok özet fonksiyonu önerilmiştir [W+14], SCrypt [Per09], X11 [X11] and Equihash [BK17].

- Keccak256 ve Keccak512'den türetilen ve Ethereum-tabanlı kripto para birimlerinde kullanılan Ethash, ASIC-dayanıklı bir hash fonksiyonu olarak kabul edilir. Ancak, Etherscan 15 Aralık 2017'de en yüksek ortalama özet alma oranının 140 THash/s olduğunu bildirmiştir.
- Percival tarafından önerilen ve IETF tarafından RFC 7914 olarak yayınlanan ve Tenebrix, Fairbrix ve Litecoin gibi birçok kripto para biriminde kullanılan SCrypt, bellek zorlu (ing. memory-hard) bir özet fonksiyonu olarak kabul edilir. SCrypt'in asimptotik olarak Bitcoin'de kullanılandan daha fazla bellek gerektirdiği iddia ediliyor. Ancak, InnoSilicon, 620 MHash/s hızında SCrypt için A4 + LTC Master cihazlarını geliştirdi.
- X11, Duffield tarafından önerilen ve X11'i oluşturmak için SHA3 adaylarından seçilen 11 özet fonksiyonunu sırayla birleştiren başka bir bellek-zorunlu özet fonksiyonudur. Bu özet fonksiyonları arasında Blake, Grostl, JH, Keçe, Skein, ECHO, Luffa, BMW, CubeHash, SHAvite ve SMID bulunur. X11 şimdi Darkcoin'de kullanılmaktadır. Ancak InnoSilicon, X11 için 32.5 GHash/s işlem kapasiteli ASIC cihazlarını tarafından geliştirdiklerini de iddia etti.
- ZCash'te önerilen Equihash, n,k, ve d parametresi tarafından belirtilen yeni bir bellek zor karma işlevidir ve amaç, belirli koşulları sağlayan 2^k sayılarını bulmaktır.

Şekil 3.1: **ECDSA Algoritmasının Tanımı**

ECDSA specified as **secp256k1**:

KeyGen: $(\mathbb{E}, q, a, b, G, n, h; d, Q)$

- $\mathbb{E}$: an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_q$
- q: a prime $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
- a, b: $a = 0,\ b = 7$
- G, n: a random base point in $\mathbb{E}$ with prime order n
- h: a hash, instantiated with **SHA1**
- Signing key: $d \xleftarrow{\$} [1, n-1]$
- Verification key: $Q = dG \in \mathbb{E}$

Sign$(d; m)$: $(r, s) \in \mathbb{F}_q^2$ where

- r: the non-zero x-coordinator of point kG for some $k \xleftarrow{\$} [1, n-1]$
- s: $s = k^{-1}(h(m) + d \cdot r) \bmod n$

Verify$(Q; r, s)$: $(r, s \overset{?}{\in} [1, n-1])$ and $(v \overset{?}{=} r)$, where

- v: the x-coordinator of point $s^{-1}(h(m)G + rQ) \in \mathbb{E}$.

3.1.2 Sayısal İmzalar

Özet fonksiyonlarının yanı sıra, sayısal imzalar da blokzincirlerde sıkça kullanılan bir başka kriptografik yapıtaşıdır. Sayısal imza kavramı, 1976'da açık anahtar şifreleme mantığının Diffie ve Hellman tarafından bulunması ile birlikte ortaya çıkmıştır [DH76]. Temel bir kriptografik yapıtaşı olarak, kaynak doğrulaması, inkar edilemezlik ve bütünlük özelliklerini sağlamak için sayısal imza kullanılır. Sayısal imzanın güvenliği, varoluşsal taklit edilemezlik uyarlamalı mesaj saldırılarına (ing. existential unforgeability adaptively chosen messages attacks EUF-CMA) karşı dayanıklılığı gerektirir. Bu da saldırganın, imza hizmetini sağlayabilecek imzalama servisine (oracle) erişebilse bile, yeni bir mesajda geçerli bir imza alamayacağını garanti eder.

ECDSA [Certicom-Research, 2000] ve EdDSA [BDL+12], blokzincirlerinde sıklıkla kullanılan iki sayısal imza şemasıdır. Prensip olarak, her ikisi de ayrık logaritma probleminin eliptik eğri versiyonunun güvenliğine dayanmaktadır. ECDSA genel bir eliptik eğri üzerinde çalışır ve günümüzde Bitcoin ve Ethereum (bkz. Şekil 3.1) yapılarında da kullanılırken, EdDSA (bkz. Şekil 3.2) bükülü (ing. twisted) Edward eğrileri üzerinde çalışır ve günümüzde Naivecoin ve Monero gibi yapılarda kullanılmaktadır. Edward eğrisi, eliptik bir eğrinin düzlem modelidir ve genel bir eliptik eğriden hız açısından daha verimli ve güvenlidir. Bu nedenle, IRPWG (Internet Research Professional Working Group) tarafından TLS'nin bir sonraki eliptik eğri çeşidi olarak seçilmiştir.

Şekil 3.2: **EdDSA Algoritmasının Tanımı**

EdDSA specified as **ed25519**:

KeyGen: $(\mathbb{E}, q, d, G, l, h; a, A)$

$\mathbb{E}$: an Edward elliptic curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbb{F}_q$

q: a prime $2^{255} - 19$

d: $-\frac{121665}{121666} \in \mathbb{F}_q$

G, l: a random base point in $\mathbb{E}$ with prime order l

h: a hash, instantiated with SHA512

Signing key: $a \xleftarrow{\$} [1, l-1]$

Verification key: $A = aB \in \mathbb{E}$

Sign$(a; m)$: $\langle R = rB, s = r + a \cdot h(A \parallel R \parallel m) \rangle \in \mathbb{E} \times \mathbb{Z}_l$

where $r \xleftarrow{\$} [1, l-1]$.

Verify$(A; R, s)$: $sB \stackrel{?}{=} R + h(A \parallel R \parallel m)A$

3.2 Gizlilik ve Anonimlik Amaçlı Kriptografik Algoritmalar

3.2.1 Gelişmiş Sayısal İmzalar

İşlemlerin gizliliğini ve mahremiyetini artırmak için, halka imzası (ing. ring signature), grup imzası (ing. group signature) ve çoklu imza (ing. multi-signature) gibi bazı gelişmiş imza şemaları blokzincirlerde yaygın olarak uygulanır.

Halka İmzalar

Halka imzası (Ring signature) kavramı ilk olarak 2001 yılında Rivest, Shamir ve Tauman tarafından önerilmiştir. Halka imzalar bir kişinin, kendisini de içerecek şekilde bir grup adına, grubun diğer üyelerinin iznine gerek olmadan ve kendi kimliğini ifşa etmeden bir mesaja imza atabilmesini sağlar. *Varoluşsal taklit edilemezlik* (ing. existential unforgeability) yanında, *koşulsuz anonimlik* (ing. unconditional anonymity) halka imzalar için bir diğer önemli güvenlik şartıdır. Bu yeni güvenlik özelliği iki alt özelliğe ayrılabilir: izlenemezlik (ing. untraceability) ve bağlantı kuramazlık (ing. unlinkability). İlki, imzalayanın tanımlanamaması anlamına gelir, ikincisi ise hiç kimsenin aynı imzalayan tarafından iki imza oluşturulup oluşturulmayacağına karar veremeyeceğini belirtir. Koşulsuz anonimlik, iki ucu keskin bir kılıç olan güçlü bir güvenlik anlayışıdır: Bir yandan, bireysel imzalama davranışlarına karşı mükemmel gizlilik koruması sağlar; öte yandan, yasal olmayan alım-satım gibi bir amaç için kötüye de kullanılabilir. Bu nedenle, anonimlik konusunda bazı kısıtlamalar dikkate alınmalıdır.

Aslında, halka imza kavramını ortaya çıkmasından on yıl önce, Chaum, grup imzalama yöntemini tanımlamıştır. Grup imzada bir kişinin bir grup adına anonim olarak bir mesaj üzerine imza atmasına olanak sağlar. Ancak, önceden tanımlanmış grup yöneticisi grup adına imza atanı gerektiğinde ortaya çıkarabilmektedir. Grup imzası ile halka imzası arasındaki ana fark, halka yapısı, bir kısıt gerektirmeden anında bir amaçla (ad hoc) oluşturulabilirken, grup imzası, grup yöneticisinin kontrolü altında oluşturulabilmektedir. Ayrıca, grup imzada gruba katılmak isteyen herkes ilk önce çevrim içi veya çevrim dışı bir kayıt işlemi gerçekleştirmelidir.

2004 yılında Liu ve arkadaşları [LWW04], bağlanabilir spontan anonim grup (ing. linkable spontaneous anonymous group(LSAG)) imza şemasını önermiştir. LSAG imza şeması spontane grup oluşumunu göz önünde bulunduran ve grup yöneticisi gerektirmeyen, kendiliğinden anonim bir grup imzalama tekniğidir. Son zamanlarda, Back, Liu ve arkadaşlarının yaklaşımını baz alarak gerekli iyileştirmeler ile daha verimli olan Ring-Coin'i önerdi. Başka bir bakış açısıyla, Fujisaki ve arkadaşları 2007 yılında, imzaya bir eklenti (issue-related tag) yaparak halka imza kavramını genişletti ve izlenebilir olmasını sağladı. Bu durumda, bir kişi, aynı mesaja halkadaki başka bir kişi adına imza atarsa kimliğinin açığa çıkarma riskiyle karşı karşıya kalacaktır. Bu fikir çift harcamaları önlemek için oldukça fayda sağlamakta ve günümüzde bazı değişikliklerle CryptoNote'un temelinde kullanılır hale gelmiştir.

Ancak, CryptoNote veya Ring-Coin, belirli bir işlemde gönderilen tutarların gözlenmesi ve analizine dayanan saldırılara maruz kalabilir (Noether, 2015). Maxwell, herhangi bir işlemde tutarları gizlemek için homomorfik taahhüt protokolünü kullanarak gizli işlem kavramının kullanılmasını önermiştir. Daha sonra, Noether, bu üç tekniği birleştirerek Monero protokolü için bir değişiklik önermiştir: (1) Maxwell'in gizli işlemi, (2) halka imzası ve (3) çok katmanlı, bağlanabilir spontane, anonim grup imzası (ing. multilayered linkable spontaneous, anonymous group signature (MLSAG)). Noether'in bu fikri artık Monero'da kullanılmakta ve Halka Gizli İşlemleri (ing. Ring Confidential Transactions - RingCT) olarak adlandırılmaktadır.

2017 yılında Sun ve ark. tarafından RingCT 2.0 olarak adlandırılan RingCT'ye yönelik bir iyileştirme sürümü önermiştir. RingCT'nin güvenlik modelleri, söz diziminin titiz bir şekilde biçimlendirilmesinin yanı sıra, RingCT 2.0 da önemli depolama ve iletişim maliyet tasarrufu elde etmek için tek yönlü alana sahip olan akümülatör ve Pedersen taahhüdü de dahil olmak üzere bazı iyi bilinen kriptografik yapı taşları eklenmiştir. Daha spesifik olarak, imza boyutu O(nm)'den O(m)'e düşürülür, burada n ve m sırasıyla halkadaki grup sayısı ve her bir gruptaki hesapların sayıdır. Başka bir deyişle, RingCT 2.0'daki işlem büyüklüğü, halkadaki grup sayısından bağımsızdır ve bu özellik her blokun daha fazla transfer işlemini içermesini sağlar.

Verimlilik özelliği kriptografik yapı taşı veya algoritma seçimi için önemli hususlardan biridir. Ancak, mevcut bağlanabilir halka imza şemaları (ing. linkable ring signature schemes) O(1) imza büyüklüğüne sahip olmasına rağmen blokzincirlerde doğrudan uygulanmaz. Bu durumun asıl nedeni, "güvenilir kurulum" (ing. trusted setup) problemidir. Güvenilir kurulum gereken durumlarda, merkezi olmayan blokzincir konseptine aykırı olarak sistem parametresini dağıtmak için güvenilir üçüncü bir taraf gerekmektedir. Ancak, bu durumun kademeli olarak da iyileşebileceğine inanılmaktadır.

Yakın zamanda, RingCT 3.0 da önerilmiştir ve bu konuda daha ayrıntılı literatür bilgisine [SALY17] çalışmasından erişilebilir.

Tek Seferlik Halka İmzaları

1979'da Lamport, [**L**am79], tek seferlik imza (OTS) kavramını önerdi. Bu sistemde imzalama anahtarı güvenli bir şekilde ancak bir kez kullanılabilir ve imzalama anahtarı iki kez veya daha fazla kullanılırsa ortaya çıkar. OTS, şifreleme ve kimliği doğrulanmış anahtar sözleşmeleri oluşumunda çoğunlukla yapı taşı olarak kullanılır. OTS ve halka imzası fikirlerini birleştirerek Saberhagen [CryptNote 2.0], özel anahtarın bir grup adına imzalamak için yalnızca bir kez kullanılabileceği yeni bir imza şeması önermiştir.

Borromean (Halka) İmzaları

Halka imzası ve blokzincir ile ilgili bir başka ilginç yapı taşı ise Maxwell ve Poelstra tarafından 2015 yılında önerilen Borromean (ring) imzasıdır (BRS) [MP15]. Poelstra BRS'nin günümüzde Elements, Liquid ve Monero yapısında kullanılabileceğini iddia etmiştir. Bununla birlikte BRS tabanlı aralık ispatından (ing. range prrof) Bölüm 3.2.4'te bahsedeceğimiz Bul-

letproof [BBB**+17**] yöntemine kadar birçok yapıda kullanılabildiği gösterilmiştir.

$$x_1 \vee x_2 \vee \cdots \vee x_n,$$

Özet olarak, bir halka imzası, imzalayanın belirli bir grup içindeki gizli anahtarlardan birini bildiği bir imzadan başka bir şey değildir.

Bir Borromean halka imzası yöntemi ise bu fikri imzalayanın her bir grup için bir gizli değer bildiği senaryosuna genişletir.

$$(x_1 \vee x_2 \vee \cdots) \wedge (y_1 \vee y_2 \vee \cdots) \wedge \cdots \wedge (z_1 \vee z_2 \vee \cdots) \quad (3.1)$$

Böylece, bu fikir imzalama anahtarının herhangi bir monoton boolean fonsiyonu hakkında bilgiyi ifade etme yeteneği kazanıyor. Her ne kadar öz nitelik temelli imza (ing. attribute-based signature - ABS) [MPR11] $x_1,x_2,\cdots,y_1,y_2,\cdots,z_1,z_2,\cdots$ imzalama anahtarları dikkate alındığında Denklem 3.1'in de gerçekleşmesini sağlasa da ABS ve BRS arasında önemli bir fark vardır. Özellikle, ABS geçerli bir imzayı kimin üretilebileceğine odaklanırken, BRS anonim olarak birden fazla halka imzasının nasıl toplanacağına odaklanır. Diğer bir deyişle, bir BRS programında yer alan tüm halka imzalarının onayları birbirine bağlıdır. Ortak Borromean imzasına katılan halka imzalarından biri geçersizse, o zaman imzanın tamamı geçersizdir ve hangisinin geçersiz olduğu belirlenemez. Borromean halka imzası adının nedeni budur. Topolojik olarak Borromean halkaları, her bir halkanın birbirinden geçeceği şekilde birbirine geçen halkaların bir stilidir (Poelstra, 2017;Cromwell et al., 1998). BRS şemasının yapısı [MP15] Schnorr kimlik doğrulaması [Sch91], AOS halka imzası ve yeni geliştirilen "yarı bukalemun özeti" (ing. *half-chameleon hash*) ve "çoklu bukalemun özeti" (ing. *multiple-chameleon hash*) dahil olmak üzere birçok etkin tekniğin bir kombinasyonuna dayanmaktadır (daha fazla ayrıntı için bkz. [MP15]).

Çoklu-İmzalar

Çoklu imza yöntemleri, tek bir imzanın aynı mesajda birkaç imza gibi çalışmasına izin verir. Çoklu imzanın kritik şartı tek imzanın bir normal imzayla aynı boyutta olmasıdır. Bu yöntem ilk olarak 1983'te Itakura ve Nakamura tarafından ortaya konulmuş ve ardından birçok farklı çalışma tarafında geliştirilmiştir [Oka88], [OO99], [MOR01], [Bol02]. Çok yakın bir zamanda ZILLIQA ekibi, EC-Schnorr çoklu imza protokolünü yenilikçi bileşenlerinden biri olarak kullanarak, yeni nesil yüksek verimli blokzinciri platformu önermiştir. Daha spesifik olarak, ZILLIQA'daki protokol aşağıdaki adımlardan oluşur:

- Standart Schnorr imzalama şeması [Sch91], [Certicom-Research, 2000] tarafından belirtilen eliptik eğri üzerinde başlatılır.
- Tek bir kullanıcı için yukarıdaki EC-Schnorr imza şeması, [MOR01]'deki fikri temel alan birden fazla kullanıcı için bir EC-Schnorr çoklu imza şemasına genişletilmiştir .
- Yukarıdaki EC-Schnorr çoklu imzası, PBFT (pratik Bizans hata toleransı - ing. practical Byzantine fault tolerance) ayarları için uyarlanmıştır, burada mesajın komitede en az $\frac{2}{3}n+1$ tane uç tarafından uygun şekilde imzalanması gerekir.

Biriktirilmiş imza (ing. *aggregate signature*), çoklu-imza yöntemi ile yakından ilgili olan yapıtaşıdır ve Boneh ve arkadaşları tarafından Eurocrypt 2003 konferansından tanıtılmıştır

[BGLS03]. Bu tür imzada, k farklı imzalayıcıdan gelen k farklı mesaja atılmış k adet imza, sadece tek bir imza alaanında toplanır. Biriktirilmiş imzanın çoklu imzanın basit olmayan bir genellemesi olduğunu görmek zor değildir ve depolama ve bant genişliğinden tasarruf etmek için oldukça kullanışlıdır.

BLS İmzası

Bohen-Lynn-Shacham imzasının kısa hali olan BLS imzası, büyük imza kümelerinin kısa bir imzada toplanmasını sağlamaktadır. Yani, kurulum ve imzalama zamanlarında neredeyse hiçbir fark olmadan, çoklu katılımcı için çok verimli sonuçlara ulaşılabilmektedir. Kurulum aşaması için yapılması gereken tek şey, her bir özel anahtar için üyelik anahtarları oluşturmaktır, ve bu sadece bir tur iletişim gerektirmektedir. Kullanıcılar kendi özel anahtarlarını sağladıkları için, çoklu anahtarların kolay yönetimi için HD Derivation gibi teknikleri kullanmak mümkündür. Kullanıcılar işlemleri çevrimdışı olarak imzalarlar ve tek bir toplayıcı imzaları ekler ve gönderir.

3.2.2 Taahhüt Şemaları

Taahhüt Şemaları (ing. Commitment Schemes), örn. Pedersen commitment [Ped91] ve onun vektör versiyonu (bkz. Şekil 3.3 ve Şekil 3.4) blokzincirlerde aralık ispatı (ing. range proof) sistemlerinde kullanılmaktadır. Bulletproof [BCC+16, BBB+17] ve onun eliptik eğri versiyonu Monero'da [MP15], homomorfik tabanlı versiyonu mini-blockchain'de [Cryptonite] kullanılmaktadır.

Şekil 3.4: **Pedersen Taahhüt (ing. Pedersen commitment) Protokolünün Tanımı**

PEDERSEN COMMITMENT

$\mathtt{Setup}: g, h \xleftarrow{\$} \mathbb{G}$

$\mathtt{Com}(x; r): z = g^x h^r \in \mathbb{G}$

Şekil 3.4: **Pedersen Taahhüdünün Vektör Versiyonunun Tanımı**

PEDERSEN VECTOR COMMITMENT

$\mathtt{Setup}: \vec{g} = (g_1, \cdots, g_n), h \xleftarrow{\$} \mathbb{G}$

$\mathtt{Com}(\vec{x}; r): z = h^r \cdot \vec{g}^{\vec{x}} = h^r \prod_{i=1}^{n} g_i^{x_i} \in \mathbb{G}$

Kriptografik taahhüt protokolünü iki tarafın (Alice ve Bob) iki aşamalı olarak oynadığı aşağıda anlatılan oyunda kullanılan, mühürlü zarfın dijital analogu [Ric14] olarak görebiliriz. Taahhüt aşaması olarak adlandırılan ilk aşamada Alice, gönderilen zarfın içinde gizli bir *m* vermek üzere Bob'a *Com(m,r)* değerini taahhüt eder. Açık faz olarak adlandırılan ikinci

aşamada ise Alice, taahhüt aşamasında aldatmadığını kanıtlamak için *Com(m,r)* değerini açar. *Com(m,r)* iki güvenlik gereksinimini karşılamalıdır: gizleme (ing. hiding) ve bağlama (ing. binding).

Kabaca, gizleme Bob'un açık fazdan önce *m*'yi görmek için zarfı açmadığından emin olurken, *bağlama* da Alice'in taahhüt aşamasından sonra gönderilen mühürlü zarfın içindeki değerleri değiştiremeyeceğini garanti eder. Mevcut taahhüt protokollerinde de görebileceğimiz gibi, bu iki gereksinimin dereceleri, hesapsal, istatistiksel veya mükemmel gizli olarak ifade edilebilir [Ric14]. "Taahhüt" terminolojisinin 1981'de Blum tarafından uzaktan yazı-tura oynama protokolünde bahsedildiği bilinmektedir. Ayrıca, bundan önce, tek yönlü özet fonksiyonları yoluyla yapılan bağlama, Lamport tarafından 1979'daki orijinal tek seferlik bir bitlik imza planının bir parçası olarak kabul edilmiştir [Dam98].

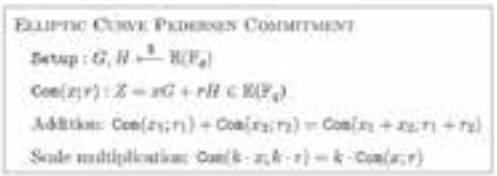
Oldukça yaygın bir yapı taşı olan kriptografik taahhüt protokolleri birçok önemli uygulamada kullanılmaktadır. Örneğin, Pedersen taahhüdü [Ped91] ve varyantları [DHS15] blokzincir uygulamalarında sıklıkla kullanılmaktadır. Pedersen taahhüdü ve onun vektör versiyonu, sırasıyla Şekil 3.3 ve 3.4'de gösterilmiştir. Şekil 3.5'de eliptik eğri tabanlı Pedersen taahhüdü gösterilmiştir. Pedersen (vektör) taahhütlerinin toplamsal homomorfik özelliğine sahip olduğu görülmektedir.

$$Com(x_1; r_1) * Com(x_2; r_2) = Com(x_1 + x_2; r_1 + r_2),$$

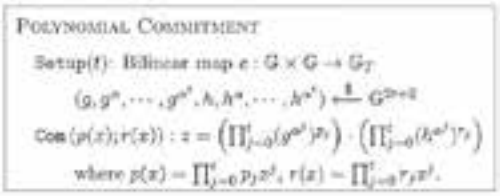
Zerocoin'de, kullanıcıların paralarını saklamak için Pedersen taahhüt yapısı kullanılmıştır. Özellikle, seri numaraları ve gizli numara olan *r* değeri saklamak için *z* değeri kullanılır, öyle ki, $z = g^s h^r \in G$ Bundan sonra, taahhüt edilen parayı harcamak için, kullanıcı *r* ve $z = g^s h^r$ değerini bildiğini ispatlamak için *z* hakkında bir bilgi imzası oluşturur.

Diğer taraftan Monero, eliptik eğri tabanlı Pedersen taahhüt yöntemini işlem değerlerini saklamak için kullanır. Bir işlemde, girdi değeri b_{in} ve çıktı değerleri $b_{out,1}$ ile $b_{out,2}$ 'nin saklanmak istediğini varsayalım. Bu durumda üç gizli (*ing. blind*) değer a_{in}, $a_{out,1}$ ve $a_{out,2}$ rastgele seçilir. Daha sonra, girdi taahhüdü C_{in} ve çıktılar $C_{out,1}$ ile $C_{out,2}$ aşağıdaki gibi

Şekil 3.5: **Eliptik Eğri Tabanlı Pedersen Taahhüdünün Tanımı**



Şekil 3.6: **Polinom Taahhüdün Tanımı**



oluşturulur:

$$C_{in} = a_{in}G + b_{in}H,$$
$$C_{out,1} = a_{out,1}G + b_{out,1}H,$$
$$C_{out,2} = a_{out,2}G + b_{out,2}H,$$

Ayrıca, yukarıdaki taahhüt şemasını uygularken işlemin girdi ve çıktı değerlerinin

$b_{in} = b_{out,1} + b_{out,2}$ bakiye kısıtlamasına uyduğunu kanıtlamak için; $t = a_{in}\ a_{out,1}\ a_{out,2}$ geçici gizli anahtar bilgisiyle üretilip, sadece $tG = C_{in}\ C_{out,1}\ C_{out,2}$. geçici açık anahtarıyla doğrulanabilen bir imza oluşturmak gerekir.

Yakın zamanda, taahhüt kavramı polinom taahhüt [KZG10] ve fonksiyonel taahhüde [LRY16] genişledi. Bu yöntemlerin de blokzincir tabanlı sistemlerde kullanışlı araçlar olabileceğine inanıyoruz. Burada bu iki kriptografik yapıtaşının sadece kurulum ve taahhüt algoritmalarını ele alan konuya özel bir tasvirini yaptık. Daha detaylı anlatımlar [KZG10] ve [LRY16]'da bulunabilir (bkz. Şekil 3.6).

3.2.3 Akümülatörler

Akümülatör, bir küme üzerinde herhangi bir üyenin, kendini ifşa etmeden üyelik kanıtı oluşturabilmesini sağlayan tek yönlü bir fonksiyondur [DHS15]. Akümülatörler, taahhütler ve imzalar (halka) gibi blokzincirlerde kullanılan kriptografik yapıtaşlarıdır. Örneğin, RingCT 2.0 [SALY17]'deki bağlanabilir halka imzası, akümülatör tasarımı üzerine kuruludur. Ayrıca akümülatörler aralık kanıtları oluşturmak için de doğrudan blokzincirlere uygulanabilir. Örneğin, Zerocoin'deki tipik bir aralık kanıt örneği

$$(c = c_1) \vee (c = c_2) \vee \cdots \vee (c = c_n)$$

üye kümesi $\{c_1, c_2, \ldots, c_n\}$ üzerinde bir üye şahidi ile uygulanır.

Şekil 3.7: **Farklı Akümülatörlerin Özellikleri**

Contributors	Functionalities[a]			Security Properties[b]				Building Features[c]	
	MW	NMW	DYN	OW	CF	UND	IND	TSF	TDF
Benaloh et al. (Benaloh and de Mare, 1993)	✓	–	–	✓	–	–	–	–	–
Nyberg et al. (Nyberg, 1996)	✓	–	–	✓	✓	–	–	✓	✓
Baric et al. (Barić and Pfitzmann, 1997)	✓	–	–	✓	✓	–	✓	–	–
Sander et al. (Sander, 1999)	✓	–	–	✓	–	–	–	✓	✓
Camenisch et al. (Camenisch and Lysyanskaya, 2002)	✓	–	✓	✓	✓	–	–	–	✓
Nguyen et al. (Nguyen, 2005)	✓	–	✓	✓	✓	–	–	–	✓
Li et al. (Li et al., 2007)	✓	✓	✓	✓	–	–	–	–	–
Damgård et al. (Damgård and Triandopoulos, 2008)	✓	✓	✓	✓	✓	✓	–	–	–
Camacho et al. (Camacho et al., 2008)	✓	✓	✓	✓	✓	–	–	–	–
Camenisch et al. (Camenisch et al., 2009)	✓	–	✓	✓	–	–	–	✓	✓
Au et al. (Au et al., 2009)	✓	✓	✓	✓	–	✓	–	–	–
Mashatan et al. (Mashatan and Vaudenay, 2011)	✓	✓	✓	✓	–	–	–	–	–
Acar et al. (Acar and Nguyen, 2011)	✓	✓	✓	✓	✓	–	–	–	–
Lipmaa et al. (Lipmaa, 2012)	✓	✓	–	✓	✓	✓	–	✓	✓
Buldas et al. (Buldas et al., 2000; Buldas et al., 2002)	✓	✓	✓	✓	✓	✓	–	✓	✓
Boneh et al. (Boneh and Corrigan-Gibbs, 2014)	✓	–	–	✓	✓	–	–	–	–
Libert et al. (Libert et al., 2016b)	✓	✓	✓	✓	✓	–	–	–	✓

[a] MW = Membership Witness, NMW = Non-Membership Witness, DYN = Dynamic.
[b] OW = One-Wayness, CF = Collision-Free, UND = Undeniable, IND = Indistinguishable.
[c] TSF = Trust-Setup-Free, TDF = Trapdoor-Free.

Genellikle, akümülatörün üç işlevi vardır: *üyelik kanıtı, üye olmama kanıtı* ve *dinamiklik*. Üyelik kanıtı işlevi, bir kanıtlayıcının bir kümenin herhangi bir elemanı için verimli bir şekilde üye şahidi oluşturmasını sağlar. Üye olmama işlevi ise, kanıtlayıcının bunun üstüne kümeye dahil olmayan herhangi bir eleman için de üye olmama kanıtı oluşturmasına izin verir. Üye olmama kanıtı oluşturulabilen akümülatörler *evrensel akümülatörler* olarak adlandırılır. Son özellik olan dinamiklik özelliği, kanıtlayıcının kümenin içerdiği elemanları ve bunlara karşılık gelen kanıtları dinamik olarak güncelleyebilmesini sağlar.

Akümülatörlerin güvenli olması için sahip olması gereken özellikler tek-yönlülük, ayırt edilemezlik, çakışma direnci, ve reddedilemezliktir. İlk ikisi kanıtlardan bilgi sızmasıyla alakalıyken, diğerleri kanıtların oluşturulmasıyla ilgilidir. Tek-yönlülük kanıtın küme üyeleri hakkında herhangi bir bilgi ortaya çıkarmamasını garanti eder. Ayırt edilemezlik, Q_0 ve Q_1 ayrık kümeler olmak üzere, herhangi birinin kanıt $x \in Q_0 \cup Q_1$ *ile* $x \in Q_0$ veya $x \in Q_1$ olduğunu anlayamamasını sağlar. Çakışma özelliği, herhangi birinin kümeye dahil olmayan bir eleman için üyelik kanıtı oluşturabilmesini önlerken, reddedilemezlik özelliği de bir değer için hem üyelik hem de üye olmama kanıtı oluşturulmasını engeller.

Ayrıca, akümülatörler için güvenilir *kurulum gerektirmeme* ve *tuzak kapısı gerektirmeme* (*ing. trapdoor-free*) isimli iki özellik daha bulunur. Figür 3.7'de, var olan akümülatör tasarımlarını yukarıda bahsi geçen özellikler üzerinden özetliyoruz. Var olan akümülatör tasarımlarını temel aldıkları varsayımlara göre de üç kategoride inceleyebiliriz: *RSA-temelli, Eşleme(ing. pairing)-temelli* ve *özet-temelli.*

RSA'ya Bağlı Varsayımları Temel Alan Akümülatörler

RSA kriptosisteminin popülaritesinden dolayı, RSA ile alakalı varsayımlar pek çok kriptografik yapıtaşının temel karmaşıklık varsayımları olarak kullanılmıştır. [BDM93] 1993'te sadece tek-yönlülük güvenlik özelliğine sahip ilk akümülatör tasarımını RSA'nın trapdoor problemine dayalı olarak sunmuştur. Ancak, tek-yönlülük saldırganın aktif olarak kümülatif değerler seçebildiği düşmanca ortamlar için yeterli değildir. Bu problemi çözmek için [BP97] çakışmasızlık özelliğini başka bir güvenlik gerekliliği olarak önermiştir. Ayrıca, Benaloh ve De Mare'ın tasarımı RSA modülüsünü hesaplamak için güvenilir bir partiye (tarafa) ihtiyaç duyar. Bu ihtiyacı ortadan kaldırmak için [San99] RSA problemine dayanan fakat herhangi bir tuzak kapısı kullanmayan yeni bir akümülatör tasarımı önermiştir. Bu sırada, yukarıdaki bütün tasarımlar statik akümülatörler olsa da akümülatörlerin uygulamalarında dinamiklik genellikle gerekli bir özellik olmuştur. Bu amaçla, [CL02] dinamik akümülatör konseptini ileri sürmüş ve güncelleme maliyeti küme boyutundan bağımsız olan somut bir akümülatör tasarımı ileri sürmüştür. Akümülatörün gelişmesiyle üye olmama kanıtı da arzu edilen bir özellik haline gelmiştir. Üye olmama kanıtlarını destekleyen ilk akümülatör tasarımı [LLX07] tarafından oluşturulmuştur. Ancak bu tasarım [BDM93]'teki gibi güvenilir kurulum gerektirmektedir. Daha sonra güvenilir kurulum işlemini ortadan kaldırmak için [Hel12] kök varsayımına dayanan ve kök akümülatörü olarak adlandırılan, verimliliği [LLX07]'yle kıyaslanabilir seviyede yeni bir akümülatör tasarımı ortaya koymuştur. Ayrıca [MV13], [LLX07] tasarımını temel alan ve eklenen/silinen üyeler için yeni kanıtlar oluşturabilen tamamiyle dinamik ve evrensel bir akümülatör tasarımı öne sürmüştür.

Eşleme Dönüşümleri Temelli Akümülatörler

İlk pairing temelli akümülatör tasarımı [Ngu05] tarafından önerilmiştir ve bu tasarım sabit imza boyutlu ilk kimlik temelli halka imzalama yöntemini oluşturmak için kullanılabilir. Ancak bu tasarım üye olmama kanıtları oluşturamaz ve akümülatörü güncellemek için bir ana sırra (*ing. master secret*) ihtiyaç duyar. Bu iki dezavantaj akümülatörün halka imza-

sında kullanımını engelleyebilirdi. İlk problem için, Damgard ve Triandopoulos [DT08] üye olmama kanıtını destekleyen bir geliştirme önerdiler. İkinci problemle alakalı olarak ise, [ATSM09], [LLX07]'de kullanılan tekniğin aynısını uygulayarak bir dinamik evrensel akümülatör tasarımı sundu. Ancak yukarıda bahsedilen tasarımlardaki kanıt güncellemeleri beklenildiği kadar verimli değildir. Bu problem için [CKS09] yeni bir dinamik akümülatör tasarımı öne sürmüşlerdir. Acar ve Nguyen, [AN11] temsilcili (ing. delegated) üye olmama kanıtlarıyla [Ngu05]'teki akümüle edilmiş eleman sayısı limitinden bağımsız olan başka bir tasarım sunmuşlardır.

Özet Fonksiyonu Temelli Akümülatörler

İlk özet temelli akümülatör tasarımı [Nyb96] tarafından önerilmiştir. Ortaya çıkan tasarımın trapdoor gerektirmediğini ve RSA ile alakalı varsayımlara dayanan tek yönlü tasarımlardan daha verimli olduğunu görmek zor değildir. Sertifika yönetiminde (akümülatörlerin uygulama alanlarından biri), bir sertifikanın aynı anda hem geçerli hem de geçersiz olduğunun kanıtlanamaması temel bir kriterdir. Bu kriter reddedilemezlik güvenlik özelliğine gerek duyar. [BLL02] özet fonksiyonları ve özet ağaçlarını kullanarak birkaç reddedilemez evrensel dinamik akümülatör tasarımı sunmuştur fakat bu tasarımlar güncelleme yapmak için güvenilir partiye ihtiyaç duyar. [CHKO08] bu problemi çözmek için güçlü bir evrensel akümülatör tasarımı önermiştir. Son zamanlarda, özet temelli akümülatörlerin reddedilemezlik özelliği dikkate değer bir seviyede ilgi çekmektedir. [BCG14], 2014'te özet fonksiyonu RSA modüler uzayı üzerinde basit iki değişkenli Zagier polinamlarından çıkarsanan yeni bir özet temelli akümülatör tasarımı ortaya koymuştur. Ayrıca, [DHS15] var olan akümülatörlere reddedilemezlik özelliğini eklemek için basit ve hafif bir dönüşüm önermiştir. Yakın zamanda, [LLNW16] özet ağaçlarını temel alan ve *sıfır-bilgi argümanı bilgisini* destekleyen yeni bir yapı tanımlamıştır.

3.2.4 Sıfır Bilgi İspatları

Bir işlemin gizlilik ve anonimliğini korumak için akla gelen ilk yöntem işlemleri bağlanamaz bir yapıda kurgulamaktır. Ancak kripto para sistemlerinde, parayı harcamak isteyen kişinin paranın bulunduğu adrese karşılık gelen bir sırrı bildiğini; gerekmektedir. Neyse ki bu noktada sıfır bilgi ispatları (ZKP) oyuna katılır. ZKP primitifleri bir sırra sahip olan tarafa (kanıtlayıcı), bu sırrın sahip olduğu bazı özellikleri sırrın kendisini açığa çıkarmadan, başka bir kişi veya kuruma (onaylayıcı) kanıtlama imkanı verir.

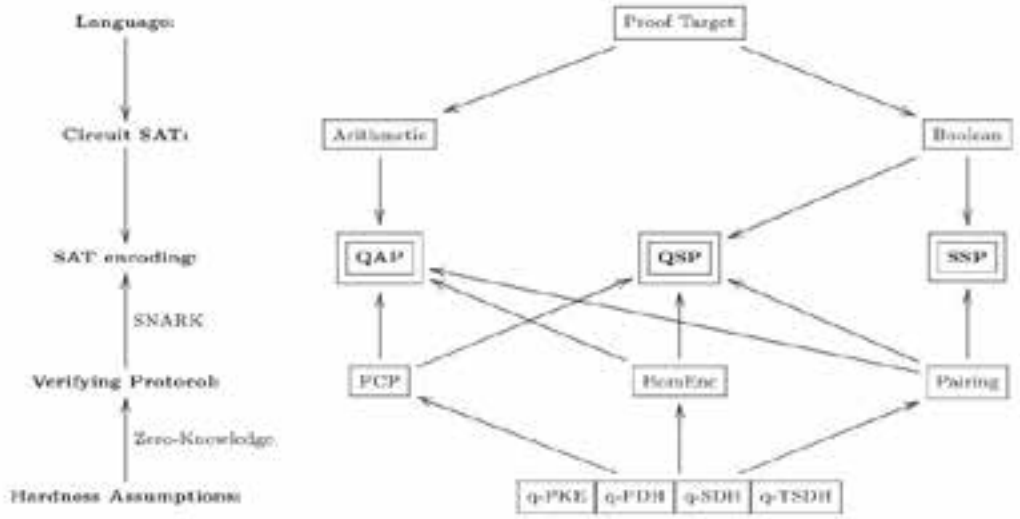
Kanıtlardan ZK-SNARK'lara

Bilgisayar biliminde, NP-tam bir dil olan L için bir kanıt, bir kanıtlayıcının bir onaylayıcıyı $x \in L$ olduğuna ikna etmesine yarayan protokoldür. Bir kanıtın genellikle iki temel gereklilik olan tamlık (*ing. completeness*) ve doğruluğu (*ing. soundness*) sağlaması beklenir. İlki yeter şart ile benzerdir. Eğer $x \in L$ ise, bu kanıt protokolün gerçekleştirilmesinden sonra kabul edilmelidir. İkincisi gerek şarta benzemektedir. Eğer $x \notin L$ ise, bu kanıtın kabul edilme olasılığı ihmal edilebilir olmalıdır. Genellikle, bu iki temel özellik hesapsal, istatiksel ya da mükemmel (*ing. perfectly*) şekilde sağlanabilir [Ric14]. Ancak matematiksel bakış açısıyla,

hesapsal doğruluk kanıtı bir kanıt değil argümandır [**BCC88**]. Çünkü bu kanıt, hesaplama teknolojisindeki bir ilerleme ya da yeni bir algoritmanın bulunmasıyla yanlış hale gelebilir. Ayrıca, bir kanıt (ya da argüman):

- Eğer kanıtın kabulünden sonra onaylayıcı $x \in L$'nin ötesinde hiçbir şey öğrenemiyorsa sıfır bilgi (*ing. zero knowledge*) [GMR89];
- Eğer hem kanıtın uzunluğu hem de onaylama zamanı $x \in L$' yi temsil eden C devresinin boyutuna göre polilog fonksiyonlarla sınırlandırılmışsa öz (*ing. succinct*)[Kil92];
- Eğer verilen kabul edilebilir bir kanıt veya argüman için, herhangi biri kanıt/argümanı destekleyen bir şahidi polinom zamanda üretebiliyorsa *bilginin kanıtı* (*POK*) ya da bilginin argümanı (*AOK*) [BDSMP91];
- Eğer kanıtlayıcıdan onaylayıcıya sadece tek geçişlik bir iletişim gerektiriyorsa interaktif olmayan (*ing. non-interactive*) olarak adlandırılır.

Şekil 3.8: **zk-SNARK Teknik Mimarisi**



Öz interaktif olmayan bir argüman genellikle kısaca SNARG olarak adlandırılır [Kil92]. AOK özelliğine sahip bir SNARG ise SNARK olarak adlandırılır. Fiat-Shamir mekanizması [FS86] kullanılarak herhangi bir interaktif kanıttan interaktif olmayan bir kanıt türetilebilir.

Sıfır bilgi özelliğine sahip bir SNARK, kısaca zk-SNARK olarak adlandırılır. Son yıllarda zk-SNARK'ları oluşturmak için çeşitli teknikler önerilmiştir [Gro10, Hel12, BCI+13, GGPR13, PHGR13, Lip13, BSCG+13, BSCTV14a, BSCTV14b, Gro16, BGM17, ABLZ17]. Bunları Şekil 3.8'de görüldüğü gibi 5 seviyede özetlenebilir. Alt seviyeden orta seviyeye QAP, QSP ve SSP ile kodlanmış karşılanabilme problemleri (*ing. satisfiability problems*), q-PKE, q-PDH, q-SDH veya q-TSDH gibi zorluk problemlerine dayanan PCP, homomorfik şifreleme [XWZ+18], pairing vs. yöntemleriyle onaylanırken; üst seviyeden orta seviyeye, yüksek seviye dillerle tanımlanmış kanıt hedefleri, ikinci dereceden aritmetik programlara (QAP), ikinci dereceden geren programlara (QSP) ve kare geren programlara (SSP) dönüştürülmüştür.

Daha detaylı bir açıklama aşağıda verilmiştir:

- İlk dönüştürme kanıt hedeflerinden devre karşılanabilirliğine doğrudur. Bu dönüşümdeki kritik bileşen, uygun şekilde sınırlanmış program uygulamalarının doğruluğunu aritmetik devrelere veya Boole devrelerine çevirebilen devre üretecidir [BSCTV14b]. Burada, uygun şekilde sınırlandırılmış program uygulamaları kanıt hedeflerini temsil eder.
- İkinci dönüşüm devre karşılanabilirliğini karşılanabilirlik kodlamasına çevirmektir. Detaylandıracak olursak, aritmetik devreleri ve boole devreleri sırasıyla kıyaslanabilir boyutlarda ikinci dereceden aritmetik programlara (QAP) [GGPR13] ve ikinci dereceden geren programlara (QSP) [GGPR13] veya kare dereceden geren programlara (SSP) [DFGK14] çevirmektir.
- Karşılanabilirlik kodlaması ve onaylama protokolleriyle beraber artık zk-SNARK'lara sahip olabiliriz. zk-SNARK'ların çoğunda, kanıtlayıcının gizli girdilerin bilgisini gizli girdiyi açığa çıkarmadan kanıtlamasında ve devre karşılanabilirliğinin gizli onaylanabilirliğini sağlamada bilineer eşleme dönüşümleri kritik bir rol oynarlar. *Olasılıksal olarak kontrol edilebilen kanıtlar* (*PCP*) [BFLS91] ve homomorfik şifrelemeler zk-SNARK'lardaki kanıt onaylamalarında kullanılan diğer iki önemli araçtır. PCP'ler ve homomorfik şifrelemeler genelde fazla zaman tüketseler de [BCI+13, BSCG+13] gibi çoğu zk-SNARK bu yapılar üzerine kuruludur.
- Son olarak, onaylama protokolleri , q-dereceden üstsel bilgi varsayımı(q-*PKE*) [Dam91], q-*dereceden* Diffie-Hellman varsayımı (q-*PDH*) [**Gro10**], q-*güçlü* Diffie-Hellman varsayımı (q-*SDH*) [Gro10], ve $q(\lambda)$ hedef grup güçlü Diffie-Hellman varsayımı (q-*TSDH*) [BB08] da dahil olmak üzere, genelde bazı zorluk varsayımlarına dayandırılmaktadır.

QAP'leri [BCI+13, GGPR13, PHGR13, BSCG+13, BSCTV14b, BGM17, ABLZ17] QSP'leri [Lip13, GGPR13] temel alan pek çok verimli zk-SNARK vardır. Ancak, bu yöntemlerin hepsi güvenilir kurulum probleminden muzdariptirler. Ayrıca uygulamaları ölçeklenebilir değildir. Detaya indiğimizde, hepsi oldukça karmaşık *ortak referans katarları (CRC)* oluşturmak için hesaplama ve uzunluk açısından ağır protokoller gerektirirler.

Yakın zamanlarda zk-SNARK metodolojilerinde ciddi ilerlemeler görülmüştür. Örnek olarak, [BSBC+17], *Ölçeklenebilir Hesaplamalı Bütünlük (SCI)* olarak adlandırılan bir kanıt sistemi sunmaktadır. SCI basit bir kurulum gerektirir ve sadece çakışmasız özet fonksiyonlarına dayanır. Fakat, bu sistem ne bir sıfır bilgi sistemidir ne de [BSCG+13, BCC+16] kadar verimlidir. Bunu takip eden çalışmada, Ben-Sasson vd. sıfır bilgi olan ve SCI'dan daha verimli olan, *bilginin ölçeklenebilir, şeffaf argümanını (ing. scalable, transparent argument-of-knowledge, STARK)* tasarlamışlardır. Buna ek olarak, Bootle vd. devre karşılanabilirliği için çakışmasız özet fonksiyonlarına dayanan bir argüman önermişlerdir. Bu yapıda kanıtlayıcının maliyeti aritmetik devrenin boyutuyla lineer ilişki gösterirken onaylayıcı doğrusal yük altındadır. Dolayısıyla, bu yapı [BCC+16, BSBC+17]'daki tasarımlardan daha verimlidir. Bunun yanında, Veeningen Meilof [Vee17] taahhüt (commitment) sağlanan veri üzerinde birden fazla farklı hesaplama yapılabilen adaptif bir zk-SNARK sunmuştur.

Zerocash'te ZK-SNARK'lar

Miers vd. tarafından tasarlanmış Zerocoin [MGGR13b], paraların izlenebilirliğini bozarak Bitcoin'i anonimlikle beraber sunmayı amaçlar. Ancak sonuç olarak ortaya çıkan kripto para tam teşekküllü anonim ödemeleri çeşitli nedenlerden dolayı destekleyemez. İlk olarak, Zerocoin sabitlenmiş nominal değerleri kullanır. İkinci olarak, ödemeden önce anonim paralar anonim olmayan bir hesaba transfer edilmelidir. Son olarak, işlemlerin içindeki para miktarını belirten veya diğer anlamlı veriler saklanmaz. Bu problemleri çözmek için Ben-Sasson vd. [SCG+14b] Zerocash'i tasarlamışlardır. Zerocash kullanıcının anonimliğini ve anonim paralarla işlem verisinin gizliliğini sağlar. Üstelik, Zerocash işlem boyutunu önemli boyutlarda küçültür (tek bir para için 1 KB'den daha az) ve onaylama zamanını 6 ms'den daha aza indirir.

Zerocash, tam teşekküllü merkezi olmayan bir kripto para sisteminin fonksiyonel gerekliliklerini ve güvenlik ve gizlilik hedeflerini zk-SNARK'lar [BSCTV14b] ile tartışılmaz bir şekilde karşılar. Zerocash'te, işlemler üçe ayrılır: *basecoin* işlemi, *mint* (*para basma*) işlemi ve *pour* (*dökülme*) işlemi. Zerocash'te zk-SNARK'ları anonimlik artırmak için kullanmanın anahtar noktaları aşağıdaki gibidir:

- **Basecoin işlemi (Anonimlik koruması olmadan):** Bir basecoin işlemi Bitcoin işleminin aynısıdır, yani kullanıcı adresleri ve işlem değerleri halka açıktır.
- **Mint işlemi (Üzerinde taahhüt sağlanmış para değerleri ve açık adreslerle):** *cm* para taahhüdü, *v* para değeri ve * diğer gerekli bilgileri saklamak için ayrılmış alan olmak üzere, Zerocash'te bir mint işlemi tanımlama grubu (tuple) (*cm,v,* *)'dır. Bir mint işlemi defteri kebire eklendiği zaman, belli sayıda para blokzincire işlenmiş olur. Burada anahtar nokta mint işlemini gerçekleştiren kişinin kendi adresini ya da transfer edilen değerleri açığa çıkarmadan blokzincire işlenmiş bu değerleri transfer edebilmesidir.
- **Pour işlemi (artırılmış anonimlik koruması):** Verilen bir mint ya da pour işlemi için, herhangi bir kullanıcı yeni bir pour işlemi üretebilir. Biçimsel olarak, *rt* para taahhütlerinin Merkle ağacının kökü, sn_1 ve sn_2 iki para seri numarası, cm_1 ve cm_2 iki yeni para taahhüdü, π gizli girdiler üzerinde zk-SNARK kanıtı ve * diğer gerekli bilgileri saklamak için ayrılmış alan olmak üzere, Zerocash'te bir pour işlemi tanımlama grubu (tuple) $(rt, sn_1, sn_2, cm_1, cm_2, \pi, *)$ olarak gösterilir. Bir pour işlemi blokzincire eklendiğinde belli sayıda para kullanıcıların adresleri ve transfer edilen paraların miktarları açığa çıkmadan bir grup kullanıcıdan diğer bir grup kullanıcıya transfer edilir.

Bulletproof'lar: zk-Aralık Kanıtları ve Birleştirmeler

Kullanıcılar, transfer gerçekleştirebilmek için, transfere giren para mktarının transferden çıkan para miktarından büyük olduğunu kanıtlamalıdırlar. Fakat, bunu yaparken kötü niyetli kullanıcıların yazılı değeri 1 olan bir parayı yazılı değerleri sırasıyla 10 ve -9 olan iki paraya bölmeye çalışması muhtemeldir. Bu durum, ciddi karışıklıklara yol açabilir ve sistemin dürüst kullanıcıların güvenini kaybetmesine sebep olabilir. Neyse ki, bu problem aralık kanıtı isimli teknikle çözülebilir. Örneğin, Borromean Halka İmzası

Monero'da ve Elements'te işlenen değerin pozitif ve belli bir aralıkta olduğunu kanıtlama için kullanılır. Bünz vd. [BBB+17], yakın bir tarihte Bulletproof isimli, birden fazla aralık kanıtını birleştiren ve daha verimli bir yöntem ortaya koymuşlardır.

Bulletproof'lar, kanıtlayıcılara, birden fazla işlenmiş değerin verilen aralıkta olduğunu birleştirilmiş kısa bir kanıtla kanıtlama imkanı sağlayan, interaktif olmayan ve birleştirilebilir iç çarpım aralık kanıt protokolleridir. Esasen, Bulletproof'lar [BCC+16] tarafından sunulmuş iç çarpım argümanlarını (IPA) temel alır. [BBBпп17], bu tasarımı taahhüt için gereken temel vektörün boyutunu yarıya indirerek geliştirmiştir. Bunu yapmak için n boyutlu bir vektörü log2 n seferlik bir yinelemeyle 1 boyutlu bir vektöre dönüştürürler. Böylece orijinal iç çarpım argümanındaki iletişim karmaşıklığı oldukça düşmüştür.

3.3 Kriptografik Olmayan Yapı Taşları

Bu bölüm, blokzincirlerde güvenlik ve gizliliği artırmaya yönelik kriptografik primitiflere dayanmayan teknikleri tanıtmaktadır. Bölüm içeriği ağırlıklı olarak [ZXL19] ve [McD13] kaynaklarından yararlanılarak hazırlanmıştır.

3.3.1 Mixcoin

Bonneau vd. 2014'te, Bitcoin ve Bitcoin türevi kriptoparalarda anonim ödemeler sağlayan Mixcoin'i ortaya koymuşlardır. Mixcoin, pasif saldırganlara önlem olarak anonimlik kümesini paralarını karıştırması için bütün kullanıcılara genişletir. Aktif saldırganlara karşı koymak içinse geleneksel iletişim karıştırmalarına benzer bir yöntem izler. Mixcoin, hesap verebilirlik mekanizmasını hırsızlıkları teşhis etmek için kullanır ve bu, kullanıcıların Mixcoin'i özendirici teşvikler sayesinde bitcoin çalmadan kullanacağını gösterir.

3.3.2 CoinJoin

CoinJoin, Bitcoini işlemlerini anonimleştirmek için alternatif bir yöntem olarak 2013 yılında ortaya konmuştur. Bu yöntem, ortak ödemelerden yola çıkılarak tasarlanmıştır. Bir ödeme yapmak isteyen kullanıcı, ödeme yapmak isteyen başka bir kullanıcı daha bulur ve kullanıcılar anlaşıp ödemeleri tek bir ortak işlem halinde gerçekleştirirler. Ortak ödemeler sayesinde bir işlemde girdi ve çıktıların arasında bağlantı kurulması ve spesifik bir kullanıcının para hareketinin izlenmesinin olasılığı önemli bir oranda düşer.

CoinJoin, kullanıcıların beraber ortak ödemeyi gerçekleştireceği işlem için anlaşmalarını gerektirir. Bu özelliği önermek için oluşturulan ilk karıştırma servisleri (SharedCoin) merkezi sunucuları kullanmıştır ve kullanıcıların bu servisleri kullanmak için servis işletmecilerinin herhangi bir tür hırsızlığa izin vermeyeceğine dair servis işletmecilerine güven duymasını gerektirir. Ancak merkezi sunucular, merkezi arıza noktası olarak, kullanıcıların mahremiyetinin zarar görmesine sebep olabilir. Bunun nedeni, bu sunu-

culaın işlem log'larını tutması ve ortak ödemelerin kullanıcılarını kaydetmesidir. Ek olarak CoinJoin protokolünün yanlış uygulanması anonimliği azaltacaktır.

3.3.3 CoinShuffle

CoinShuffle 2014'te Tim Ruffing vd. tarafından sunulmuştur ve CoinJoin konseptini, işlemleri karıştırmak için güvenilir bir üçüncü partiye duyulan ihtiyacı ortadan kaldırarak genişletir ve gizliliği artırır. CoinJoin'in bütünüyle merkezi olmayan bir para karıştırma protokolü olduğu ve hırsızlığa karşı güvenliği sağladığı iddia edilir. CoinShuffle, anonimliği sağlamak için Dissent olarak adlandırılan, yeni bir sorumlu anonim grup iletişim protokolü kullanır.

3.3.4 Gizli Adres

Gizli(stealth) adres , mahremiyet artırma amacıyla ilk olarak 2011 yılında ByteCoin için BSAP (Basic Stealth Address Protocol) adıyla kullanılmıştır. 2013 yılında CryptoNote tanıtım yazısında ISAP (Improved Stealth Address Protocol) adıyla tanıtılan protokol, 2014 yılında Bitcoin için gerçeklenmiştir. 2014 yılında tanıtılan daha etkin bir yöntem olan DKSAP(Dual Key Address Protocol) ise Monero gibi pek çok sistemde kullanılmıştır. Temel olarak göndericinin, her işlem için alıcıya tek kullanımlık bir adres üretmesi temeline dayanır. Böylece aynı alıcıya yapılan ödemeler, birbiri ile ilişkilendirilemezler. Yöntemlerin birbirinden farkları, gizli adresin alıcıya ulaştırma yöntemlerinin farklı olmasıdır.

3.3.5 Özel Donanımlar

Blokzincirlerde güvenlik ve mahremiyet artırma amacıyla başvurulan diğer bir yol, güvenilir hesaplama donanımları kullanmaktır. Intel SGX gibi donanımsal güven sağlama araçları, blokzincir düğümlerinde işlemlerin bir kısmının, erişilebilir olmaktan uzak şekilde gerçekleştirilmesine olanak sağlar. Hawk gibi pek çok kriptopara blokzincirinde güvenlik SGX donanımları üzerine kuruludur. Bazı izinli blokzincir türlerinde ise düğümlerin kriptografik işlemlerini (kripto anahtarı üretme, depolama, verileri şifreleme, imzalama vb.) mahrem bir şekilde gerçekleştirmek üzere donanım güvenlik modülleri kullanılır.

BLOKZİNCİR PLATFORMLARININ MAHREMİYET ÖZELLİKLERİ

Mahremiyet ve gizlilik sağlayan kullanım senaryolarını desteklemek üzere blokzincir platformları, Bölüm.3'de tanıtılan yapı taşlarına dayalı çeşitli teknikleri kullanmaya çalışmaktadır. Bu yöntemlerin hepsinin kendi içinde avantajlı ve dezavantajlı noktaları bulunmaktadır:

- Verileri şifrelemek, mahremiyet sağlama yollarından birisidir. Ancak özellikle Açık blokzincirlerde, her düğümde kopyası bulunan şifrelenmiş verinin, yeterli zaman ve hesaplama gücü elde edildiğinde çözülebileceği göz ardı edilmemelidir. Bu tür bir risk bazı kurumsal uygulamalarda kabul edilemez olabilir.
- Sıfır bilgi ispatları, başvurulan diğer bir yöntemdir. Buradaki sorun, ZKP hesaplamalarının önemli miktarda zaman ve hesaplama kaynağı gerektirmesidir. Performanstan ödün verilmesi gerekebilir.
- İzinli ağ tiplerinde kullanılabilecek bir yöntem ise mahrem bilgilerin sadece yetkili düğümlere dağıtılmasıdır.

Bu bölümde mevcut blokzincir platformlarının yukarıdaki yöntemleri kullanış şekli ve mahremiyet gereksinimlerine uygunluğuna değinilecektir. Önce kriptopara blokzincirleri, daha sonra da merkeziyetsiz uygulamaların geliştirilebileceği genel amaçlı blokzincir platformları ele alınacaktır. Ayrıca, blokzincir platformlarının kişisel verilerin korunması bağlamında uyum durumu irdelenecektir. Bölümün içerisinde, sadece herhangi bir mahremiyet mekanizması içeren blokzincir platformları incelenecektir.

4.1 Kriptoparalarda Mahremiyet

Bu alt bölümde, mahremiyeti koruyan ve/veya gerçek banka sistemlerine benzeyen çeşitli kriptoparaların geniş bir sınıflandırması verilecek ve kullanılan güvenlik mekanizmaları incelenecektir.

Kriptoparalar genel itibariyle iki kategoride sınıflandırılabilir: gönderici-alıcı anonimliğini ve/veya işlem miktarı gizliliğini hedefleyen mahremiyet odaklı paralar(Dash, Zcoin [MGGR13a], ZCash [SCG+14a], Monero [Sab13], Zether [BAZB19] gibi) ve mahremiyet odaklı olmayan paralar (Bitcoin [Nak09], Ethereum [But14], Cardano, Ripple, Stellar vs. gibi). Finans endüstrisi sistemleri güncel banka sisteminin işlem akışını destekler niteliktedir. Mesela Ripple [rip], işlem grafı mahremiyeti bulunmayan değer transferleri için yaygın bir şekilde kullanılan bir şema iken, Dijital Varlık Platformu ise işlem detaylarını zincir dışında tutup denetlenebilirlikten ve zincir onayından tamamıyla feragat ederek mahremiyeti sağlamaktadır [CZJ+17].

Açık ve Özel, birçok kriptopara ağında kullanılan iki ana blokzincir türüdür. Açık bir blokzincirde, Bitcoin'de de olduğu gibi, her kullanıcı kişisel bir adres oluşturabilir, sisteme işlem yollayabilir ve kayıt defterine kayıt ekleyebilir. Bitcoin'de bir kullanıcı Bitcoin blokzincirinin kopyasını kendi makinasına indirmekte, bir düğüm kurup madencilik yapmakta serbesttir.

İzinli blokzincirler ise kapalı ekosistemlerdir ve kullanıcıların serbestçe katılmalarına, kayıt defterine erişmelerine ve işlem yollamalarına izin verilmez.

Nakamoto tarafından tavsiye edilen tek kullanımlık hesaplar, göndericilerin mahremiyetini korumak adına hesaplar arası ilişkilendirmeyi azaltmak için Bitcoin'de kullanılan ana mahremiyet mekanizmasıdır. Bu yüzden Bitcoin protokolünün anonimlikten yoksun ve yarı anonim bir yapıda olduğu söylenebilir. Özellikle belirtmek gerekir ki Bitcoin adreslerinin tekrar ve aynı anda kullanımı, birçok adresi bir kullanıcıyla eşleştirmeyi ve hatta biraz ekstra bilgi ile bu kullanıcı adreslerini gerçek kimlikleriyle eşleştirmeyi mümkün kılmaktadır [LSY+19]. Benzer şekilde [BAZB19]'de belirtildiği gibi, Ethereum uygulamalarına işe yarar bir mahremiyet tabakası eklemenin kolay bir yolu bulunmamaktadır.

Mahremiyet Odaklı Olan UTXO Tabanlı Kriptoparalar

Bitcoin için mahrem işlemler, ilk kez Maxwell tarafından Girdi/Çıktının homomorfik şifrelenmesi şeklinde Bitcoin'in anonimlik sorununa bir çözüm olarak sunuldu. Bu gibi sistemler her ne kadar kıymetleri ve miktarları gizlese de işlem grafını sızdırırlar [NVV18].

Zerocoin [MGGR13a], güçlü anonimlik sağlamak adına sıfır-bilgi kanıtlarını kullanıp işlem graf analizlerini önleyerek Bitcoin protokolünü genişletmiştir. Zerocoin'e paralel olarak kompleks anonimleştirme teknikleri kullanarak işlemleri ve işlemin paydaşlarını gizleyebilen Monero geliştirildi. Monero bunu, işlem göndericisinin seçtiği bir grup işlemin (anonimlik kümesi) gönderici ve gönderenlerini özel bir çeşit imzalama şeması kullanıp gizleyerek yapar. Ne yazık ki imzanın boyu Zether'de de olduğu gibi [BAZB19] anonimlik kümesinin boyu ile doğru orantılı olarak büyümektedir. Güvenlik ve anonimlik sağlamak adına Monero [Sab13], bağlanabilir halka imzası (Ring Signature) şemasını ve bir çeşit mahrem işlem şeması olan Halka Mahrem İşlem şemasını kullanır. CryptoNote da işlemler arası gönderici adresi ilişkisini gizlemek için halka imzasını kullanır. Daha açıkça ifade edersek, CryptoNote göndericinin açık anahtarını diğer birçok anahtar ile beraber oluşturur ve bu şekilde işlemi gerçekten kimin gönderdiğini (imzaladığını) anlamak imkansız hale gelir. Halka imzası kullanıldığı için, halka üyeleri sayısı n olmak üzere bir saldırganın gerçek göndereni doğru tahmin etme olasılığı 1/n'dir. Daha sonra 2015'te Ethereum da halka imzaları kullanmaya başlamıştır. Bununla beraber Ethereum kullanıcıları Monero gibi bir CryptoNote parasındakine benzer bir anonimlik elde ettiler. Ethereum akıllı kontratları daha yüksek güvenlik ve kontrol için, blokzincirde tutulan veriye homomorfik şifreleme yapma imkanı sunmaktadır.

ZeroCash, kullanıcılarına anonimlik imkanı vererek daha iyi bir değiştirilebilirlik (ing. fungibility) seviyesi sunar. Zerocash [SCG+14a], zk-SNARK (zero-knowledge Succinct Non-interactive ARgument of Knowledge) ve kriptografik mutabakat şemalarını kullanarak daha eski bir protokol olan Zerocoin'den hem fonksiyonellik açısından (Zerocoin bir ödemenin yalnızca gönderenini gizler, gönderileni ve miktarı değil. Ayrıca koinleri küçük parçalara bölmeyi ve direkt olarak Zerocoin ile ödeme yapmayı desteklemez) hem de performans açısından (Zerocash işlemleri 1KB'tan azdır ve onaylanmaları 6ms'den kısa sürer) daha ileri gitmiştir. ZeroCash, UTXO modeli tabanlı kriptoparalar içinde en yüksek seviye güvenlik koruması ve anonimlik sağlar. Fakat kullandığı kriptografik mutabakat şemasının homomorfik

özelliklerden yoksun olması nedeniyle hesap-tabanlı sistemler için uygun değildir. Ayrıca, zk-SNARK onaylayıcısı kullanılarak, Zerocash'in basitleştirilmiş bir versiyonunu (ki Zcash'i inşa etmekte kullanılan bir akademik protokoldür) kullanan orijinal bir jeton karıştırma kontratı uygulanır. Bu yüzden "bebek" ZoE (Zerocash over Ethereum) olarak adlandırılır. Kontrat, kontrat tarafından idare edilen bir Merkle Tree'ye bir "seri numarası"nı mutabakat olarak eklemek yoluyla kullanıcıya ayrık miktarları (ETH birimlerini) tutma olanağı sunar.

Mahremiyet Odaklı Olan Hesap Tabanlı Kriptoparalar

Hawk [KMS+16], mahremiyet koruyan akıllı kontrat inşası için geliştirilmiş bir altyapıdır. Kullanıcıların oluşturduğu (committed) koinleri saklamak için akıllı kontrat çalıştırır ve ödeme dağılımını belirler [MDH+17]. Kısaca, Hawk [KMS+16] hassas işlem bilgilerini açığa çıkarmayı gerektirmeyecek bir programlanabilirlik şartıyla, kontratları zincir dışında çalıştırarak ve yalnızca sıfır-bilgi kanıtlarını zincire koyarak mahremiyet imkanı sunan bir akıllı kontrat sistemidir. Hawk Yöneticisi, kullanıcıların biçtikleri fiyatları her daim bildiği için bu şema, işlem miktarı ve hesap bakiyesi açısından mahremiyet korumaya uygun değildir [MDH+17].

ZeroCash ve Hawk, güçlü işlem-graf mahremiyeti sunar. Ne yazık ki güvenilir bir kurulum gerektirirler ve bu da pratikte merkezi olmak zorundadır (bu amaç için bir multiparty hesaplama pratik olmayacağı için) [CZJ+17]. Ayrıca Hawk "yönetici" diye tabir edilen tek bir hesap düğümü için dizayn edilmiştir ve bu yüzden yüksek elverişlilik sunmamaktadır [CZK+18]. Her ne kadar [KMS+16]'in yazarları, yöneticinin protokolden sapmasının veya başkalarıyla gizlice illegal işler yürütmesinin, kontratın doğru çalışmasına bir etkisi olmayacağını savunsalar da modelin güvenliğini arttırmak için Hawk Yönetici'yi Intel SGX gibi güvenilir bir donanım üzerine kurmak veya kullanıcılar arasında çoklu katılımlı hesaplamaya geçmek gibi tavsiyelerde bulunmuşlardır. Sonuç olarak, her ne kadar Hawk oldukça güçlü olsa da ve daha iyi bir güvenlik sağlasa da tamamıyla dağıtık değildir ve basit akıllı kontratlar için kullanımı fazlasıyla pahalıdır. Diğer bir genel amaçlı yapı olan Ekiden [CZK+18], akıllı kontrat platformlarında performans ve mahremiyet problemlerini adresler, fakat yine Intel SGX gibi güvenilir donanımlara dayandığı için tam merkezi olmayan özellikte değildir [BAZB19]. [MDH+17] 'in yazarları [KMS+16]'dekinden ve [CZK+18]'dekinden farklı bir mimari kullanarak hesap tabanlı blokzincir üzerinde, bakiye ve işlem miktarı gizleme özelliği bulunan dağıtık bir akıllı kontrat sistemini tanıtmışlardır. Fakat gönderici ve alıcı adresleri, yani açık anahtarlar işlem bilgisine eklemlendirildiğinden sistem yalnızca yarı-anonimliği garanti edebilir. Son olarak, [BAZB19] Ethereum ve diğer akıllı kontrat platformlarıyla uyumlu ve tamamen dağıtık yapıda bir mahrem ödeme mekanizması olan Zether'i önermiştir. Burada, verimlilik ve kullanışlılık için Ethereum'dakine benzer hesap tabanlı bir yaklaşım izlenmiştir. Ayrıca, hesap bakiyelerini şifreli halde tutan; hesaba para yatırma, transfer ve para çekme metotlarını ise regülasyonları düşünmeksizin kriptografik kanıtlar yordamıyla açık eden yeni bir akıllı kontrat geliştirilmiştir.

Banka Aracılı Sistemler

RSCoin, Solidus ve zkLedger'in üzerine kuruldukları model, Bitcoin ve Ethereum gibi tamamen dağıtık bir model ile günümüz modern finansal sistemlerindeki merkezi modelin arasında kalmaktadır [BAZB19]. Bu modelde bankalar para arzını kendileri düzenlerler fakat işlemler için bir blokzincir kullanırlar. [BAZB19]'te kullanılan teknik ile her bankanın bir hesabının olduğu zkLedger'ınki arasında bazı benzerlikler vardır.

Yakın zamanda duyurulan Solidus ise [CZJ+17], gerçek dünya finans kuruluşu tabanlı bir yapıya sahiptir. Bu yapıda mütevazi sayılardaki bankaların her biri büyük miktarda kullanıcı hesabını yönetmektedir. Solidus, açık onaylanabilirliği koruyarak [CZJ+17], işlem değerlerini ve işlem grafını (tarafların kimlikleri de denebilir) gizler. Fakat protokol, zincir-içi ödemeli değer transferi ile sınırlandırılmıştır. İcra ve takas, gönderici ve alıcı bankalar tarafından yapılır.

Son olarak, Solidus'un denetleme desteği ancak sistemde kullanılan tüm anahtarların denetleyiciye verilmesi ve işlemlerin açılması ile mümkünken, yakın zamanda ortaya çıkan zk-Ledger [NVV18] Solidus'a yakın bir performans sergilemesinin yanında gizli denetlemeyi (private audit) de desteklemektedir.

zk-Ledger'ı kullanmanın ana dezavantajı, diğer bankaların hiçbirinin bakiyesi değişmediği için bir işlemin diğer tüm kısımlarının 0'a taahhütler içerebilmesidir. Bu verimsiz yapısı zkLedger'a güçlü işlem güvenliği kazandırmıştır: zkLedger, her işlemin her girdisi için hazırlanmış token'leri denetleyen ekstra sıfır bilgi kanıtlarını ve aralık kanıtlarını (ing. range proof) kullanmak karşılığında işlem grafını veya işlemlerarası bağlantıları açık etmez.

RSCoin [DM16], Solidus gibi denetlenebilirlik desteği olan bir merkez bankası kriptopara basma şemasıdır, ancak işlem mahremiyetini desteklemez. Bitcoin'deki gibi tek ve bütün bir blokzincirin tüm düğümlerce tutulması yerine RSCoin, para arzının oluşturulması ve kayıt defterinin bakımı olarak ikiye ayrılmıştır. Merkez bankası güvenilir üçüncü taraftır, para arzı ve işlem kaydı ile sorumludur fakat işlemlerin toplanması ve onaylanmasından sorumlu değildir. Merkez bankası, işlemlerin toplanmasını ve onaylanmasını, yani kayıt defterinin bakımını yönetmeleri için mintet'leri yetkilendirir. Kullanıcılar için yüksek haberleşme maliyeti, RSCoin'in cep telefonları gibi hafif cihazlar için gerçeklenmesini imkansız kılmıştır. Bu yüzden [HLX17]'da yazarlar, RSCoin'in kullanıcı trafiğini azaltmaya odaklanmıştır.

Son olarak, PRCash [WKCC18], güçlü güvenlik ve regülasyonu aynı anda garanti etmeye yarayacak sıfır-bilgi kanıtlarına dayalı yeni bir regülasyon mekanizması önermiştir. Ancak [SCG+14a]'da olduğu gibi sistem UTXO modeline dayanmaktadır ve bu yüzden hesap tabanlı sistemler için uygun değildir. Bunun haricinde regülasyon mekanizması herhangi bir kullanıcının belirli bir zaman periyodunda (epoch) alabileceği toplam anonim ödeme miktarını kısıtlamaktadır. Bu yüzden bu sistem, günümüz mevcut finansal sistemleri ile uyuşmamaktadır.

4.2 Mahremiyet Odaklı Blokzincir Platformları

Blokzincir platformlarının dayandırıldığı iki tasarım seçeneği bulunmaktadır; veri odaklı mimari (Bitcoin'in dayandırıldığı model olduğu ve oradan genelleştirildiği için bazen UTXO modeli diye de anılan) ve Ethereum'da da kullanılan hesaplama odaklı mimari. Sağlanan mahremiyet seviyesi blokzincir platformunun hangi modele dayandırıldığıyla yakından ilgilidir. UTXO modelleri tam anonimlik ve mahremiyet sağlayabilirken, aynı seviyeyi hesap tabanlı modellerde yakalamak hiç kolay değildir. İçerik mahremiyeti, ZKP ve şifreleme yöntemleri kullanılarak sağlanabilirken, anonimliği sağlamak için karıştırma (ing. mixing) gibi teknikler uygulanması gerekir. İzinli blokzincirlerde, mahremiyet sağlamak amacıyla eş düğümlere (peer node) özel modüller eklenmesi, problemin çözümünü kolaylaştırır. Bu alt bölümde, mahremiyet meselesi göz önünde bulundurularak tasarlanmış, genel amaçlı blokzincir platformları incelenecektir. Bitcoin ve Ethereum, güvenli blokzincir platformları olarak hizmet vermektedir. Bünyelerinde varsayılan olarak minimum düzeyde mahremiyet koruyucu özellik barındırırlar. Halefleri olan platformlar ve uygulamalar ise bu varsayılan yapı üzerine mahremiyet sağlayıcı özellikler koymuştur. İşlem verisi için mahremiyet sağlama mekanizmaları açısından Hyperledger Fabric ve Quorum birbirine benzer. Mutabakat protokolü sırasında veri şifrelenerek taşınır ve bu veriye, yalnızca şifreyi açabilen anahtarlara sahip bazı düğümler tarafından erişilebilir. Bu durum, blokzincir tarafından idare edilen iki çeşit durum (state) verisi olmasına sebep olur: sıradan işlem verisi ve mahrem işlem verisi. Her ne kadar işlem verisi korunsa da iki durumda da gönderici ve alıcı adresleri anonim değil yarı anonimdir. Aslında izinli blokzincirler için, Intel SGX veya HSM gibi donanım ve yazılım araçlarıyla desteklenmiş eş düğümlerle şebekeyi kurmak oldukça mantıklıdır. Bu düğümler, blokzincir yapısı hesap tabanlı (Account-based) olsa bile mahrem veriyi işleyebilirler. Ama aynı kolaylık, Açık blokzincir platformları için, özellikle de hesap tabanlı olanlar için, geçerli değildir.

4.2.1 Hyperledger Fabric

Hyperledger Fabric [Tea19b, Tea19a], mahremiyet sağlamak için kanal (channel) kavramını kullanan izinli bir platformdur. Temel itibariyle, işlemleri görmeleri istenen Fabric ağının bir grup katılımcısı arasında "kanal"lar kurulabilmektedir. Dolayısıyla yalnızca kanala üye olan düğümler akıllı kontrata (chaincode) ve işlenen veriye erişebilir. Mahremiyeti güçlendirmek adına Fabric geliştiricileri, mahrem veri desteği getirmiştir ve gelecekte uygulamaya koymak için sıfır bilgi kanıtları üzerine çalışmaktadır.

Veri mahremiyeti sağlamak için başvurulabilecek yöntemler şunlardır:

- Ağ, her biri kanala özel çalıştırılan akıllı kontratlara tahsis edilmiş veriyi görmek için yetkilendirilmiş bir grup katılımcıyı temsil eden kanallara bölünebilir.
- Kanal içinde, görünürlük ayarlarıyla oynayarak, akıllı kontrata girdi verme işi Endorser'lara mahsus hale getirilebilir. Görünürlük ayarları, gönderilen işleme, girdi ve çıktı akıllı kontrat verisinin mi yoksa yalnızca çıktı verisinin mi ekleneceğini belirler.
- Akıllı kontratı çağırmadan önce verinin özeti alınabilir veya şifrelenebilir. Orderer

düğümler, işlemleri yalnızca sıralarlar, içlerini açıp bakmazlar. Eğer verinin Orderer düğümlerinin elinden geçmesi istenmiyorsa ve yalnızca girdi verisiyle ilgileniliyorsa görünürlük ayarları bunu sağlamak için kullanılabilir. Girdi verisinin sadece, işlemin ön denetimini yapacak Endorser düğümlerce görülmesi sağlanabilir. Orderer düğümlerin, akıllı kontrat çıktısını görmeleri istenmiyorsa akıllı kontrat çağrılmadan önce veri şifrelenebilir veya özeti alınabilir. Özeti alınırsa verinin açık halinin paylaşılacağı bir araç da sağlanmalıdır. Eğer şifrelenirse, çözme anahtarlarının paylaşımı için bir yöntem sağlanmalıdır.

- Veri erişimi, akıllı kontrat içinde bir erişim kontrolü mantığı kurularak, organizasyondaki belirli bazı rollere tahsis edilebilir.
- Kayıt defteri verisi, blokzincir düğümünün dosya sistemi şifrelemesi kullanılarak şifrelenebilir. Düğümler arasında taşınmakta olan veriler TLS ile korunarak taşınabilir.

Fabric Platformundaki Güvenlik Mekanizması

Fabric, MSP'ler (Üyelik Servis Sağlayıcıları) vasıtasıyla işleyen kurallı bir yapıya sahiptir. Fabric, kullanıcılara hem güçlü kimlik doğrulama hem de çeşitli sistem operasyonlarını gerçekleştirmek için kimliklerini kanıtlama olanağı sağlayan bir üyelik altyapısı içerir.

Fabric Platformundaki Mahremiyet Mekanizmaları

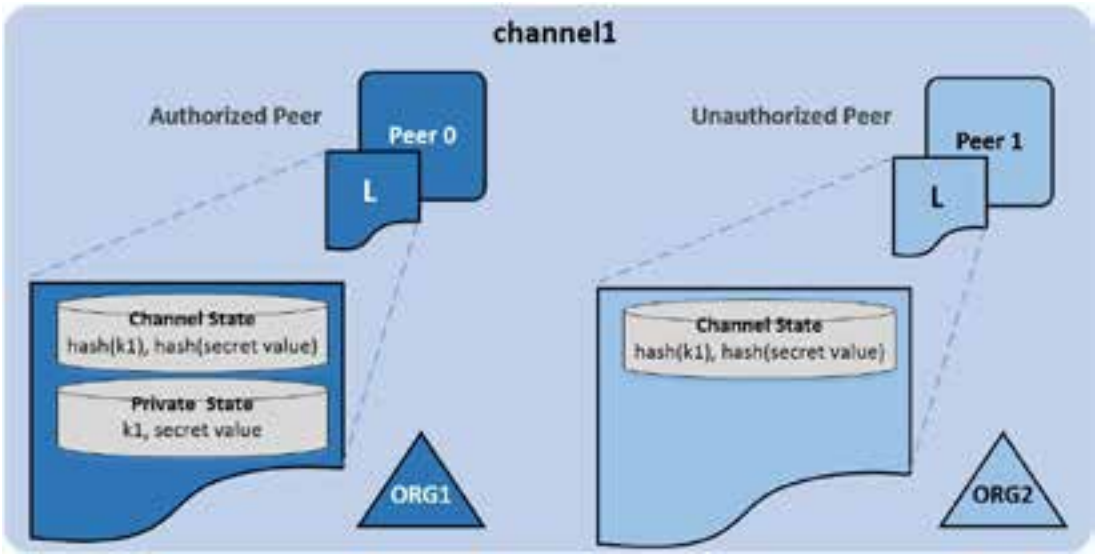
- **Kanallar:** Kanal mimarisi bazı kullanım senaryolarında mahremiyet sağlamak için kullanılabilir. Bir kanal, fiziksel blokzincir ağının üzerine oturtulmuş sanal bir blokzincir ağı gibi düşünülebilir. Kanallar kendi işlem sıralama mekanizmalarını kullandıkları için etkin işlem sırlama ve veri paylaşımının yanısıra ölçeklenebilirlik sağlarlar. Kanallar, kanal kaynaklarına (chaincode, işlemler ve ledger state'i gibi) erişimi düzenleyen erişim politikalarına sahiptir. Bu sayede kanal üyeliği çerçevesinde bilgiye erişimi kısıtlarlar. Kanallar ayrıca mahremiyeti güçlendirmek için mahrem işlemler ve sıfır-bilgi kanıtları ile birlikte kullanılabilir.
- **Mahrem İşlemler:** Yeni kanallar açmak gibi mekanizmalar yönetimsel olarak ek yük oluşturur (chaincode versiyonlarının kontrolü, politikalar, MSP'ler, vs.). Ayrıca tüm kanal katılımcılarının bir işlemi görmesi ama bir katılımcıdan verinin bir kısmının gizlenmesi gereken kullanım senaryolarını desteklemez.

Fabric 1.2 sürümü, bir kanaldaki organizasyonların tanımlı bir altkümesinin, ayrı bir kanal açmak zorunda olmadan mahrem veriyi doğrulamasını,oluşturmasını veya sorgulamasını sağlayan mahrem veri koleksiyonlarına izin verir. Mahrem işlemler, kanallara nispeten daha detaylı işlem mahremiyeti sunar.

Mahrem işlemler sayesinde hassas (mahrem) verinin, açık kayıt defterinde yalnızca özeti tutularak işlemle ilgili olan taraflar arasında P2P dağıtımı yapılır. Mahrem veri, yalnızca onu görmeye izni olan organizasyonlara ait eşlere Gossip protokolüyle gönderilir. Mahrem veri, erişim izni olan organizasyonların düğümlerinin üzerinde mahrem

durum veritabanı ("yan" veritabanı ya da "SideDB" de denir) içerisinde tutulur ve Fabric altyapısı tarafından idare edilir. Erişim izni bulunan eşlerdeki akıllı kontrat vasıtasıyla SideDB'ye erişilebilir. Mahrem veriye referanslar içeren işlemler onaylandıkça açık kayıt defteri yanında bu mahrem veritabanı da güncellenir.

Şekil 4.1: **Fabric'te normal ve gizli durum bilgileri ayrımı**



Açık kayıt defterindeki özet değerleri, veriye dair doğrulanabilir kanıt niteliği taşır ve doğrulama için kullanılır. Ayrıca denetleme amacıyla da kullanılabilirler. İşlem sıralayıcı (Orderer) burada işin içinde değildir ve mahrem veriyi görmez. Verinin özeti onaylanır, sıralanır ve ardından kanaldaki her eşin açık kayıt defterine yazılır.

Mahrem verinin açık halinin, işleme dahil olan tarafların dışına çıkmasına izin verilmez. Bu olayı yansıtan bir örnek sağlık sektöründen verilebilir. Mesela belirli yaşlardaki sağlık kayıtları yalnızca belirli bir süreliğine açık edilmelidir (örneğin hastanın reçete geçmişinin cerrahi bir operasyonunun belirli bir miktar zaman öncesinden uzman doktora açık edilmesi gibi). Mahrem işlemler, yalnızca hastanın ve uzman doktorun belirli bir süreliğine bilgiyi görmesini sağlayıp bilginin özetini de işlemin gerçekleştiğine dair kanıt olarak açık kayıt defterine kaydederek veri mahremiyetini sağlarlar. Mahremiyet, kimin hakikaten hassas bilgiye erişebileceğini kontrol edebilmeyi gerektirir. Mahrem işlemler, mahrem veri güncelleme örüntülerinin de hassas bilgi olduğu ve hassas veriye erişmede basamak olarak kullanılabileceği durumlarda dikkatlice kullanılmalıdır. Hyperledger Fabric mimarisi her ne kadar gerçek mahrem veriye izinsiz erişimi ve değiştirilmesini engellese de açık kayıt defter katılımcılarının bu mahrem verinin ne zaman değiştirildiğini öğrenmelerini engellemez. Mahrem veri özetleri, değişimi herkese açık olan kayıt defterinde anahtar-değer (key-value) çiftleri olarak tutulur. Ayrıca mahrem işlemler mekanizması, mahrem veriye erişimi olan tarafları gizleyemez. Bu bilgi, mahrem veri dağıtımının düzgünce yapılabilmesi için kayıt defterinde açık halde bulunmalıdır.

Bu sebeplerden ötürü mahrem işlemler, işlem yaratıcısının kimliği ile açık kayıt defterinde depolanan veri (özeti) arasındaki bağlantıyı açık etmemek için anonim istemci kimlik denetimi mekanizmaları ile desteklenmelidir.

Kanallar, kanalın üyesi olan bir grup organizasyon arasındaki tüm işlemlerin (ve kayıt defterlerinin) gizli tutulmasının gerektiği zamanlarda kullanılmalıdır. Koleksiyonlar ise işlemlerin (ve kayıt defterlerinin) bir grup organizasyon arasında paylaşılacağı ama yalnızca bu organizasyonların bir altkümesinin işlemlerdeki bazı (veya tüm) verilere erişmesinin gerektiği durumlarda kullanılmalıdır. Bunlara ek olarak, mahrem veri bloklar şeklinde değil de eşler arasında yayıldığından, işlem verisinin, Orderer düğümlerden gizli tutulması istendiğinde mahrem veri koleksiyonları kullanılmalıdır.

Eğer mahrem veri nispeten basit ve tahmin edilebilir yapıda ise (dolar miktarı gibi), mahrem veri koleksiyonuna erişim izni olmayan kanal üyeleri zincirdeki özetle eşleşme bulmak ümidiyle veri uzayına kaba kuvvet (brute force) saldırısı yaparak mahrem verinin içeriğini tahmin etmeye çalışabilir. Bu yüzden tahmin edilebilir mahrem veri durumlarında, özet değerleri hesaplanmadan önce, mahrem veri anahtarının ve mahrem verinin kendisinin değerine rastgele tuz (gürültü) değerleri eklenmelidir ki kaba kuvvetle özet değeri tutturmak mümkün olmasın. Rastgele tuz değeri istemci uygulama tarafında üretilip (mesela güvenli pseudo-random bir kaynak kullanılarak) akıllı kontrat çağrıldığında geçici bir alanda, mahrem veri ile birlikte iletilebilir.

Versiyon 1.3'e kadar mahrem veriye, koleksiyon üyeliğine dayalı erişim kontrolü yalnızca eşler için uygulanıyordu. Chaincode önerisi göndericisi tabanlı erişim kontrolü ise akıllı kontrat içinde kodlanmak zorundaydı. v1.4'ten başlayarak memberOnlyRead isminde bir koleksiyon konfigürasyon seçeneği, bu işi otomatik olarak yapmaya başlamıştır.

Sıfır Bilgi Kanıtları(ZKP) Tabanlı Teknolojiler Fabric 1.3 ve sonrasının sınırlı ZKP desteği vardır. Fabric'in ZKP ile ilgili aşağıdaki iki mahremiyet sağlama amaçlı yetenek hedefi vardır. Ancak ZKP halen yalnızca Kimlik Karıştırma sertifikaları kullanılırken anonim/ilişkilendirilemez sertifikalar için kullanılmaktadır.

>> **Kimlik Karıştırıcısıyla Anonim İstemci Kimlik Denetleme:** Hyperledger Fabric bünyesindeki Idemix mimarisiyle anonimlik (kimliğinizi açık etmeden işlem yollamak) ve ilişkilendirilemezlik (birçok işlem yolladığınız halde yolladığınız işlemlerin aynı kaynaktan geldiklerine dair bilgi sızdırmamak) sağlar. Idemix, Fabric 1.2'den beri desteklenmektedir. ZKP, istemcilere, işlemlerinde anonim kimlik denetimi olanağı sunar. ZKP protokolleri, sırrı kendi gerçek kimliği (ve onunla ilgili olan diğer özellikler) olan Fabric istemcisi ile ağdaki diğer elemanlar (mesela istemcinin paydaşları) arasında gerçekleşir. Bu elemanlar, bir işlemin yaratıcısının belirli bir organizasyonun üyesi olduğunu (üyelik kanıtı da denir), veya spesifik bir takım özelliklere haiz olduğunu (özelliklerin seçici teşhiri de denir) onaylamak isterler. İki durumda da protokoller, karşılık gelen önermenin doğruluğundan öte istemcinin kimliği hakkında hiçbir şeyin ifşa edilmediğini garanti ederler. ZKP'lerin gücünü gösteren temel bir örnek vermek gerekirse, sadece yaş kontrolü ile girilebilen bir tesisin girişinde güvenlik görevlisine kimliğinizi gösterirseniz, pek çok bilginizi göstermiş olursunuz. Eğer ZKP kullanırsa-

nız kimliğinizi, kimliğinizin gerçek bir kimlik olduğu gerçeğini ve yaşınızın tesisin izin verdiği aralıkta olduğu gerçeğini koruyan fakat diğer bilgilerinizi gizleyen bir forma dönüştürmüş olursunuz.

›› ZKAT (Sıfır Bilgi Değer Transferi) ile Mahremiyet Muhafazalı Değer Değiş Tokuşu: ZKAT'ın yeteneğinin ilk duyurusu 2018'de olmuştur. ZKP'nin diğer işlem çeşitlerinde uygulanması amacıyla yürütülen araştırmalar mevcuttur ama henüz tam olarak devreye girmemiştir.

Bu özellik ZKP'yi, değer yönetimini hedefleyen daha geniş uygulama alanlarıyla entegre edecektir. ZKAT, işlem aktörlerinin aralarındaki değer aktarımını ve bu değerin transferinin talebini, blokzincir kayıt defterine, transferin değer yönetimi kurallarına uygunluğu (her değer, sahibinin isteğinin ardından transfer edilir ve transfer süreci yeni bir değer üretmez) dışında hiçbir bilgi sızdırmadan gerçekleştirmelerine izin verir. ZKAT, Identity Mixer tarafından sunulan anonim kimlik denetleme mekanizmaları üzerine inşa edilmiştir. Blokzincir için geliştirilmiş diğer mahremiyet koruyucu değer sistemlerinin aksine ZKAT, şirket ağlarının ihtiyaçlarına göre şekillendirilmiştir.

Gizliliğini korunan işlemlerin denetlenebilirliği konusu, piyasadaki rakipleriyle arasındaki en önemli farklılıktır. Her kullanıcıya, o kullanıcının tüm işlemlerine sınırsız erişim hakkı veren bir denetçi atanır. Bir denetçi gelip, denetlediği kullanıcının tüm gizli işlemlerini okuyabilir ama diğer kullanıcıların işlemlerine erişemez. Denetimli gizlilik, özellikle finansal kullanımlarda faydalıdır. İşlemlerin bulunduğu kayıt defteri paylaşımlıdır, ancak işlemleri, bu işlemlerin kimler arasında gerçekleştiğini ve işlemdeki değerleri açık etmez. Bu yetenek, gizlilik yönetmeliklerine uyumu artıracak ve yeni iş modelleri ortaya çıkaracaktır. Sıfır bilgi ispatları ile değerin (paranın) harcanabilir olduğunun ispatı, işlemlerin içinde bulunabilir, bunu yaparken de para miktarlarını, borç faizlerini veya işlemin hangi bankayla gerçekleştiğini açık etmez. Bir diğer avantajı ise şu anda ZKAT'e göre denetlenebilmeleridir. Örnek olarak, 3 gizli değer

Şekil 4.2: **Senaryolarla mahremiyet dereceleri [Tea19b]**

yönetim modeli (UTXO'nun genişletilmiş uyarlamaları), var olan blokzincir sistemine adapte edilmiş (Şekil 4.2'de gösterilen); 3 banka (BANKA A, BANKA B and BANKA C), 3 farklı değer(Loyyal points, Water Canary, MFG) ile blokzincir üzerinden transfer gerçekleştirilmiştir.

Resimde, soldaki modelde gizlilik mekanizması yok. Ortadaki model tam gizlilik sağlar, işlemin kimler arasında gerçekleştiğini ve varlıkların ayrıntılarını gizler. Sağdaki model ise ZKAT'in güvenli denetleme kabiliyetini gösterir yani banka denetçi rolündedir ve bu bankayla olan işlemlere, kısıtlanmamış bir şekilde erişebilir. Sıfır bilgi ispatı protokolleri, varlık yönetimi için kullanıldığında güçlü bir güvenlik sağlar. Sadece işlem'e katılanların anonimliği değil, varlıkların işlem geçmişinin izlenebilirliğinini ortadan kaldırır. Kullanıcıların, uzun süreli kimlikleri üzerinde de işlemle alakalı kullanıcıların hesap verebilirliğini, inkar edemezliğini sağlanır. Blokzincir üzerinde gizliliği korunan işlemlerin, güçlü ve güvenli denetlenme özelliklerini sağlar. Hyperledger Fabric'in protokolleri, denetçinin bir veya birden fazla olduğu ancak işlemlere dahil olmayan denetim modelini destekler. Bu protokoller, denetçilerin, kullanıcıların onlara verdiği yetkiye dayanarak, işlemleri denetleyebilmesini garanti eder. Denetçi bunu yaparken, sadece blokzincirdeki işlem log'larına bakar. Ekstra bir avantaj ise Hyperledger Fabric ZKAT'a bağlı olarak denetlenebilir. Hyperledger'daki protokoller, standart kriptografik yaklaşımlarına dayanır ve kuruluma ihtiyaç duyar.

4.2.2 Quorum

JP Morgan tarafından geliştirilen Quorum, mahremiyet özellikleri sağlayan bir başka blokzincir platformudur[Tea19d]. Quorum, Go Ethereum(geth) kodu değiştirilerek oluşturulmuştur ve yeni özellikler eklenerek genişletilmiştir (işlem ve kontrat gizliliği, çoklu-oylama bazlı konsensus mekanizmaları, ağa giriş izinlerinin yönetimi ve yüksek performans vb.). Quorum, Ethereum'un İzinli Ağ türünden bir gerçeklemesidir.

Quorum aşağıdaki bileşenleri içerir:

- Quorum Düğümü (modifiye edilmiş Geth istemcisi)
- Constellation/Tessera-İşlem Yöneticisi (Transaction Manager)
- Constellation/Tessera-Enclave: Özel anahtar yönetimi, şifreleme ve özel işlem verilerinin şifresini çözmekten sorumludur.

Consellation modülü, Quorum'da gizliliğin en önemli bileşenidir. Bu ve Tessera, sisteme güvenli yoldan bilgi yüklemek için kullanılan Haskell ve Java dillerinde gerçeklenmiş modüllerdir. Mesajların PGP ile şifrelendiği MTA (Mesaj Transfer Etmenleri) ağı ile kıyaslanabilir. Bu yetenek, blokzincire özel değildir, potansiyel olarak, herhangi bir ağdaki katılımcılar ile ayrık bir biçimde mühürlenmiş mesaj alışverişi yapılabilmeye olanak sunar.

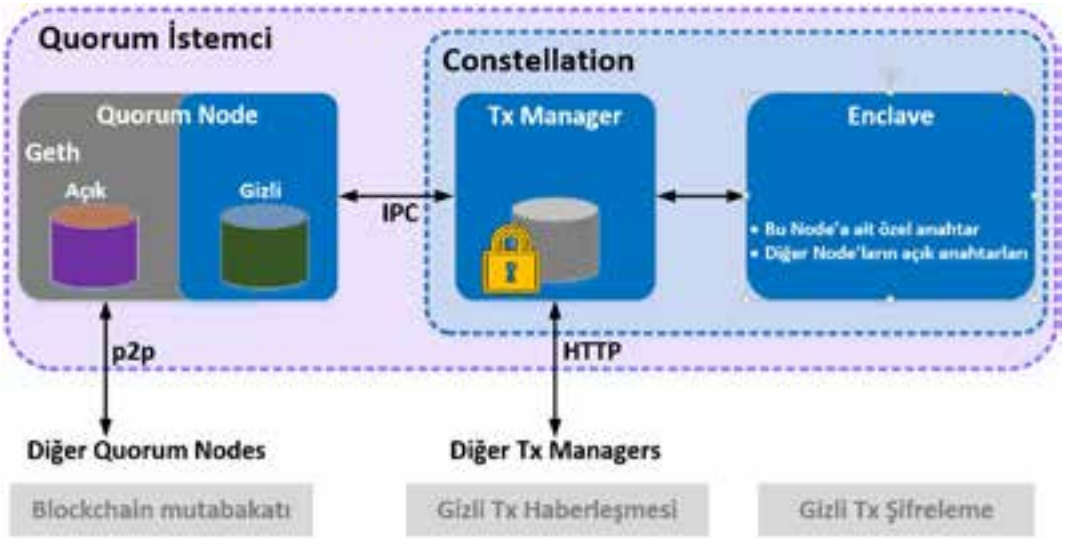
İşlem yöneticisi durumsuzdur (stateless). Enclave, gizliliği güçlendirmek için şifreleme ve deşifrelemeyi izole bir yoldan yapar ve bunu yaparken işlem yöneticisi ile birlikte çalışır. Özel anahtarları tutar ve esasında diğer katılımcılardan izole bir "Sanal HSM"'dir.

Quorum'daki mahremiyet özellikleri aşağıdaki gibidir:

1. Ağ ve katılımcı izinleri yönetimi. Quorum izinli bir blokzincir ağıdır. Sadece bir otorite tarafından yetkilendirilmiş ve onaylanmış kişiler bu ağın bir parçası olabilir.

2. İşlem ve kontratın gizliliğini artırır. Ethereum gibi birçok blokzincir platformu, verinin güvenliğini tümüyle garanti edemez. Görünürlük ve erişilebilirlik kolaylığı blokzincirin kilit unsurlarından biri olduğundan, bankacılık ve finans kuruluşları bu teknolojiyi kullanmaktan kaçınmaktadır. Fakat, Quorum'un yapısı, bunu elverişli bir hale getirir. Açık ve Gizli işlem ayrımı vardır. Açık işlemler Ethereum'a benzer ancak gizli işlemler daha güvenlidir ve dışarıya açık edilmez. Quorum açık işlemleri (standart Ethereum işlemleri) ve gizli işlemleri birbirinden ayırır. Gizli işlemlerin verisi, sadece işlemde açık anahtarları belirtilen ağ düğümleri tarafından görüntülenebilir. Açık akıllı kontratların içindeki veriler ise bütün düğümler tarafından görüntülenebilir. Gizli işlemler için, veri transferi ve depolaması zincir dışı (off-chain) gerçekleşir. Constellation modülü mesajı gizler. Burada önceki işlemlerin kimlik doğrulamaları da vardır.

Şekil 4.3: **Qurom düğümünün bileşenleri.**



Özel/Gizli kontratlar, bu kontrata erişmeye ve kontratı çağırmaya hangi düğümlerin yetkisi olduğunu belirtir. Diğer düğümler kontratın kodunu veya verisini göremez, sorgulayamaz çalıştıramaz. Quorum, Constellation sistemi ile gizli mesaj transferini yönetir. Constellation, blokzincire özgü olmayan genel amaçlı bir mekanizmadır. Belirli mesajları Enclave yardımıyla şifreler. Eski işlemlerin deposu, orijinallik ve kimlik doğrulamalarını içerir. Kriptografik işler bu modülde yapılır.

Gizlilik/Mahremiyet

>> Özel kontratlar, açık kontrat olarak değiştirilemezler. Çünkü bütün katılımcıların bu özel kontratı çalıştıramaması istenir.

>> Açık kontratlar ise sonradan özel kontrat olarak değiştirilemezler. Eğer açık kontratı, özel yapmak isteniyorsa, açık olan blokzincirden silinmeli ve yeni özel kontrat oluşturulmalıdır.

Quorum gizli işlem desteği:

Gizli işlemlerde veri, sadece "privateFor" parametresinde belirlenen açık anahtarlara sahip ağ düğümleri tarafından görülebilir. Quorum düğümü, işlemi ağ aracılığıyla göndermeden önce, veri Enclave tarafından şifrelenir ve İşlem Yöneticisi tarafından depolanır. Şifrelenmiş mesajın özeti, verinin kendisine değil de işleme eklenir ve ağa dağıtılır. PrivateFor parametresinde belirtilen düğümler, işlemin verisini Constellation bileşeninden alır. Diğer düğümler ise sadece mesajın özetini görebilir. Bütün adımlar aşağıdaki diyagramda görülebilir.

Constellation protokolü, şifrelenmiş mesaj alışverişi için kullanılır. Özel işlemler şöyle çalışır: Her düğümün kendisine ait açık ve özel anahtarları vardır. KullanıcıA, KullanıcıB ile özel bir iş yapacaksa (privateFor = AçıkAnahtarA, AçıkAnaharB şeklinde tanımlanmalıdır.) aşağıdaki adımlar izlenir [Tea19c]:

- **KullanıcıA'nın Enclave'i**
  - Göndereni doğrular.
  - Rastgele simetrik anahtar ve TEKSA(nonce) üretir, bunları kullanarak işlemi şifreler. *k<–Gen, ETX<–ENC$_k$(TX +NONCE)*
  - KullanıcıA'nın özel anahtarını, KullanıcıB'nin açık anahtarını ve ikinci bir nonce'ı (NONCE2) kullanarak paylaşımlı gizli anahtar üretirler.
  - Paylaşımlı anahtarı kullanarak, simetrik anahtar'ı şifreler. *EK<–ENC$_{pubB}$(k + NONCE2)*

- **KullanıcıA'nın İşlem Yöneticisi**
  - Şifreli işlemden SHA3-512 özeti üretir. *HASH<–SHA3(ETX)*
  - ETX ve EK'yı depolar.
  - ETX, EK, NONCE2'yi KullanıcıB'ye aktarır (HTTPS ile). Zincir üzerinde: ÖZET, zincir dışında: *ETX, EK*.
  - İşlemi Quorum düğümüne gönderir.

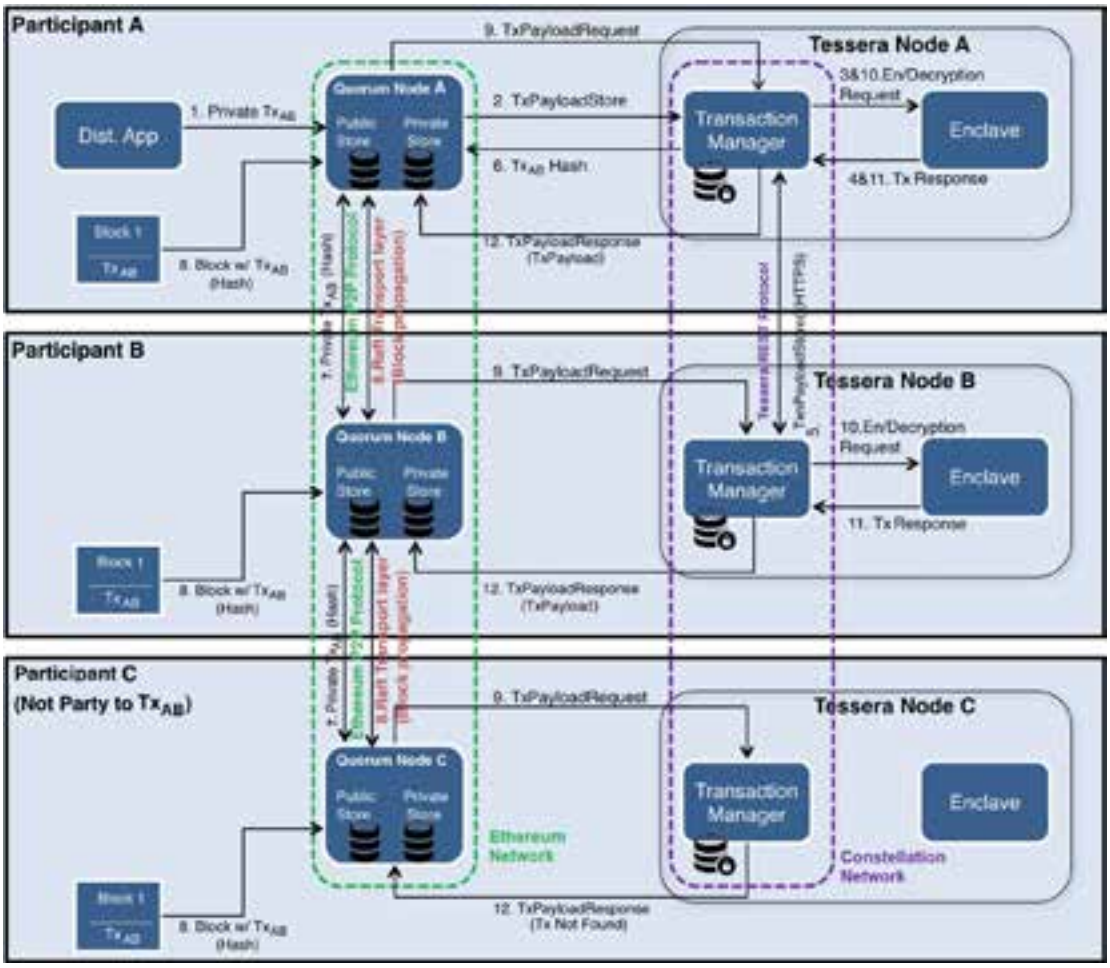
- **KullanıcıB'nin İşlem Yöneticisi ve Enclave'i**
  - KullanıcıA'nın açık anahtarı, KullanıcıB'nin özel anahtarını ve NONCE2'yi kullanarak paylaşımlı gizli anahtarı türetir.
  - Kendi özel anahtarını kullanarak, simetrik anahtarın şifresini çözer ve şifreli işlemin özetini üretir. Zincir'deki özet ile eşleşip eşleşmediğine bakar ve eşleşirse işlem verisinin doğru olduğunu bilir.
  - Simetrik anahtarı kullanarak işlemi deşifre eder.

Veriye istenilmeyen erişimden kaçınmak için, sadece işlemin özeti zincir üzerinde depolanır. Diğerleri zincir dışında saklanır. Özet, işlem verilerinin yeniden oluşturulmasına izin

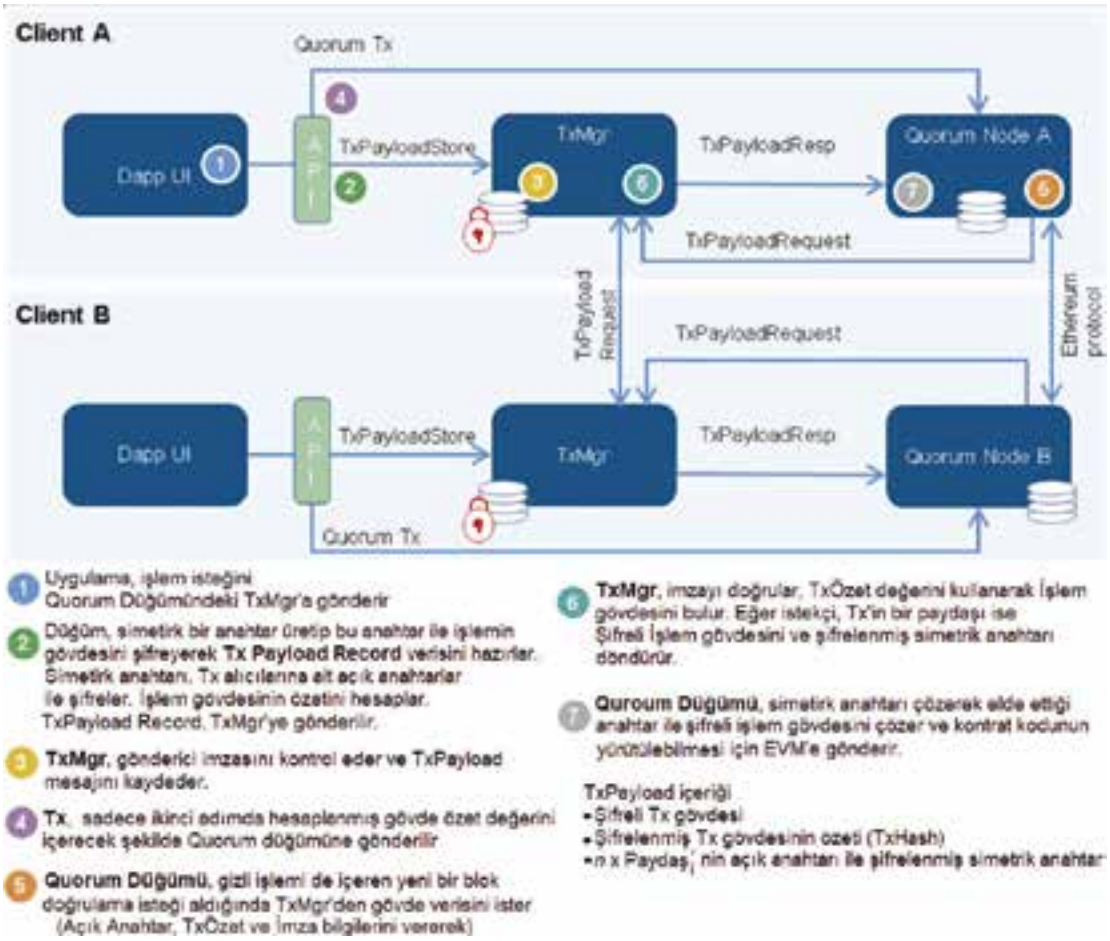
vermez; fakat, işlem verilerinin doğru olduğunu doğrulamaya izin verir (eğer veriler değişirse özet değeri farklı olacaktır ve zincirdeki özet ile eşleşmeyecektir).

Quorum'daki özel işlemler, kullanıcıların gizli işlemler göndermesini sağlar. Buna kontrat çağrısı içeren işlemler de dahildir. İşlemdeki gizliliğe ek olarak, akıllı kontratlar için de gizlilik vardır.

Şekil 4.4: **Quorum gizli işlem akışı**



Şekil 4.5: **Quorum gizli işlem akışının detayları**



Pek çok banka özellikle güvenlik nedeniyle ifşaya açıktır. Bu akıllı kontratlar; yatırım stratejileri, işlem verileri veya hassas iç bilgiler içerebilir. Akıllı kontratlar için hazır protokoller aslında nispeten basittir ve aşağıdaki diyagramda gösterilmektedir:

İşlem Yöneticisi tarafından Enclave'a gönderilen her bir payload'ın şifrelenmesinden sonra, Payload Bölümü (PC) ve N Alıcı Kutuları (RB'ler) üretilir, burada N, İşlemin privateFor alanında belirtilen alıcıların sayısıdır. Enclave, xsalsa20poly1305'i kullanarak PC'yi, curve25519xsalsa20poly13 kullanarak ve RB'leri şifreler.

>> Payload Bölümü (PC), simetrik bir anahtar ve rastgele bir nonce ile şifrelenmiş payload içerir.

>> Bir alıcı kutusu (RB), alıcının açık anahtarı için rastgele bir nonce kullanarak şifrelenmiş, PC için Ana Anahtardır.

Mevcut Quorum gerçeklemesinde, tüm açık anahtar beyaz-listeleri el ile tanımlanır ve ayrıca anahtarların otomatik rotasyonu da yoktur. Bununla birlikte, sistem, karşı tarafların aynı

anda birden fazla anahtarı açık etmesine izin vererek, dönüşü önemsiz bir şekilde desteklemek için inşa edilmiştir. Quorum'un kullandığı bir PKI sistemi de yoktur, ancak rastgele olarak beyaz listeye elle eklenen anahtarlar (örneğin, blokzincirdeki yetkili eşlerin bir kaydı) kullanılır. Quorum ekibi, sıfır bilgi güvenlik katmanını (ZSL) Quroum protokolüne entegre etmek için Zcash ekibiyle birlikte çalışmaktadır. Çalışma henüz üretime hazır olmasa da konsept onaylı teknik tasarım belgesi yakın zamanda yayımlanmıştır.

4.2.3 Corda

Corda, gizlilik özelliklerine sahip bir başka kurumsal blokzincirdir. R3 Bankacılık Konsorsiyumu tarafından, özellikle finansal hizmet sektörü için oluşturulmuştur ve yasal gerekliliklerle uyum sağlamak amacıyla tasarlanmıştır[TK19a].

Her bir blokzincir düğümü, ağda işlenen işlemlerin hepsini değil, yalnızca bir kısmını görür. Tüm işlemleri içeren tek bir mantıksal kayıt defteri tanımlanırken, bu defterin bütünü tek bir düğüm tarafından görüntülenmez. Corda düğümü, sadece doğrudan dahil olduğu (işlemlerin girdi veya çıktısının kendi kullanıcısı olduğu) işlemleri görebilir. Bir işlemi sisteme gönderecek kişi, ayrıca, varlığın yaratıldığı orijinal işleme ("issuance transaction") kadar olan yoldaki işlemleri de sisteme sağlamak zorundadır. Doğrulamak için gereken işlem sayısı, varlıkların kaç kez el değiştirdiğine ve geriye doğru dallanmanın derecesine bağlıdır.

R3 Corda'daki akıllı sözleşmelere yasallık kazandırmak için koda ek olarak belirli yasal ifadeler vardır. Hyperledger Fabric platformu gibi, R3 Corda, düğümleri belirli rollere böler ve mutabakat PoW'dan farklı yolla yapılır. Mutabakat mekanizması, işlemin geçerliliğinin(validity) ve tekilliğinin(uniqueness) kontrolünü gerektirir. Akıllı sözleşmeler geçerliliği garanti eder. Söz konusu işlemin girdisi olan varlıkları tüketen başka işlemler yoksa, işlemin tekilliği de doğrulanmış olur.

Tüm katılımcı düğümler arasında verinin yayımlandığı çoğu blokzincirin aksine, Corda, verileri kontrol altında tutmak ve paylaşılması gereken bilgi miktarını sınırlamak için tasarlanmıştır. CordaNotary hizmeti, yasal olup olmadıklarını kontrol etmek için, işlemleri görüntüleyebilen onaylama noterlerinin kullanımı ile bunun yerine sadece bir kayıt tutabilen onaylama yapmayan noterler arasında bir seçenek sunar.

Corda'nın mahremiyet özellikleri için, adres rastgeleleştirmesi, sıfır bilgi ispatları, varlıkların yeniden yayımlanması (reissuance) şemaları gibi teknolojileri kullanır.

Corda, kullanıcı mahremiyetini artırmak için birçok teknikten yararlanır [RGB16], [Hea16]:

- **Kısmi veri görünürlüğü:** İşlemler, diğer birçok blokzincirinden farklı olarak blokzincir çapında yayınlanmamaktadır. Corda, işlem geçmişini, bilmesi gereken prensibine göre sadece ilgili düğümlerle paylaşır.
- **İşlem bilgisi parçalanabilirliği:** İşlemler Merkle ağaçları olarak yapılandırılmıştır. İşlem bilgisinin alt parçaları, işleme ait Merkle özet kökünü bilen taraflara açıklanmasına

olanak sağlanır. Buna ek olarak, taraflar, işlem bilgisinin tamamını göremeden imzalayabilirler.

>> **Anahtar rastgeleleştirmesi:** Düğümdeki cüzdan, ilgili bağlantı sertifikası olmadan, bir kimliğe bağlanamayan rastgele anahtarlar üretir ve kullanır.

>> **Grafik budaması:** Likit varlıkları içeren büyük işlem grafları, varlığı ilk üreten kuruluştan varlıkları kayıt defterine yeni bir referans alanı ile yeniden yayımlamaları istenerek budanabilir. Bu işlem atomik değildir, ancak varlığın yeni sürümünün eski sürümlerinden etkin bir şekilde ilişkisinin koparılmasını sağlar. Yani, düğümler doğrulama sırasında orijinal bağımlılık grafını keşfetmeye çalışmaz.

Yukarıdaki özelliklere ek olarak, Corda, aşağıdaki ek mahremiyet teknolojilerinin gelecekteki entegrasyonu göz önünde bulundurularak tasarlanmıştır:

>> **Güvenli donanım:** Veriler yalnızca bu verileri görmesi gereken düğümlere yayılsa da yalnızca güvenlik denetimlerini gerçekleştirmek için veriler gerekir. Kontrat doğrulama işlemini, Intel SGXTM ile güçlendirilmiş bir JVM içinde koşturmak planlanmaktadır. Güvenli donanım platformları, sadece kendilerinin erişebileceği şifreleme anahtarları üretme ihtiyacı duyan bu güvenli ortam içindeki yazılımlar ve üçüncü taraflara uzaktan, bu yazılımın güvenli modda çalıştığını ispatlayacak olan yazılımlar için hesaplamanın kurcalamaya karşı korumalı bir yürütme ortamında yapılmasına imkan tanır. Akıllı kontrat doğrulama işini bir güvenli bölge içinde gerçekleştirdiklerini birbirlerine uzaktan ispatlayabilen düğümlerin bulunması sayesinde, bir işlemin bağlantılı bilgilerinin, bir güvenli donanım anahtarı ile şifrelenmiş olarak diğer düğümlere aktarılması mümkün hale gelir, böylece kendi denetledikleri yazılımı kullanarak ancak üzerinde çalıştığı verileri görmeden bağımlılıkları doğrulamaları sağlanır. Bu sayede, düğümler, işlemin bağlantılarını, kendi kontrollerinde olan ama işlediği verileri göremedikleri yazılımlar ile doğrulayabilirler. Güvenli donanım, akıllı sözleşmeleri oldukça basitleştirme potansiyeli taşımaktadır. Bununla birlikte, hassas verilerin hala, iş zekasını şifreli yapının içinden çıkarmak için donanıma saldırmaya veya yan kanal bilgilerinden yararlanmaya çalışabilecek eş düğümlere gönderilmesi gerekmektedir.

>> **Karıştırma ağları.** Noter ve Düzenleyici gibi bazı düğümler, kendileri ile ilgili olmayan işlemler hakkında bilgi edinme konumunda olabilirler. Anahtar rastgeleleştirmesi kullanılsa bile, bu düğümler hala kaynak IP'yi veya düğümlerin kendilerine gönderdikleri kimlik doğrulama sertifikalarını inceleyerek değerli kimlik bilgilerini öğrenebilirler. Buradaki sorunun geleneksel kriptografik çözümü karıştırma ağıdır [Cha81]. En ünlü karma ağ Tor'dur, ancak Corda için tam uygun değildir. Bir karma ağda bir mesaj, rastgele seçilen küçük bir düğüm kümesinin sahip olduğu anahtarlar kullanılarak soğan benzeri bir tarzda tekrarlı olarak şifrelenir. Soğandaki her katman, bir sonraki gidilecek katmanın adresini içerir. Mesaj ilk katmana iletildiğinde, bir sonraki şifreli katmanı ortaya çıkarmak için şifresini çözer ve iletir. Geri dönüş yolu da benzer şekilde çalışır. Corda protokolüne bir karıştırma ağı eklemesi, kullanıcıların yüksek gecikme süreleri yaşaması ve başarısız ağ düğümlerinden daha fazla etkilenmesi pahasına mahremiyet yükseltmesine olanak sağlar.

>> **Sıfır bilgi kanıtları.** Corda veri modeli, zkSNARK kullanmaya hazır halde tasarlanmıştır. Corda içinde ZKP kullanımı konusunda çalışmalar sürmektedir. Yakın zamanda, ING DLT ekibinin yayımladığı makale [TK19b], bulletproof tabanlı ZKP kullanarak Corda platformunda mahremiyet artıran bir çözümü tanıtmıştır. Bu çözümde, ZKP tabanlı noter servisi, işlemlerin geçerliliğini, mahrem içeriklerinin ifşa edilmesini gerektirmeden kontrol edebilmektedir.

4.2.4 Hyperledger Indy

Hyperledger Indy, Everynym firması tarafından geliştirilip 2017 yılında Hyperledger platformuna bağışlanmış ve bu platform altında geliştirilmeye devam eden, dijital kimlik yönetimi odaklı blokzincir platformudur. Mahremiyeti sonradan yapılarına katan diğer pek çok blokzincir platformlarının aksine, tasarımında mahremiyet amacı güdülerek geliştirilmiştir. GDPR benzeri kişisel veri koruma düzenlemelerine, diğer blokzincir platformlarına göre daha fazla uyum seviyesine sahiptir.

Merkezi kimlik sağlayıcılara olan bağımlılığı ortadan kaldırarak kullanıcı egemen kimlik modelini hayata geçirmeye imkan sağlar.

Indy kayıt defterinde kullanıcıların açık kimlikleri (kişi ve kurumlara ait öz nitelikler) depolanmaz. Sadece hizmet erişim noktalarına referans işaretçiler tutulur. Öz nitelikler, açık veya sıfır bilgi ispatları kullanılarak mahrem bir şekilde, doğrulanabilir öz nitelikler (verifiable credential) olarak servis sağlayıcılarla paylaşılabilir. Indy blokzincirinin kendisinin de dahil olduğu kimlik yönetim modeli tarafından mahremiyet artıran pek çok yetenek sunulmaktadır. Bu yetenekler arasında, zincir dışı güvenli ikili haberleşme kanalları, tarafların ilişki başına kullandıkları parametreler (pair-wise did), sıfır bilgi ispatları sayesinde sınırlı veri ifşa teknikleri, kişisel verilerin zincir dışında kullanıcı cüzdanlarında tutulması, kişisel verilerin sistemden mahremiyeti ihlal etmeden imha edilebilmesi sayılabilir. Indy blokzinciri üzerinde depolanan meta bilgiler ve paylaşılan doğrulanabilir öznitelik bilgilerinin meta bilgileri doğru kullanılmaz ise işlemler ile kişiler arasında ilişki kurulmasına neden olabilir.

4.2.5 Diğer Platformlarda Mahremiyet

NEO, Incognito (PoS tabanlı ZKP kullanan blokzincir platformu) ile başlattığı işbirliğinde (Aralık 2019) mahrem işlem desteği eklemek üzere çalışmaya başlamıştır. Hedeflenen mimari, işlem paydaşlarının kimliklerinin gizlenmesini sağlamanın yanı sıra ZCash ve Monero'da olduğu gibi mahrem paralar da içerecek. NEO'ya Incognito tarafından sağlanacak yanzincir sayesinde işlemlerin gizliliği ve anonimliği sağlanacak. Sistemde, CryptoNote ile Monero'nun kullandığı teknolojilerin (halka imza, Bulletproof sıfır bilgi ispatı, görünmez adres, mahrem işlem) kullanılması planlanmaktadır. Monero ve Zcash'den farklı olarak, otorite ile paylaşılabilecek anahtarlar sayesinde, gizli işlemlerin denetlenebilmesi mümkün olacaktır. Cardano platformunda da Fabric gizli işlemlerine benzer destek bulunmaktadır. zk-SNARK ispatlarını eklemek üzere de çalışmalar sürmektedir.

4.3 Kanun ve Düzenlemeler Bağlamında Blokzincir Platformlarının Mahremiyet Özellikleri

Aşağıdaki alt bölümler, [BG18], [BtGDPR19], [BCD+18], [Har19] ve [KVK18] kaynaklarından özetlenerek yazılmıştır.

Her gün milyonlarca insan, kişisel verilerini ve bilgilerini çeşitli kurumlarla paylaşırlar. Bu bilgi paylaşımında, kişiler genel olarak verilerinin başka kimlerle paylaşıldığını, verileri üzerinde kimlerce ve başka hangi işlemler yapıldığını bilmezler. Son zamanlarda yaşanan olaylar, bireylerin, kendi kişisel verilerinin ticari amaçla kullanılması ve sızdırılması tehditleri hakkındaki farkındalığını arttırmıştır. Kişisel veriler konusunda Dünya'da ve ülkemizde çeşitli kanuni düzenlemeler bulunmaktadır. Bu bölümdeki değerlendirmeler, 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu(KVKK)[KVK18] ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR") açısından yapılacaktır.

Blokzincir ve Kişisel veri koruma kanunları, çok farklı amaçlarla başlamış olsa da (birisi merkezi otoriteden bağımsız bir para birimi oluşturma diğeri ise veri mahremiyeti yasalarını uygulamaya koyma) iki girişim de "kullanıcının güvenli ve kendi sorumluluğundaki veriler" prensibinde örtüşürler[BG18].

Düzenlemelerde Veri Sahibi, kişisel verisi işlenen gerçek kişidir. Veri Sorumlusu (Controller) ise KVKK'da, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır. Veri İşleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır.

Bununla birlikte, yukarıdaki düzenlemeler, kişisel veri sahiplerinin yasalar çerçevesinde kendilerine tanınan haklarına ilişkin başvurularını yöneltebilecekleri ve kişisel veri işleme faaliyetlerini düzenlemelerle uyumlu şekilde gerçekleştirmekle yükümlü gerçek veya tüzel kişi veri sorumlularının mevcudiyeti varsayımına göre hazırlanmıştır. Dolayısıyla, söz konusu yasal düzenlemeler, merkeziyetçi bir yapı üzerine inşa edilmiştir. Oysa blokzincir teknolojisi merkezi olmayan mimariye sahiptir ve veri sorumlusu gibi ara aktörler ortadan kaldırılmaktadır. Bu nedenle blokzincir üzerinde kişisel mahremiyet sağlanması konusu bir takım belirsizlikleri de tartışma konusu yapar.

4.3.1 Genel Veri Koruma Düzenlemesi (GDPR) ve Kişisel Verilerin Korunması Kanunu (KVKK)

GDPR(General Data Protection Regulation), AB vatandaşlarına, diğer kişi ve kuruluşlarla paylaştıkları kişisel bilgileri üzerinde daha güçlü bir kontrol sağlama hedefiyle mahremiyet ve güvenliğe güncel bir yaklaşım getirmek ve tüm üye devletlere ortak bir yasal çerçeve olarak uygulamak üzere tasarlanmıştır[Har19]. GDPR kapsamına yalnızca AB üye devletleri değil, fiziksel olarak Avrupa Birliği'nde bulunmayan şirketler bile, eğer AB'de yaşayan bireylere ücretli veya ücretsiz mal ve hizmet sunuyorsa veya AB'de yaşayan bireylerin davranışlarını izliyorsa girmektedir[BG18].

GDPR, kişisel verileri yöneten veya işleyen tüm varlıkların, AB vatandaşlarının kişisel verilerini korumak için organizasyonel süreçlere sahip olmasını ve uygun teknik önlemleri almasını zorunlu kılar [Har19].

GDPR, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesi ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesi faaliyetlerinde uygulanmaktadır. Veri koruma ilkeleri[BCD+18], tanımlanmış veya tanımlanabilir bir gerçek kişi ile ilgili herhangi bir bilgi için uygulanır. Anonim haldeki veriye (tanımlanmış veya tanımlanabilir bir gerçek kişiyi adreslemeyecek bilgilere veya anonim hale getirildiği için artık ilgili veri sahibinin tanımlanamaz hale geldiği kişisel verilere) uygulanmaz. Ama ek bilgi sayesinde gerçek bir kişi ile ilişkilendirilebilecek, takma adlandırma işleminden geçmiş kişisel bilgiler de kapsama girer. Bir gerçek kişinin tanımlanabilir olup olmadığını belirlemek için, bir gerçek kişiyi doğrudan veya dolaylı olarak belirlemede kullanılması muhtemel tüm yöntemlerin, veri işleme anındaki mevcut teknoloji ve teknolojik gelişmelerin, tanımlama için gereken maliyet ve süre gibi tüm objektif faktörlerin dikkate alınması gerekir.

Mahremiyet kuralları kişinin doğrulanmasından ziyade tanımlanmasıyla ilişkilidir. Bu nedenle, kuruluşlar, hem resim hem de metin verilere uygulanabilecek etkili, kimliksizleştirme (de-identification) teknikleri kullanmalıdır [BCD+18].

KVKK'daki kişisel verilerin işlenmesine ilişkin usul ve esaslar, Avrupa Konseyi'nin 108 No'lu Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Sözleşmesi ve 95/46/EC nolu Avrupa Birliği Veri Koruma Direktifine paralel olarak düzenlenir. KVK Kanunu'nu, kişisel verileri işlenen gerçek kişiler ve bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmaktadır.

Kanunda, verinin olması gereken durumu belirten temel ilkeler: [KVK18]:

- Yasal ve adil olarak işlenir.
- Doğru ve gerektiğinde güncel tutulur.
- Tanımlanmış, açık ve meşru amaçlar için işlenir.
- İşlendikleri amaçla orantılı, sınırlı ve uygun olmalıdır.
- İlgili mevzuat tarafından belirlenen veya işleme amacı için gerekli görülen süre boyunca alıkonulur.

Tüm kişisel veri işleme bu ilkelere uygun olarak yapılmalıdır. [KVK18].

4.3.2 Blokzincir ve Kişisel Veri

KVKK'ya göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Kişisel veri, ilgili kişinin kimliğini doğrudan gösterebileceği gibi, herhangi bir kayıtla ilişkilendirilmesi ile kişinin belirlenmesini sağlayan tüm bilgileri kapsar. GDPR'da ise kişisel veri tanımı, KVKK'ya göre daha kapsamlı düzenlenmiştir. Örneğin, "takma ad" (pseudonymo) kavramına yer verilmiştir. Rumuzlaştırma da denilebilecek bu kavram, (ilave bilgilerin teknik ve idari önlemler alınarak belirli veya belirlenebilir bir ilgili kişi ile ilişkilen-

dirilemeyecek şekilde ayrı olarak muhafaza edilmesi şartı ile) kişisel verilerin ilave bilgiler kullanılmaksızın belirli bir ilgili kişi ile ilişkilendirilemeyecek şekilde işlenmesi olarak tanımlanmaktadır [BH19].

Blokzincir ağında depolanan veriler; işlemler ve bazı blokzincirlere özel olmak üzere kullanıcılara ve kurumlara ilişkin hesap detayları olarak sıralanabilir. Blokzincirlerdeki işlemlere ait adres ve diğer içerik verilerinin kişisel veri olup olmadığı konusunda çeşitli değerlendirmeler yapılmaktadır [BtGDPR19].

Ayrıca, kişisel verilerin işlenmesinden sorumlu tutulan veri sorumlusu, blokzincir teknolojisinde tartışmalı bir roldür. Blokzincir teknolojisinde veri sorumlusunu tespit edebilmek çoğu zaman kolay olmamakla birlikte, blokzincir ağının türüne göre değerlendirme yapılması gerekmektedir. Ağın kurulum ve işletmesinden sorumlu olanların belli olduğu kapalı blokzincir ağlarında bu tespit daha kolay yapılmaktadır. Açık ve izin gerektirmeyen blokzincir ağlarında ise veri sorumlusu veya ortak veri sorumlularının kimler olduğuna ilişkin tespitin yapılması oldukça zor ve tartışmalıdır. Servis sağlayıcılar, kullanıcılara ait kripto paraların depolanması ve transferi gibi işlemlerin yürütülmesinde kontrol sahibidir. Dolayısıyla borsalar ve cüzdanlar, kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirlemeleri nedeniyle işlemlerin yürütülmesi veya kullanıcıya ait kripto para birimlerinin depolanması bakımından GDPR ve KVK Kanunu kapsamında hizmet alan kullanıcılar karşısında veri sorumlusu olarak kabul edilebileceklerdir[BH19].

Açık anahtarlar, işlem verileri ve tersine çevrilebilir şekilde şifrelenmiş veriler çoğu zaman kişisel veri olarak kabul edilmekte ve blokzincir ağında kullanılmaları halinde KVKK ve GDPR hükümleri ile uyumlu şekilde işlenmeleri gerekmektedir. Bu yargının detayları aşağıdaki alt bölümlerde verilmiştir.

Açık Anahtarlar

Blokzincirdeki her kullanıcının, başkalarıyla paylaşmasında sakınca bulunmayan, hesap numarası gibi düşünebileceğimiz bir açık anahtarı (kullanıcıyı temsil eden bir dizi harf ve rakam) ve başkalarıyla asla paylaşmaması gereken, kişiye özel bir şifre gibi düşünebileceğimiz özel bir anahtarı vardır. Bu iki anahtarın arasında matematiksel ilişki vardır. Özel anahtar, açık anahtar aracılığıyla şifrelenmiş verilerin şifresini çözebilir. Açık anahtarlar böylece ek tanımlayıcılarla bağlantılandırılmadıkça bireyin kimliğini gizler. Blokzincir perspektifinden bakıldığında, açık anahtarların GDPR'da belirtilen tanımlayıcı/belirleyici veri türü olarak işlev gördüğü söylenebilir. Açık Anahtarlar adres ve isim bilgilerini bünyelerinde barındırdıkları için anonim olarak kabul edilmeyen; takma adlı veri olarak tanımlanan kişisel verilerdir. Sistemin doğası gereği mecburen ağda depolanırlar.

Açık anahtarlar belirli bir gerçek kişinin tanımlanmasını sağlayabilir. Açık anahtarlar ve işlemler arası ilişki grafının analizi sayesinde, gerçek kişiler belirlenebilir, zaten bilinmekte olan adreslerle girilmiş alış verişleri ortaya çıkarılabilir. Bitcoin blokzincirindeki şifreli veriler kullanılarak, bir kullanıcının ve işlemlerin kullanıcılara bağıntısının ortaya çıkarılabildiği kanıtlanmıştır. Bu nedenle tanımlanmış veya tespit edilebilir bir gerçek kişi ile doğrudan veya dolaylı olarak ilgili olan açık anahtarlar, AB kapsamında kişisel veri olarak değerlendirilmektedir.

İşlem Verisi

İşlem verisi (Transactional data), blokzincirlerde kullanılabilen, açık anahtarlar dışındaki diğer verileri temsil eden bir terimdir. Bu verilerin GDPR'ın kişisel veri tanımına girip girmediğini belirlemek için her durum özelinde analiz yapılması gerekir. Blokzincirde bir verinin depolanması üç alternatif şekilde gerçekleşmektedir: Bunlar düz metin, şifreli metin veya kritografik özet olarak sıralanabilir.

İşlem verileri, şifrelenmiş bile olsa doğru anahtarlarla tekrardan ulaşılabilir olduğu için anonim veri olarak kabul edilmemektedir. İlgili kişi dolaylı olarak tanımlanabileceği için şifreleme, GDPR'a göre bir takma ad kullanımı olarak kabul edilmektedir. Şifrelenerek ağda depolanan veriler, takma adlı veriler olarak değerlendirilmekte ve ilgili kişilerin verileri, belirlenebilir olduğu için de kişisel veri olarak kabul edilmektedir.

KVKK kapsamında takma adlı veri kavramı bulunmadığı için bu konu Türk hukukuna göre belirsizlikler içerir.

Verilerin kriptografik özeti de GDPR'a göre kişisel veri olarak nitelendirilmektedir [Fin18]. Veriyi ilgili kişi ile ilişkilendirmenin hâlâ mümkün olması nedeniyle özet almanın, bir anonimleştirme değil; takma adlandırma tekniği olduğu görüşü hakimdir.

Kısaca özetlemek gerekirse; açık şekilde saklanan veri GDPR ve KVKK'ya göre kişisel veri olarak değerlendirilir. Şifreli ve kriptografik özetli şekilde bulunan veriler takma ad olarak kabul edilmekte ve GDPR'a göre kişisel veri olarak değerlendirilmektedir; KVKK'da takma ad kavramı bulunmadığı için durumları belirsizdir.

Aşağıdaki bölümler [BG18] 'den özetlenmiştir.

4.3.3 Veri Sahibinin Hakları

GDPR, bireylere kişisel verileri (tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilgili herhangi bir bilgi) üzerinde daha iyi bir kontrol sağlamalarını amaçlar. Kişisel verilere daha kolay erişim, kendi verilerini güncelleme/düzeltme hakkı, silme hakkı ("Unutulma hakkı"), veri taşınabilirliği hakkı, rıza hakkı ve hak ve özgürlüklerinde potansiyel olarak yüksek bir etkiye sahip olması durumunda kişisel veri ihlallerinden haberdar edilme hakkı, işleme faaliyetini kısıtlama hakkı, itiraz hakkı, kişisel verilerin paylaşıldığı üçüncü taraflara bildirim yükümlülüğü, otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı gibi haklar güvence altına alınır.

KVKK'ya göre herkes, veri sorumlusuna başvurarak, kişisel verilerinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme, işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, kişisel verilerinin aktarıldığı üçüncü kişileri öğrenme, kişisel verilerinin eksik veya yanlış işlenmiş ve paylaşılmış olması halinde bunların düzeltilmesini isteme hakkına sahiptir. Ayrıca kişi, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin, aktarıldığı üçüncü kişiler de dahil olmak üzere silinmesini isteme, veri işleme sonucunda aleyhine bir sonucun ortaya çıkması durumunda buna itiraz etme, kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme, verilerin işlenmesinin kısıtlanmasını talep etme, işleme faaliyetine itiraz etme, bir denetim makamına şikayette bulunma hakları da mevcuttur.

Kişisel verilerin aynı amaç için birden fazla yerde bulunması, bu hakların uygulanmasını zorlaştırır.

GDPR ve KVKK'ya göre, ilgili kişinin açık rızası olmaksızın kişisel veriler aktarılamaz. Özellikle, Açık ve İzin Gerektirmeyen Blokzincir Ağlarında verilerin aktarılması sorun oluşturabilir. Bir blokzincirdeki işlem kayıtları; tüm madencilere gönderilen işlem (kişisel veri içerebilir) onay talebi ve tüm katılımcılar için zincire yeni eklenen blokların güncel halini içermektedir. Madenciler veya katılımcılar, herhangi bir ülkeden olabilmektedir. Bu nedenle, dış ülkelere aktarımlar için KVKK ve GDPR uyarınca belirtilen yükümlülüklere uyulması sorunludur. Ülke dışına veya uluslararası kuruluşa veri aktarımı için uygun güvenlik önlemlerinin alınması, Kapalı ve İzin Gerektiren Blokzincir ağında pratik olarak mümkün iken, veri sorumlusunun madencilerin konumları bakımında gerçek bir kontrole sahip olmadığı Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda pratik olarak mümkün değildir.

Blokzincir temelli çözümler, bu kuralları yerine getirirken basitleştirmeye de yardımcı olur.

Müşterini Tanı (KYC) veri paylaşımı gerçeklenmesinde blokzincir, şirketlere, veri taşınabilirliği gereksinimlerini karşılamaları (bireylerin kişisel hizmetlerini elde etme ve kendi amaçları için farklı servislerde yeniden kullanmalarına olanak sağlamak) için yardımcı olur.

Blokzincir "sadece ekleme" yapılan bir sistemdir ve değişmezlik, mimarinin istenen anahtar özelliğidir. Bu nedenle GDPR'ın silinme hakkı ile uyum sağlamak zor olabilir. Silinme hakkı ile uyum için kişisel veri blokckchain dışında gizli olarak tutulmalı, sadece kanıtları (özet değeri) zincir üzerinde tutulmalıdır. Böylece, kişisel veri gerektiğinde fazla etkisi olmadan silinebilir.

Blokzincirin değişmezlik karakteristiği, rıza yönetiminin gerçeklenmesinde ve kurumların, tanımlanmış sürecine uygunluğu gösterme gibi konularda uygulamaya yardımcı bir araç olarak kullanılabilir.

4.3.4 Veri İşleme Güvenliği

GDPR'a göre, kişisel verilerin işlenmesi ancak aşağıdaki şartlardan en az biri geçerli olduğunda hukuka uygundur:

- ilgili kişinin bir veya birden fazla sayıda belirli amaç için kişisel verilerinin işlenmesine onay vermesi,
- ilgili kişinin taraf olduğu bir sözleşmenin uygulanması veya sözleşme yapılmadan önce ilgili kişinin talebi üzerine adımlar atılması için veri işleme faaliyetinin gerekli olması,
- veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyum sağlanması amacıyla veri işleme faaliyetinin gerekli olması,
- ilgili kişinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile veri işleme faaliyetinin gerekli olması,
- kamu yararı kapsamındaki bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin uygulanması hususunda veri işleme faaliyetinin gerekli olması ve özellikle ilgili kişi bir çocuk ise kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hak ve özgürlüklerinin, bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlerine göre daha ağır olması halinde veri işleme faaliyetinin gerekli olması.

Bir istisnası ise kamu kurumları tarafından görevlerinin yerine getirilmesi hususunda gerçekleştirilen veri işleme faaliyetleridir [BH19].

GDPR'a göre, veri sorumluları ve işleyiciler, *"riske uygun bir güvenlik düzeyi sağlamak için uygun teknik ve organizasyonel önlemleri"* gerçeklemek zorundadır. GDPR'da kişisel verilerin güvenliğini gerçeklemek için; takma adlandırma ve şifreleme, sistemlerin ve hizmetlerin gizliliği, bütünlüğü, kullanılabilirliği ve esnekliği gibi bir dizi örnek ve kılavuz verilmiştir. Uygun güvenlik seviyesini belirlerken, kazara veya yasa dışı bir şekilde yok etme, kayıp, değiştirme, yetkisiz ifşa veya erişim de göz önünde bulundurulmalıdır.

GDPR, blokzincir gibi yeniliklere uyumluluk sağlayacak şekilde, teknolojiden bağımsız ve esnek olarak tasarlanmıştır. Blokzincirin doğasındaki özelliklerin birçoğu, Gizlilik, Bütünlük ve Kullanılabilirlik (Confidentiality, Integrity, and Availability) açısından veri işleme güvenliğine doğal olarak katkı sağlar. Blokzincirde kriptografi, yetkisiz kullanımı önlemek için erişim kontrolleriyle birlikte işlem(transaction) gizliliğini desteklemek amacıyla kullanılır. Ayrıca, veriler merkezi bir yerde açık olarak saklanmadığından, saldırganları toplu bir veri kaynağına erişme amacıyla (central honeypot) cezbetme riski de azaltılmış olur. Blokzincir hesap verebilirlik ve şeffaflık gibi önemli özelliklerin yanında, arıza/darboğaz riskini de ortadan kaldırarak verilerin erişilebilirliğini artırır. Bununla birlikte, tasarım gereği kayıtların değişmez olmasına rağmen, özel ve izinli (private permissioned) blokzincir ağlarında bile güvenlik riskleri bulunmaktadır. Örneğin, ağa bağlı zararlı bir uygulama kayıt defterine doğrudan disk üzerinden veya ağ üzerinden yetkisiz erişim potansiyeline sahiptir. Bu nedenle, kuruluşların ağ erişimini izlemesi ve yetkisiz erişimi engellemesi gerekir. Şifreleme anahtarları, tahrif edilerek veya silinerek veriler erişilmez duruma getirilebilir. Saldırganların geçerli kullanıcıları taklit etmesini önlemek için blokzincir katılımcılarının kimliği doğrulanmalıdır. Bu ise ancak izinli blokzincir yapılarında mümkündür.

4.3.5 Yasallık ve Rıza

GDPR ve KVKK'ya göre, kişisel verilerin işlenmesine, ancak bu işlem için yasal bir dayanak varsa izin verilir. Veri sahibinin bu tür veri işlemeye rızası anahtar roldedir. Verilerini işlemeden önce veri sahiplerinin rızasının alındığından emin olmak, geçmişte olduğundan çok daha zor hale gelecektir.

Rızanın geçerli sayılabilmesi için, baskı altında olmadan verilmeli, spesifik konuda olmalı, anlamı net olmalı ve duyurulmalıdır. Özel kişisel veri kategorilerinin ele alınmasının daha muhtemel olduğu sağlık hizmetleri gibi durumlarda açık, anlaşılır olmalıdır. Rızanın veri sahibi tarafından herhangi bir zamanda geri çekilebilmesi, konuyu daha da karmaşık bir hale getirmektedir.

4.3.6 Kanunlara Uyum, Hesap Verebilirlik

Bir veri sorumlusunun GDPR yükümlülüklerine uyum gösterebilmesi veya en azından uyum için nasıl ilerlediğini belgelemesi gerekir. Uyum sağlama yolunda atılan adımlar arasında, kurum çapında uygulanan veri koruma önlemlerini ve denetimlerini belgeleyen bir kayıt tutma sisteminin gerçeklemesi yer alabilir. Geleneksel kayıt tutma yönteminde depolanan bilgiler, doğrulanma sorunları ve eksik detaylar nedeniyle güvenilmez ve anlaşılmaktan uzak olabilmektedir. Blokzincir kullanımı, bir kurumun, verilerdeki hesap verebilirlik ve anlaşılabilirlik düzeyini yükseltmesine

ve belirli düzenlemelere uyumunu kanıtlamasına yardımcı olur. Çünkü blokzincir sadece verinin mevcut durumunu değil aynı zamanda kayıt defterinde yapılan tüm değişiklikleri de tutar.

4.3.7 İyileştirici Önlemler

Blokzincirde kişisel verilerin işlenmesi konusu ile ilgili olarak mahremiyeti artırmaya yönelik olarak kullanılabilecek yöntemler hakkında değerlendirmeler bu bölümde özetlenmiştir.

Şifreleme

Verilerin şifrelenmesi durumunda, ancak şifre çözme anahtarına sahip olan kişi, şifrelenmiş veri kümesinde kişisel veriler varsa şifre çözme yoluyla her bir veri sahibini tespit edebilir. Sonuç olarak, şifreli veriler (en azından anahtarın sahibi için) kişisel veriler olarak kalır. Servis sağlayıcının anahtara erişemediği durumlarda yeterince iyi şifrelenmiş verilerin, yeterince anonimleştirilmiş verilerde olduğu gibi, kişisel veri olarak değerlendirilmemesi gerektiği düşünülebilir. Düzenleyici, ek bilgilerle anahtara sahip olanlarla olmayanlar arasında bir ayrım yaparak kişisel verilerin korunma derecesini açıklığa kavuşturmalıdır.

Özet Fonksiyonları

Özet fonksiyonları genellikle bir ad veya müşteri numarası gibi kişisel tanımlayıcıları, tersine döndürülmesi zor bir takma adla değiştirmek için kullanılır. Ancak, bu, özet verilerini anonim veri yapmaz. Özet fonksiyonunu (çıktıdan girdiyi bulmak için) geriye doğru çalıştırmak imkansız olsa da özeti alınmış verinin ait olduğu bir kümeyi bilen herhangi biri, bu kümedekilerin özetlerini alarak, özeti bilinen verinin aslını bulabilir. Özetlenmiş verilerin GDPR'ın amaçlarına uyan kişisel veri olup olmadığı, devam eden bir tartışma konusu olsa da güçlü gizlilik garantileri olan özet fonksiyonları da vardır.

Zincir Dışı (off-chain) Veri Saklama

Kanunlarla uyum için, kişisel verilerin blokzincir ağının dışında gizli ve özel bir ağda yani "zincir dışı" (off-chain) saklanması/depolanması ve blokzincir üzerinde yalnızca bu zincir dışı tutulan verinin ispatının (örneğin şifrelemeye ilişkin kriptografik özetlenmiş veri) yer alması alternatifi bulunmaktadır.

Zaten bazı blokzincir kullanım senaryolarında, işlem verilerinin tamamının blockzincirinin üzerinde saklanması gerekli olmayabilir. Aksine, bu veriler blokzincir dışı bir veritabanında saklanabilir ve bir özet işaretçi aracılığıyla kayıt defterine bağlanabilir. Bu yöntem, veri koruma açısından birçok avantaj sağlayabilir. Zincir dışı depolama, GDPR ile uyumlu olan uygun veritabanlarında depolanan kişisel verilerin düzeltilmesine (rectification) ve silinmesi haklarının gerçeklenmesine imkan sağlar.

Ancak bu yöntemi kullanırken, "meta verinin" kişisel bilgilerin doğrudan zincirde depolanmadığı durumlarda bile kişisel bilgileri açığa çıkarılabileceğinden, dikkatli olunmalıdır. Öte yandan, zincir dışı depolama yöntemlerine başvurulması, blokzincire olan güveni azaltabileceği gibi güvenilir bir üçüncü tarafın katılımını da gerektirebilecektir. Bu durum, blokzincir teknolojisinin merkeziyetsiz ve aracıları ortadan kaldıran özelliklerini zedeler.

Sıfır Bilgi Kanıtları

Sıfır bilgi ispatları (Zero knowledge proofs), verinin kendisine erişim sağlanmadan, veri hakkında Doğru/Yanlış cevaplar sağlamakta kullanılabilirler. Gerçekten de bir Avrupa Parlamentosu raporu, zk-SNARK'ları tasarımda veri korumasına uyma gereksinimini sağlamanın bir yöntemi olarak görmektedir [BtGDPR19].

Homomorfik Şifreleme

Homomorfik şifreleme, gelişmiş bir şifreleme yöntemidir. Verilerin şifrelenmiş hallerinin hesaplamalarda kullanılmasına izin verir. Öyle ki, verinin şifrelenmiş hali ile yapılan işlemler, verinin şifrelenmemiş hali ile yapılan işlemlerle aynı sonucun şifrelenmiş halini verir. Oysa, şifreleme konusundaki düzenleyici duruşu göz önüne alındığında, bunun GDPR'ın anonimleştirme eşiğini geçip geçmeyeceği şüpheli olsa da homomorfik şifreleme, bir anonimleştirme aracı olarak kullanılabilir.

Durum Kanalları ve Halka İmzalar

Halen kullanılmakta olan diğer bir seçenek ise anlaşmazlık durumunda yalnızca ilgili taraflarla bilgi paylaşan, iki taraflı sözleşmeler için kullanılan durum kanallarıdır (state channel). Diğer yandan halka imzaları (ring signature), yalnızca bir tanesi işlemi başlatmış olsa bile, birden fazla özel anahtara o işlemi bağlayarak diğer işlemler içinde gizler. Halka imza, imzalayanın, hangisi olduğunu açıklamadan, belirli bir açık anahtar kümesinden birine karşılık gelen özel anahtara sahip olduğunu kanıtlar. Yukarıdaki çözümlerden herhangi birinin açık anahtarları anonimleştirmede işe yarayıp yaramadığı açık bir konu olsa da Durum Kanalları, işlem verilerinin bir kısmını, ana blokzincirindeki aktörlerin erişiminden koruduğu için kişisel veri kanunlarına uyumluluğu artıran, faydalı bir yöntemdir.

Yan Zincirler

Yan zincir (Sidechain) kavramı, mahremiyet artırma açısından değerlendirilebilecek diğer bir alternatiftir. Ana blokzincir aktörlerinin erişiminden saklanmak istenen bazı işlemler, bu veriler yan zincire transfer edildikten sonra gerçekleştirilirse, ana zincirin aktörlerinden daha kısıtlı bir sayıdaki aktörün erişimine açık olur.

Chameleon Özetleri ve Düzenlenebilir Blokzincirler

Düzenlemelere uyum gereksinimlerini sağlamak gibi hedeflerle, Chameleon özet fonksiyonları kullanılarak, belirli verileri düzenleme, silme veya yeniden yazmaya izin veren 'düzenlenebilir' blokzincirler tasarlanmıştır. Ayrıca, çeşitli yönetişim modelleri kapsamında (oylama vb. usüllerle) geriye doğru kayıtların değiştirilebildiği blokzincir platformları da kullanılmaya başlanmıştır. Bu çözümler, özel tasarımlarına bağlı olarak, kanunlarla uyumluluğu kolaylaştırabilirler. Bununla birlikte, bir blokzinciri düzenlenebilir yapmak, diğer (dağıtılmış) veritabanları yerine kullanılıyor olmasının önemli dayanağı yok etmiş olur.

Adres Gizleme

Tek kullanımlık anahtarlara dayanan ve bir defalık bir işlem gerçekleştiren gizli bir adresin kullanılması da kullanım senaryosu izin veriyorsa tercih edilebilecek bir yöntemdir. Örneğin; Monero kriptopara blokzinciri, yeni bir özel adres ve gizli anahtar oluşturarak işlemin alıcısını gizler. İşlemler için tek seferlik hesapların kullanılması, her işlemin bir veya daha fazla hesabı tamamen boşaltması ve bir veya daha fazla yeni hesap oluşturması gerekliliğini ortaya çıkarmıştır (merge avoidance).

Başka bir örnek olarak; Zcash, kullanıcılarına daha fazla gizlilik sağlamak için, zk-SNARK ismi verilen protokol sayesinde kullanıcılarının, yaptıkları bütün işlemlerde kimlikleri gizleyebilmesine imkan verir. Bitcoin'den farklı olarak ise tüm işlemlerin değerleri blokzincir içerisinde saklanabilmektedir ve yalnızca görmesi gereken kişiler görebilmektedir. Bitcoin ve Ethereum'da kullanıcılar gizli kalırken, bütün işlemler görülebilmekteydi ancak Zcash ile hem kişiler hem de işlemler gizli kalabilmektedir.

Verilere Gürültü Ekleme

Verilere gürültü(noise) eklenmesinin GDPR açısından kabul edilebilir bir anonimleştirme tekniği olabileceği düşünülmektedir. İlgili çözüm önerisi, birkaç işlem kaydını gruplandırmayı ve dışarıdan bakıldığında işlemlerin gönderici ve alıcı kimliklerinin belirlenmesini imkansız kılar. Bu modele benzer algoritmalar, Bitcoin ve Ethereum sistemlerinde tanımlanmıştır.

4.3.8 Sonuç

Blokzincir son yıllarda olgunlaşmış ve tedarik zinciri, kaynak, uyumluluk, gıda güvenliği ve dijital kimlik gibi çeşitli alanlarda değer üretmeye başlamıştır. Blokzincir, değer zincirinde yer alan katılımcılar için mahremiyet ve gizliliği korurken aynı zamanda hesap verebilirlik ve şeffaflık sağlar. Ama blokzincir teknolojisinin henüz kişisel veri koruma kanunları ile tam uyumlu olduğu söylenemez. Bununla birlikte, söz konusu uyumsuzlukların giderilmesi için her geçen gün yeni öneriler ortaya çıkmaktadır. Her şeye rağmen blokzincir teknolojisinin, kişisel verilerin korunması kanunlarındaki yükümlülüklerin daha sağlıklı ve kolay şekilde yerine getirilmesine hizmet edecek pek çok özelliği olabileceği de dikkate alınmalıdır. Blokzincir, tek başına bir çözüm değildir, ancak kişisel verilerin kullanımını kontrol etmeye yardımcı olan bir mekanizma olarak kabul edilebilir.

Ayrıca, kişisel verilerin korunması, teknolojiden çok teknolojinin nasıl kullanıldığıyla ilişkilidir. Dolayısıyla, tartışmaların sürdüğü ve blokzincir platformlarının bu tartışmalar ışığında olgunlaştığı bu geçiş döneminde, eğer blokzincir teknolojisinin kullanılması zorunlu ise, kullanılacak alana uygun olan blokzincir türü seçilmeli, oluşturulacak kullanım senaryoları ise mevcut düzenlemelerle azami uyumlu olacak şekilde tasarlanmalıdır.

Kapalı ve izin gerektiren blokzincir ağlarının, açık ve izin gerektirmeyen blokzincir ağlarına göre kişisel veri koruma kanunlarına daha uyumlu olabileceği açıktır. Ancak, düzeltme ve silme haklarına ilişkin problemlerin, kullanılan blokzincir, kapalı ve izin gerektiren türde olsa dahi çözülemeyebileceği göz ardı edilmemelidir.

BLOKZİNCİR UÇ TEKNOLOJİLERİNİN DEĞERLENDİRİLMESİ

Herkese açık bir ağda yüksek derecede ademi merkeziliğe izin vermek için, "Emek İspatı" (Proof of Work) tabanlı blokzincirlerdeki blokların boyutları sınırlıdır ve bu bir miktar gecikmeye sebep olmaktadır. Bu tasarım, hesaplama gücü sınırlı olan ağ üyelerinin de sistem bünyesinde yer almasına izin verir. Çünkü daha büyük blokların işlenmesi daha zordur ve ağ gecikmeleri, bu zayıf üyelerin üretilen blokları almasını engelleyebilir. Bu da, bir bloka dahil edilebilecek işlemlere ilişkin bir limitin yanı sıra, belirli bir zaman diliminde kaç bloğun doğrulanabileceğine ilişkin bir sınır da getirmektedir. "Emek İspatı" tabanlı dağıtık mutabakat mekanizmalarının en önemli zorluklarından biri, ağın güvenli ancak yavaş kalmasıdır. Bu, ademi merkezilik, güvenlik ve ölçeklenebilirlik gibi blokzincir yapılarının ana özellikleri arasındaki karşılıklı ödünleşimlerden kaynaklanmaktadır. Özellikle, ölçeklenebilirlik, token kullanım senaryolarının uygulanabilirliği açısından büyük bir sorundur.

Blokzincir teknolojileri, baskın nitelikleri arasındaki "ölçeklenebilirlik üçlü çelişkisi" ile karşı karşıyadır: (I) ademi merkezilik (II) güvenlik ve (III) ölçeklenebilirlik. Güvenlik, birbirlerine güvenmeyen eşlerin dağıtık bir ağda ihtiyaç duyduğu en önemli unsurdur. Dağıtık ağların belirgin özelliği ise ademi merkeziliktir. Ölçeklenebilirlik, bir sistemin saniyede işleyebildiği işlem sayısı ile ilişkilidir. Ölçeklenebilirlik, blokzincir gelişiminin ilk yıllarında kavram ispatı arayışının gölgesindeki temel bir özellik olarak kalmıştır.

Ölçeklenebilirliği, ademi merkeziyetçiliği ve ağ güvenliğini dengelemeyi, blokzincir teknolojilerinin ana odak noktası olarak tanımlamak mümkündür. Teknoloji geliştikçe bu dengenin zamanla oturacağı değerlendirilmektedir. Bu durum, bant genişliğinin hala az olduğu ve iletişim hatlarının yavaş olduğu İnternet'in ilk günleriyle karşılaştırılabilir. Bilgisayarları İnternet'e bağlamak için telefon kabloları kullanılırdı. 56k modemler 28k modem için büyük bir yenilikti ve sayfalardaki resimlerin piksel piksel yüklenmesi beklenirdi. Ancak zamanla bu sorun çözüldü ve WWW'nin bugünkü haline dönüşmesini sağladı.

Blokzincir bağlamında, işlemlerin daha hızlı ve daha ucuz hale getirilmesi ve bu yeni teknolojinin kitlesel olarak benimsenmesinin önünü açacak birçok çözüm önerilmiştir. Bunun protokol düzeyinde çözülüp çözülmeyeceği ve çoğu zaman ademi merkezilikten taviz vermenin gerekip gerekmediği konusunda çok fazla tartışma da bulunmaktadır. Daha fazla işlem hacmine izin vermek için, belirli katılımcılara daha fazla güç verilmesi ve böylece merkezileştirmenin seviyesinin artırılması gerekecektir. Ölçeklenebilirlik sorununu gidermeye çalışan ana protokol düzeyindeki alternatif mutabakat mekanizmaları, güven garantilemek için bir tür izin katmanı oluşturmaktır. Kayıt defterinin daha küçük parçalara bölünmesine veya alternatif kriptografik algoritmalar, protokol seviyesindeki ölçeklenebilirlik sorununu çözmenin diğer yollarıdır. Alternatif olarak, ölçeklenebilirlik çözümlerini yanzincirler veya durum kanalları gibi ikinci bir katmana taşımak için çeşitli çabalar sarf edilmiştir. Bu durumlarda, kullanıcı etkileşimi blokzincirden ikinci bir katmana taşınırken, katılımcılar arasında risksiz P2P işlemlerine izin verilmesi hedeflenmektedir.

Durum Kanalı (State Channel) ve Yanzincir (Sidechain) kavramları blokzincir topluluklarında sıklıkla birbirlerinin yerine kullanılan ve bu nedenle karıştırılabilen iki terimdir. Bu bölümün amacı iki kavramı açıkça tanımlamak ve hangi sorunları çözmeye çalıştıklarını tartışmaktır.

5.1 Yanzincirler

Yanzincirler (ing. Sidechains), token'ların ve diğer dijital varlıkların ana blokzincirden ayrı bir blokzincirde güvenli bir şekilde kullanılmasını ve daha sonra gerekirse orijinal blokzincirie geri taşınmasını sağlayan yeni mekanizmalardır. Yanzincir işlevselliği, mevcut blokzincir yeteneklerini geliştirmek için önemli bir potansiyele sahiptir. Bir yanzincir, iki yönlü mandal (2WP) kullanılarak ana blokzincire tutturulmuş ayrı bir blokzincir olarak tanımlanabilir. İki yönlü mandal, ana blokzincir ile yanzincir arasında önceden belirlenmiş bir oranda varlıkların değişebilirliğini sağlar. Orijinal blokzincir genellikle "ana zincir" olarak adlandırılır ve tüm diğer blokzincirlere "yanzincirler" denir. Bunun yanı sıra Ardor blokzincir platformunda olduğu gibi yanzincir yerine "yavru zincir" olarak adlandırıldığını görmek mümkündür.

Ana zincirdeki bir kullanıcı, ilk önce varlığını bir çıkış adresine göndermelidir. Varlık burada kilitlenir. Böylece kullanıcı bunları başka bir yerde harcayamaz. İşlem tamamlandıktan sonra, zincirler arasında bir onay iletilir ve daha fazla güvenlik için bekleme süresinin dolması beklenir. Bekleme süresinin ardından, yanzincirde eşdeğer sayıda varlık serbest bırakılarak, kullanıcının bunlara erişmesi ve orada harcaması sağlanır. Bir yanzincirden anazincire geri dönerken bu işlemler ters yönde işletilir.

Yanzincir kavramı ilk olarak Adam Back tarafından 2014 yılında yayınlanan "*Enabling Blockchain Innovations With Pegged Side Chains*" adlı makalede önerilmiştir. Bu makale, iki yönlü mandal hakkında genel fikri ortaya koymuş ve sabitlenmiş zincirler arasındaki etkileşimleri uygulamak için senkron ve asenkron olmak üzere iki işlemsel mod tanımlamıştır. Senkron mod, ana ve yanzincirlerin birbirinin farkında olmasını ve doğrudan transfer işlemlerini doğrulayabilmesini sağlarken; asenkron mod, yanzincir üzerindeki transferleri işlemek için orada tanımlı onaylayıcılara güveni gerektirmektedir.

Yanzincir yaklaşımı, sistemin kendisini değiştirmeden mevcut bir blokzincir sisteminin geliştirilmesine olanak sağlar. Temel fikir basit ama güçlüdür: hangi özelliklere ihtiyaç duyuluyorsa paralel bir zincir oluşturma ve bu zincirler arasında değer veya para transferi için bir yol sağlamayı hedeflemektedir (bkz. Şekil 5.1). Temelde, akıllı sözleşmeleri desteklemeyen Bitcoin gibi bir blokzincir sistemi, yanzincir yaklaşımı kullanılarak bu yeteneğe sahip olabilir. Aslında, ana blokzincir aynı kalırken, herhangi bir sayıda yanzincir farklı özellik(ler) eklenebilir. Bu noktada, tasarımdaki en önemli ve tartışmalı kısım, para transfer mekanizmasıdır. Mevcut yanzincir mimarileri sistem gereksinimlere bağlı olarak farklı 2WP mekanizmaları sunmaktadırlar.

Yanzincirler herhangi bir durum transferine de izin verir. Ana zincirle uyumlu 2WP kullanan, ana zincire bağlı ama ayrı blokzincirlerdir. 2WP ana zincir ile yanzincir arasında önceden belirlenmiş bir oranda varlıkların değiş tokuşunu sağlar. Bir kullanıcının ilk önce

tokenlarını ana zincirden, tokenların kilitleneceği bir adrese göndermesi gerekir; böylece kullanıcının bu varlıkları harcamaması garanti altına alınır. İşlem tamamlandığında, her iki ağa da bir onay iletilir. Bekleme süresinden sonra, aynı sayıda token, kullanıcının yanına erişmesine ve orada kalmasına izin vererek, yanzincir üzerinde serbest bırakılır. Bir grup sunucu (federasyon) ana zincir ile yanzincirleri arasında aracılık eder ve bir kullanıcının kullandığı tokenların ne zaman kilitlenip serbest bırakılacağını belirler. Bu, ana zincir ile yanzincir arasına başka bir güvenlik katmanı ekler. Federasyon, yanzincir geliştiricileri tarafından seçilir.

Bir yanzincirin ana zincir üzerindeki hesaplama katmanıyla etkileşime girmesi ve anlaşmazlıkları çözümleme amacıyla tokenların kilitlenmesi gerekir. Yanzincirin Açık türde olması gerekmez; özel olarak yönetilebilirler. Bu nedenle, biri varlıkları yanzincirlere ve sonra tekrar ana zincire taşıyabilir. Yanzincirlerin kendi mutabakat mekanizmaları ve dolayısıyla kendi güvenlik seviyeleri vardır. Bu nedenle, yanzincirlerin genellikle teşvik alma amacıyla bir araya toplanmış kendi madenci gruplarına ihtiyaçları vardır. Bu, aynı algoritmaya dayanan iki ayrı tokenın eşzamanlı olarak çıkarılması anlamına gelir. Yeterli madencilik gücü olmayan yanzincirlere saldırılar olabilir. Bir yanzincire yapılacak saldırı, sadece yanzinciri etkiler ve ana zinciri veya diğer yanzincirleri etkilemez.

Durum kanallarının (ing. State Channels) aksine, bir yanzincir üzerindeki işlemler mahrem değildir. Yanzincir üzerinde yayınlanırlar ve böylece yanzincir üzerindeki her katılımcı tarafından görülebilirler. Öte yandan, yanzincirlerde, her zaman erişilebilir olması zorunlu değildir ve katılımcı ekleme/çıkarma için ekstra maliyet yoktur. Bununla birlikte, yanzincirlerin başlangıç maliyeti yüksektir. Ağın saldırganlara karşı güvende olması için yeterli madenciye sahip olmaları gerekir. Ayrıca, federasyon, ana zincir ile yanzincir arasına başka bir katman ekler ve bunun aynı zamanda daha fazla saldırı vektörü oluşturma riski bulunmaktadır.

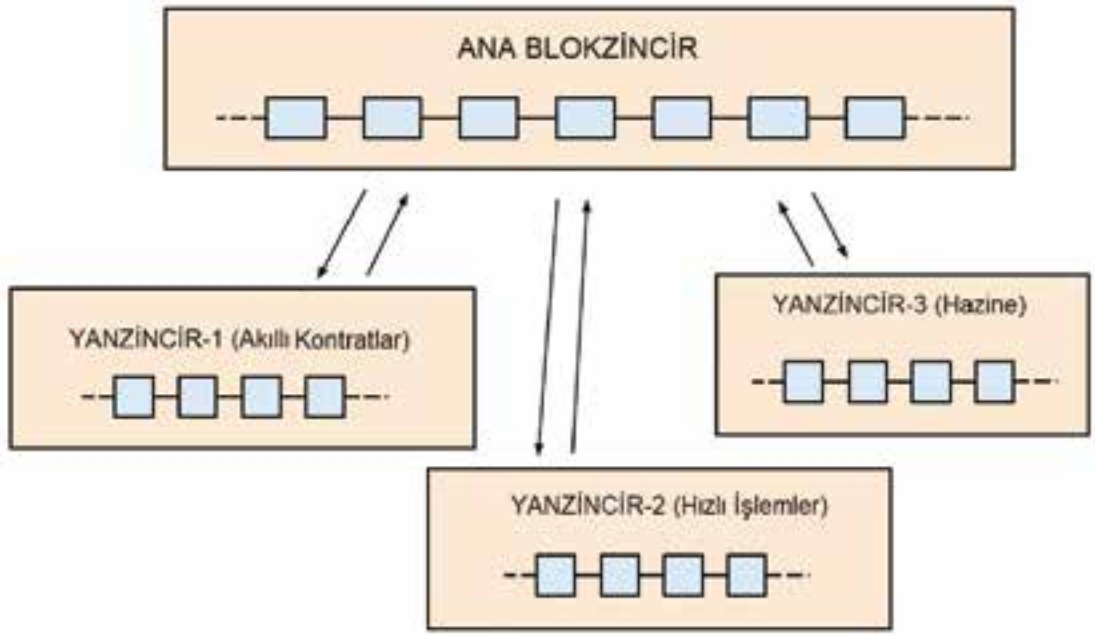
Bu tür yanzincir çözümleri, ademi merkezilikten ödün verilerek ölçeklenebilirliği ve etkinliği yüksek olarak çalışabilir. Ana zincir genel güvenlik ve uyuşmazlık çözümünü garanti ettiğinden, bir yanzincir üzerinde yapılan işlemler, ölçeklenebilirlik karşılığında ademi merkezilikten ödün verebilir. Herkesin bu mutabakatı kabul etmesi ve doğrulaması gerekmez; sadece doğrudan yanzincir üzerinde çalışanların dahil olması gerekir.

Genel yanzincir kavramının kayda değer bir uygulaması [Szt15] tarafından Drivechains adıyla Bitcoin ağının üstüne yanzincirler yerleştirme amacıyla sunulmuştur. İleri transferler (ana zincirden bir yanzincirine), [BCD+14]'deki senkron moddaki gibi ana zincirden SPV provaları sağlanırken, geriye dönük transferler onaylayıcılara dayanır. Drivechain doğrulayıcıları, yanzinciri takip etmek ve transferleri onaylamak isteyen ana zincir madencilerinden oluşmaktadır.

Kiayias ve Zindros, [GKP17] sunumlarında, akıllı sözleşmelerden yararlanarak emek ispatına dayalı blokzincir için yanzincir protokolü gerçeklemesi önermiştir. Akıllı sözleşmelere dayanan bir diğer önemli yanzincir yapısı Poon ve Buterin tarafından Plasma [PB17] adıyla önerildi. Benzer şekilde, farklı 2WP yöntemlerine dayanan, Liquid [DPW+16], Polkadot [Woo17], Interledger [ST18], Cosmos [Cos18] ve daha nice çapraz zincir transfer önerileri bulunmaktadır.

Yanzincirler kendi güvenliklerinden sorumludur, daha önce de belirtildiği üzere yeterli madencilik gücü yoksa, saldırıya uğrayabilir. Her yanzincir bağımsız olduğu için, saldırıya uğradığı ya da tehlikeye atıldığı takdirde, hasar o zincirin içinde yer alacak ve ana zinciri etkilemeyecektir. Buna karşılık, ana zincir tehlikeye girerse, yanzincir hala çalışabilir, ancak kilitlenen değerinin çoğunu kaybeder.

Şekil 5.1: **Temel yanzincir kavramları. Kullanıcıların ana ve yanzincir arasında varlık transferine izin veren işlevsellik [GV18].**



5.1.1 Yanzincir Analizi

Yanzincir Yapılarının Avantajları

›› Yanzincirler kalıcıdır. Eğer hali hazırda belirli bir amaç için bir tane varsa yenisinin üretilmesine gerek yoktur. Yanzincirler bir kez oluşturulduktan sonra korunur. Yani, yanzincirler kapatılmaz, varlıkları ana zincire geri almak için yanzincir kilitlenir. Bu, blokzincir/anazincir dışında belirli bir görevi yapan (örneğin Dogecoin transfer işlemleri) birinin aynı yanzincire geçmesi açısından faydalı olabilir. Bu nedenle, her yeni katılımcı için ayrı zincirler oluşturmak zorunlu değildir. Durum kanallarında ise, mevcut bir kanala bir katılımcı eklemek için ana zincir üzerinde bir işlem gerekir. Ancak Raiden ağı gibi projeler ve daha genelde olarak meta-kanalların tekniği buna kısmi bir çözüm sunmaktadırlar. Bu çözümler bir katılımcı ağı oluştururlar, böylece etkileşim kurulacak her yeni katılımcı için yeni bir kanal oluşturmak zorunda kalınmaz. Hem sizinle hem de alıcı için ortak olan bazı diğer katılımcılarla, sizinle alıcı arasında dolaylı olarak bir kanal oluşturarak katılımcılarla etkileşimde bulunulabilir.

>> Yanzincirler, kripto para birimlerinin birbirleriyle etkileşime girmesini sağlar. Esneklik ekler ve geliştiricilerin ana zincire aktarmadan önce Altcoins beta sürümleri veya yazılım güncellemelerini denemelerine izin verir. Hisselerin çıkarılması ve izlenmesi gibi geleneksel bankacılık işlevleri, ana zincirlere taşınmadan önce yanzincirlerde test edilebilir.

Yanzincir Yapılarının Dezavantajları

>> Yanzincirler ana zincirin güvenliğinden faydalanmazlar. Bir yanzincir üzerinde etkileşime giren bir kullanıcı, bu yanzincirin güvenlik özelliklerine güvenmelidir, çünkü bu durum tehlikeye girerse veya kötü niyetli olursa, kullanıcının ana zincire geri çekilme garantisi yoktur. Buna karşılık, bir durum kanalındaki katılımcılar protokolü takip ettiği sürece her zaman ana zincire geri dönebilirler.

>> Yanzincirler yüksek başlangıç maliyetine sahiptir. Yanzincir oluşturmak için ağın saldırganlara karşı güvenli olmasına yetecek sayıda madenci olması gerekir. Ayrıca, bu madencilerin çevrim içi olduklarından ve çalıştıklarından emin olmak gerekir. Oysa durum kanallarında herhangi bir blokzincir yoktur ve böyle bir gereklilik bulunmamaktadır.

>> Yanzincir için bir Federasyon gereklidir. Bu ise ana zincir ile yanzincir arasına başka bir katman ekler. Bu, saldırganların federasyona rüşvet vererek veya saldırarak sisteme zarar verebileceği başka bir zayıf nokta oluşturabilir. Halbuki durum kanallarında Federasyon yerine akıllı sözleşmeye ihtiyaç vardır.

5.2 Durum Kanalları

Durum kanalları (ing. State Channels), herhangi bir katılımcının riskini önemli ölçüde arttırmadan, zincirde gerçekleşebilecek işlemlerin zincir dışına çıkmasına olanak tanıyan blokzincirin üstünde ikinci bir katman sunar. İşlemler, akıllı sözleşme kullanarak iki kullanıcı arasında açılan, iki yönlü bir yol olan özel bir durum kanalı adındaki ikinci bir katmana taşınır.

Durum kanalları, herhangi bir türden merkezi olmayan uygulama için herhangi bir durumun devrine izin verir; ödeme kanalları yalnızca ödemelerin transferine izin verir. Her iki çözüm de anlaşmazlıkları kolaylaştırmak için varlıkların yatırılmasını gerektirir. Kanaldaki her katılımcı, reddetmeyeceklerini ve yetkili olduklarını kanıtlamak için bu işlemleri özel anahtarlarıyla imzalar. Bu üç aşamalı bir işlemdir:

1. Fon zinciri gibi blokzincir durumunun parçaları çok imzalı veya akıllı bir sözleşme ile kilitlenir. Diğerlerine yalnızca kanalda fon gönderebilirler. Durum zincirini güncellemek için ikili anlaşmaya ihtiyaçları bulunur.

2. Bu iki taraf, genellikle blokzincire sunulacak işlemleri inşa eder ve karşılıklı imzalayarak durumu kendi aralarında güncellerler, ancak blokzincire kayıt için iletmek yerine sadece elde tutulur;

3. Belli bir süreden sonra, her iki taraf da durumu, yeniden açılana kadar durum kanalını kapatan blokzincire geri gönderir.

Eğer iki kişi bir iş ilişkisine sahipse, belirli bir süre zarfında birbirlerine karşılıklı olarak ileri ve geri ödemeler yaptığı varsayılmaktadır. Diyelim ki Alice'in 200 ETH'si ve Bob'un 100 ETH'si olsun. Bir ay içinde Alice, Bob'a her biri 10 ETH tutarında on ödeme, Bob ise Alice'e her biri 20 ETH tutarında iki ödeme göndersin. Bir Ethereum blokzincirinde, bu işlemlerin her biri, toplamda 12 bireysel bir işlem olarak sayılır ve bu da Ethereum ağında gereksiz yük oluşturur. Ayrıca, her bir işlem, işlem ücretlerine tabi olacaktır. Aynı durum, bir durum kanalı ile kanalın açılması ve kapanması olmak üzere sadece iki işlem olarak blokzincire kaydedilmektedir.

İşlemlerin blokzincir dışında ve sadece iki taraf arasında yapılması da daha fazla mahremiyet sağlayabilir. Her şey, tüm ağ üzerinden herkese açık olarak yayınlanmak ve zincir halinde kaydedilmek yerine, bir kanal içinde gerçekleşir. Sadece açılış ve kapanış işlemleri genele açıktır. Ancak, durum kanalları katılan tüm katılımcıların tam olarak erişilebilir olması gerektirir. Kanalın son kapanışı ve bu nedenle durumun nihai olarak sunulması, bir tarafça kötü niyetli bir şekilde gerçekleşebileceğinden, yani kapanış işlemlerinin gözetilmemesi durumunda ilgili fon riski vardır. Böyle bir girişim yakalanırsa, saldırıya itiraz edilebilir ve karşı tarafın cezalandırılması sağlanabilir. Böyle bir işlem, ücret karşılığında bu tür kötü niyetli girişimleri arayan servis sağlayıcılara dış kaynaklı yapılabilir. Katılımcılar kendi adına hareket eden temsilcileri kullanabilirler, ancak temsilcinin saldırı veya rüşvet alma olasılığı da ayrı bir güvenlik riski oluşturur. Kanal yaratmanın maliyeti yüksek olduğu için, durum kanalları ancak katılımcıların uzun süre boyunca pek çok durum güncellemesi yapacağı senaryolarda kullanışlıdır.

Uygulamaya alındıktan sonra, bu kanal içindeki durum başına güncelleme maliyeti son derece düşüktür.

Durumu kilitlemek için kullanılan akıllı sözleşme, belirli bir kanalın katılımcılarını önceden bilmelidir. Bu nedenle, durum kanalları tanımlanmış bir katılımcı grubuyla iyi çalışır ancak katılımcıların eklenmesi ve çıkarılması, akıllı bir sözleşmede değişiklik yapılması veya yeni bir katılımcı eklemek için yeni bir kanalın oluşturulmasını gerektirmekteydi. Daha sonra geliştirilen Şimşek Ağı (Lightning Network, Bitcoin) veya Raiden Ağı (Ethereum) gibi projeler, katılımcılardan oluşan bir ağa ihtiyaç duyan çözümlerle her yeni katılımcının etkileşim kurması için yeni bir kanal oluşturmak zorunluluğunu ortadan kaldırmayı hedeflemişlerdir. Bu durum, ancak ağ üzerinden doğrudan kanal bağlantısı olması halinde, tüm kanallardan bir ağ oluşturarak, kullanıcıların işlemleri diğer kişilerin kanallarına yönlendirilmesine müsaade edebilmektedir.

5.2.1 Durum Kanalı Analizleri

Durum Kanalı Avantajları

›› Durum Kanalları, katılımcıların uzun süre boyunca birçok durum güncellemesini değiştirecekleri durumlarda özellikle yararlıdır. Bunun nedeni, durum kanalı akıllı sözleşmesini dağıtmada bir kanal oluşturmanın başlangıç maliyetinin yüksek olmasıdır. Ancak bir kez konuşlandırıldığında, bu kanal içindeki durum başına güncelleme maliyeti son derece düşüktür.

›› Durum kanallarının güçlü gizlilik özellikleri var: Bunun nedeni, her şeyin genele açık bir şekilde yayınlanmaktan ve zincir halinde kaydedilmekten ziyade katılımcılar arasında bir kanal içinde olmasıdır. Sadece açılış ve kapanış işlemleri genele açık olmalıdır. Yanzincirlerde ise, her işlem, etkileşime girmenizden bağımsız olarak, yanzincirdeki tüm katılımcılar tarafından görülebilmektedir.

›› Durum kanallarının anlık kesinliği vardır, yani her iki taraf da bir durum güncellemesi imzalar imzalamaz, nihai olarak kabul edilebilir. Her iki taraf da, gerektiğinde bu durumu zincir üzerinde "zorlayabilecekleri" konusunda çok yüksek bir garantiye sahiptir.

Durum Kanalı Dezavantajları

›› Durum Kanalları, katılan tüm katılımcıların her an ulaşılabilirliğine ihtiyaç duymaktadır. Yukarıda belirttiğimiz gibi, eğer katılımcılardan biri müsait değilse, o zaman bu onun için maliyetli olabilir. Katılımcılar, uygun olmamaları durumunda kendilerini temsil etmek için üçüncü taraf bir servisi kullanabilir (örneğin, [Patrick McCorry et al., 2018]), ancak temsilcinin saldırıya uğraması veya rüşvet alması olasılığı onu durum kanalları için bir sorun haline getirmektedir. Oysa yanzincirlerin, her zaman erişilebilir durumda olması gerekmemektedir.

›› Durum kanalları net tanımlanmış katılımcı grubuna sahip uygulamalar için kullanılır. Bunun nedeni, durum mevduat sözleşmesinin (durumu kilitlemek için kullanılan sözleşmenin) her zaman belirli bir kanalın parçası olan katılımcıları / kurumları (yani adresleri) bilmesi gerektiğidir. Kişi ekleyebilir veya kaldırabiliriz, ancak sözleşmede her seferinde değişiklik yapılması gerekir. Oysa yanzincirlerde katılımcıların hareketi konusunda böyle bir sınırlama yoktur.

5.2.2 Ödeme Kanalları

Durum kanalları, blokzincirde meydana gelebilecek blokzincir etkileşimleri hakkında düşünmenin çok geniş ve basit bir yoludur, ancak bunun yerine herhangi bir katılımcının riskini önemli ölçüde artırmadan blokzincirden uzaklaşılmaktadır. Bu stratejinin en iyi bilinen örneği, Bitcoin'deki ödeme kanalları fikridir; bu, anında ücretsiz ödemelerin doğrudan iki taraf arasında gönderilmesini sağlamaktadır.

Bir ödeme kanalı (ing. payment channel) ağı, doğrudan işleme bağlı olmayan katılımcılara izin verir, ancak birkaç zorlukla karşılaşılmaktadır. Örneğin, her kanal işlemi teminatlandırılacak hacim gerektirir. 1000 katılımcıya ortalama 1000 USD hizmet etmek isteyen tek bir aktör, bu kanalları başlatmak için zincir üzerinde 1000 işlem gerçekleştirmesi gerekir ve teminat olarak 1 milyon ABD Dolarını reserve beklenmektedir. Ayrıca, katılımcıların, karşı tarafın davranışını gözlemlemek ve muhtemelen yanlış davranışları rapor etmek için, bir ödeme kanalı ağında sürekli çevrim içi olması beklenir.

Ödeme kanallarının pratikte uygulanmasını mümkün kılmak için fonların güvenliğini sağlamak adına işlemleri izleyen ve bekçi (watchguards) olarak adlandırılan aktörlerin varlığına ihtiyaç duyulmaktadır. Bununla birlikte, ödeme kanallarının muhtemel en yaygın kullanıla-

bilirlik endişesi, alıcının, ödeme kabulü sırasında çevrim içi olması şartıdır. Bu gereksinim, birçok senaryo için kanalların gerçek dünyadaki kullanımını karmaşıklaştırır ve pratik kullanımını zorlaştırır.

5.3 Blokzincirlerin Birlikte Çalışabilirliği

Blokzincirler arası birlikte çalışabilirlik, merkezi bir takas gibi bir aracıya ihtiyaç duymadan farklı blokzincirlerin birbirleriyle kolayca iletişim kurmasını sağlayabilir. Bu bağlamda birlikte çalışabilirlik, tokenların ve ilgili verilerin blokzincir sistemleri arasında serbestçe paylaşılma yeteneğini ifade eder. Tamamen birlikte çalışabilir bir ortamda, *A* blokzincirindeki bir kullanıcı, *B* blokzincirdeki başka bir kullanıcıya bir token gönderebilir.

Daha analitik olarak Blokzincirler arası birlikte çalışabilirlik aşağıdaki maddeler altında değerlendirilebilir:

- Farklı zincirler arasında dijital varlık transferi,
- Farklı zincirlerdeki akıllı kontratların birbiri ile etkileşebilmesi,
- Özelleşmiş zincirlerin, diğer zincirler tarafından kullanılabilmesi

Aslında Blockzincir birlikte çalışabilirliği, bazı önerilerin tersine bir fikirdir: ağ etkilerinden dolayı sadece bir blokzincirin yaşayabileceği, kazanan hepsini alır ya da bir blokzincir hepsini yönetir iddialarına anti-tez niteliği taşımaktadır. Zaten, kazanan hepsinin alır iddiaları temelde ademi merkeziyetçilik fikrine de aykırıdır. Dolayısıyla DLT mekanizmalarının geleceği, blokzincir ağlarının birbirleriyle etkileşime girme yeteneklerine bağlı olabilir. Geniş faydalarının yanı sıra, blokzincir teknolojileri, birbirleri ile ve diğer geleneksel sistemlerle birlikte çalışabilme konusunda çeşitli sorunlar sergilemektedir.

Blokzincirlerde ve diğer dağıtık kayıt defter teknolojilerinde (ing. Distributed Ledger Technologies-DLT), yönetilen veri miktarı hızlı bir şekilde artmakta iken, bu dağıtık kayıt defterleri birbirlerinden yalıtılmış olarak kalmaktadır. Blokzincirlerin ve diğer DLT'lerin çoğu bir silo olarak çalışır. Bu ise bir blokzincirin diğer blokzincirlerde veya kayıt defterlerinde neler olduğu hakkında hiçbir bilgisi olmadığı anlamına gelir. Birçok ağda, diğer ağlar işlemlerle tıkanırken kapasite kullanımı düşük olabilmektedir. Uygulamaların, belirli bir blokzinciri teknolojisine bağımlılığı sorunu da oluşmaktadır. Bu gibi sorunlar, teknolojinin geniş kitlelerce kabulünü geciktirmekte, uygulamaların kapsamını sınırlamakta, ölçeklenebilirliği baskılamakta, veri güvenliği ve mahremiyeti için gerekli kontrollerin düşük seviyede kalmasına yol açmaktadır.

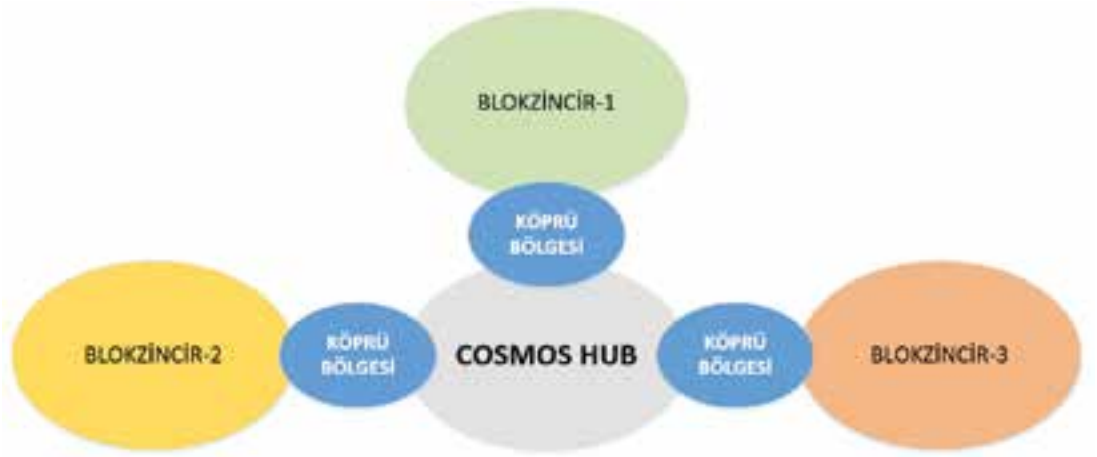
Yanzincirler, blokzincir birlikte çalışabilirliğine doğru atılmış ilk adım olarak görülebilir. Ancak, çalışmaları sürmekte olan Cosmos, Polkadot veya Wanchain gibi birlikte çalışabilirlik standartları, yanzincirlere göre çok daha büyük bir ölçeklendirme sağlayabilecektir.

Bununla birlikte, birlikte çalışabilirliği gerçekleştirmekten için henüz çok erken olabilir. Yukarıda tanımlandığı şekliyle bir birlikte çalışabilirliğin ne zaman mümkün olacağını önceden tahmin etmek şu an için zordur. Zira mevcut blokzincirleri birbirine bağlamak kolay bir iş değildir. ConsenSys'in konuyla ilgili araştırmasına göre, "ticarileştirme rekabeti ve yeniliği

teşvik ediyor, geliştiricileri ve girişimcileri müşterileri için en iyi şekilde çalışan sistemler kurmaya teşvik ediyor" olsa da açık kaynaklı birlikte çalışabilirlik göz ardı ediliyor ve çoğu blokzincir, henüz birlikte çalışabilirliği destekler nitelikte değildir.

Bir dizi blokzincir projesi farklı yaklaşımlar kullanarak birlikte çalışabilirliğe odaklanmış olarak ilerlemektedir. Aşağıdaki paragraflarda, bu proje ve uygulamaların birkaçına ait kısa bilgiler sunulmuştur. Ancak Blokzincir birlikte çalışabilirliğini sağlamak için aşağıda değinilenlerin yanı sıra, Interledger, Virtualchain, Cardano, AION, Icon, Ark, Bytum, Dragonchain ve Ferrum ağı gibi projeler de yürümektedir.

Şekil 5.2: **CosmosHub üzerinden bağlantılanan farklı blokzincirler**



5.3.1 Cosmos

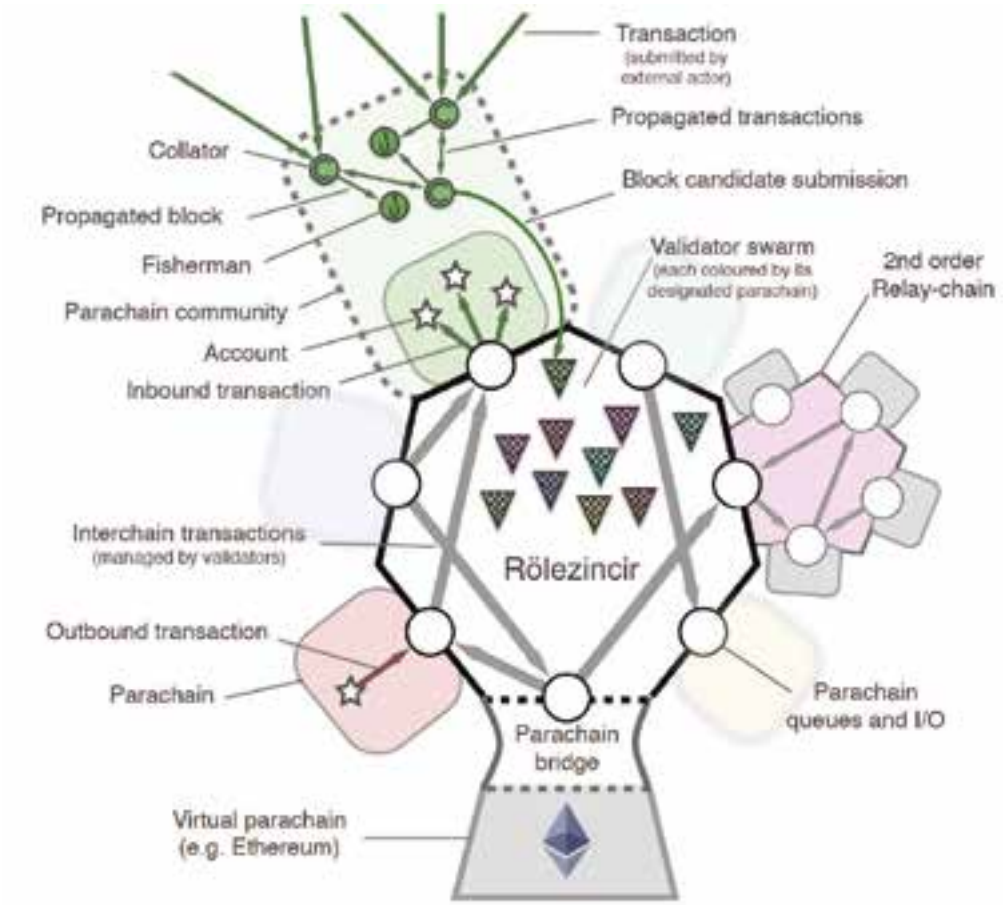
Cosmos [Cos18] çapraz-zincir prensibini izlemektedir. Spesifik olarak, blokzincir birlikte çalışabilirliğini sağlamak için blokzincirler arası bir iletişim (ing. inter-blockchain communication-IBC) protokolü kullanır. Blokzincirler için TCP/IP benzeri mesajlaşma protokolü görevi görür. Cosmos Hub, bölgeler (Zones) olarak adlandırılan blokzincirleri birbirine bağlayıp konuşmalarına olanak sağlayan bir blokzincirdir. Etehereum, Bitcoin, ZCash gibi PoW tabanlı blokzincirler veya özel blokzincirler IBC yoluyla bir köprü bölgesine (bridge-zone) ve onun üzerinden Cosmos Hub'a bağlanabilir. Mevcut blokzincirler (Bitcoin gibi) tasarımsal olarak IBC'yi desteklemediğinden, Cosmos Hub a bağlamak için peg zone kullanmaktadır. Cosmos Hub projesi tüm gemileri birleştiren manasında "amiral gemisi" blockzinciri ile birlikte peg zone ve standartlaştırılmış dillerle blokzincirler arasındaki iletişimi koordine eder. Bununla birlikte, Cosmos Hub, diğer varlıkları içerebilen daha büyük zincir içi ekosistemin bir parçasıdır. Cosmos Hub, PBFT benzeri Tendermint mutabakat algoritmasını kullanır. CosmosHub Polkadot'dan farklı olarak, kullanıcı, kaynak zincire, yönlendirme zincirlerine ve varış zincirine güvenmelidir. Her Blokzinciri kendi güvenilir Köprü bölgesindeki Doğrulayıcıları bulmalıdır. Herhangi bir bölgedeki Doğrulayıcılar, kendi blokzincirlerindeki varlıkları CosmosHub'a, Cosmos-

Hub'da başka bölgenin Doğrulayıcıları tarafından depolanmış herhangi bir varlığı ise kendi blokzincirlerine, belirlenmiş dönüşüm oranlarını kullanarak transfer edebilirler. Göndericiler, Doğrulayıcıların, değerleri transfer ederken dürüst davrandığına güvenmek zorundadır.

5.3.2 Polkadot

Ethereum'un kurucu ortağı Gavin Wood tarafından başlatılan Polkadot [Woo17], bir çoklu-zincir teknolojisidir. Genişleyebilirlik, Ölçeklenebilirlik ve Heterojenlik amaçlarına odaklanır. Temel olarak, farklı teknolojilerle geliştirilmiş, farklı amaçlar için çalışan blokzincirlerin daha büyük ve standart bir ekosisteme bağlanmasını ve aralarında varlık transferi yapabilmelerini sağlar. Örneğin İzinli ve Açık tipten blokzincirlerin birlikte çalışmasına olanak sağlar.

Şekil 5.3: **Polkadot şebekesinin mimarisi**



Polkadot, parachain'ler (işlemleri işleyen ve orijinal blokzincirine transfer eden paralel blokzincirler), onları irtibatlayan bir relay-chain (onları birleştiren, aralarında mutabakatı ve güvenliği sağlayan röle zincir) ve Polkadot'u harici blokzincirlere bağlayan köprülerden oluşur. Parachain'ler işlemleri (transactions) toplayıp işlerler ve zincirler arası işlemler için relay-chain üzerinden gerçekleşen mutabakatı kullanırlar. Mutabakat protokolünde rol alan aktörler şunlardır:

- **Collator:** Parachain'ler için blok üretip doğrulanması için Doğrulayıcılara iletirler. Parachain'lerin kendi işlem ücretlerinden faydalanırlar.
- **Nominator:** Doğrulayıcıların seçimi için hisselerini kullanırlar.
- **Validator:** Relay-chain için blok üretir ve ödül alırlar. Farklı parachain'lere rastgele atanırlar.
- **Fishermen:** Kural dışı davranan Doğrulayıcıları tesbit edip raporlar ve ödül alırlar.

Bütün parachain'ler ve relay-chain birlikte bir sistem gibi hareket eder. Paracahin, kendi iş mantığı kapsamında durum geçişlerini yönetirken diğer zincirlerle mesaj alış verişi de yapabilir. Parachain'lerin birbirleri ile etkileşimi eş zamanlı yürüdüğü için, işlem hızlarının ölçeklenebilirliği açısından iyileşme elde edilir.

Parachain, köprü kontrat üzerinden pasif olarak bilgi dinleyebilir. Parachain'ler birbiri ile eş statüdedir. Parachain'ler başka bir parachain için değil relay-chain odaklı davrandıkları için sistem, tamamıyla güven otoritesi bağımlılığı olmadan çalışır. Parachain'ler birbirlerine güvenmek zorunda değildir ve relay-chain'in doğrulayıcı kümesi tarafından sağlanan ortak güven seviyesinden faydalanırlar. Aksi halde sistemde güvenlik seviyesi en düşük olan Parachain, sistemin en zayıf halkası olurdu. Polkadot ağına bağlanan parachain, artık ağın sağladığı, PoS tabanlı, eş ve tek bir güvenlik seviyesine ortak olmuş olur. Cosmos da ise her yeni zincir, kendi doğrulayıcı kümesine sahiptir ve kendi güvenliğini kendisi kurup başlatır.

Polkadot, parachain'lerde oluşabilecek arızalara veya kötü niyetli davranışlara müdahale için bir çevrim-içi yönetişim mekanizması da içerecek şekilde geliştirilmektedir. Kötü niyetli davranan Doğrulayıcıların tespiti ve bildirilmesi için mekanizmalar içerir.

5.3.3 Chainlink

Chainlink [EJN17] merkezi olmayan bir kahin (oracle) hizmetidir. Verilerin zincir dışı API'lerden alınmasına ve bir blokzincire konmasına izin verir. Başka bir deyişle, Chainlink blokzincirlerle zincir dışı var olan tüm altyapı arasında bir köprü görevi görür: Oracle düğümleri gerçek dünyadan veri alır, ağ üzerinden işler ve blokzincire eklemektedir. Chainlink, özellikle dünya genelinde bankaların çoğunun kullandığı küresel bankalararası veri transferi ve ödeme sistemi SWIFT ile işbirliği yapmaktadır.

5.3.4 Wanchain

Wanchain [LYL+19], bağlantısız blokzincirler arasında veri transferini kolaylaştırmak için farklı bir protokol kullanır. Bu nedenle, peg zone'ları veya çoklu-zincir analoglarını dağıtmak yerine, Wanchain diğer bloklarla takas edilebilen sözde "sarılmış" token'ları yaratır.

Örneğin, 10 ETH'yi BTC zincirine taşımak için, platform ilk önce akıllı sözleşmeler kullanarak Ethereum blockchain üzerindeki bu ETH miktarını kilitler. Bu WETH daha sonra bir ticaret platformunda Wanchain sarılı BTC (WBTC) için takas edilebilir. Bu sarılmış BTC token'ları daha sonra Bitcoin blokzincirinde bulunan orijinal token'lara dönüştürülür.

5.3.5 Quant

Yukarıda bahsedilen ve farklı blokzincirleri birbiri ile haberleştirmeye yönelik olan örneklerin aksine, Quant [VTPM18] bir blokzincir değildir. İş katmanını teknolojik katmandan ayırmak için, mevcut blokzincirlerin üzerinde bir katman olan ve mesaj tabanlı çalışan Overledger protokolünü kullanır. Overledger, aynı anda birden fazla blokzincir üzerine kurulmuş katmanda çalışan ve haberleşebilen merkezi olmayan uygulamaların (DApps) geliştirilmesine olanak tanır. Bu uygulamalar, alttaki blokzincirin tipinden bağımsız olarak haberleşebilir ve değer alış verişi yapabilir. Örneğin, bir DApp, veri aktarımı için Bitcoin Cash (BCH) kullanırken veri depolaması için Ethereum blokzincirine güvenebilir.

SONUÇ

Bu raporda, hayatımıza dokunmaya başlamasıyla birlikte iş yapış biçimlerinin yeniden tasarlanmasını sağlayan blokzincir teknolojisinin, temelinde bulunan mahremiyet ve güvenlik olguları incelenmiştir. Kullanım senaryolarının çeşitlenerek daha fazla sektöre yaygınlaşması, GDPR ve KVKK gibi düzenlemelerin de hayatımıza girmesiyle birlikte blokzincir platformlarının sunduğu güvenlik ve mahremiyet özellikleriyle birlikte teknikleri de değişkenlik göstermeye başlamıştır. Yapısı gereği tecrübe edildiğinde öğrenilen bir teknoloji olan blokzincir, gelişimini tüm hızıyla sürdürmeye devam etmektedir.

BKM ve TÜBİTAK BİLGEM tarafından hazırlanan Blokzincirlerde Güvenlik ve Mahremiyet başlıklı raporda, blokzincir teknolojisinin bu başlıklarda tek başına çözüm olarak görülmemesi gerektiği vurgulanmıştır. Bununla birlikte blokzincir tabanlı uygulamalarda, kullanım amacına uygun yardımcı tekniklerle kullanılarak karmaşık olmayan güvenli çözümler üretilmesi gerektiği sonucuna ulaşılmıştır:

- Blokzincir platformlarının mahremiyet ve güvenlik seviyeleri, basit takma isimlerden tam gizlilige kadar çesitlilik gösterebilir.
- Blokzincirin güvenlik ve mahremiyet isteklerini tek başına çözen bir yöntem yoktur. Bu nedenle, güvenlik ve mahremiyet gereksinimlerine ve uygulama içeriğine uyan teknikler seçilmelidir. Genel olarak, çoklu teknolojilerin kombinasyonunun, tek bir teknolojiden daha etkili çalıştığı gözlemlenmiştir.
- Kusursuz veya her yönüyle mükemmel olan hiçbir teknoloji yoktur. Karmaşık bir sisteme yeni teknolojiler eklemek, başka sorunlara veya yeni tür saldırılara neden olabilir. Bu nedenle, bazı güvenlik ve mahremiyet tekniklerinin blokzincirlere entegre edilmesiyle ortaya çıkan tuzaklara ve olası zararlara dikkat edilmesi gerekir.

KAYNAKÇA

[ABLZ17] Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, and Michał Zając, *A subversion-resistant snark,* International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2017, pp. 3–33.

[AN11] Tolga Acar and Lan Nguyen, *Revocation for delegatable anonymous credentials,* International Workshop on Public Key Cryptography, Springer, 2011, pp. 423– 440.

[ATSM09] Man Ho Au, Patrick P Tsang, Willy Susilo, and Yi Mu, *Dynamic universal accumulators for ddh groups and their application to attribute-based anonymous credential systems,* Cryptographers' Track at the RSA Conference, Springer, 2009, pp. 295–308.

[BAZB19] Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh, *Zether: Towards privacy in a smart contract world,* IACR Cryptology ePrint Archive 2019 (2019), 191.

[BB08] Dan Boneh and Xavier Boyen, *Short signatures without random oracles and the sdh assumption in bilinear groups,* Journal of Cryptology 21 (2008), no. 2, 149– 177.

[BBB+17] Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, *Bulletproofs: Short proofs for confidential transactions and more,* Cryptology ePrint Archive, Report 2017/1066, 2017, **https://eprint. iacr.org/2017/1066.**

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau, *Minimum disclosure proofs of knowledge,* Journal of computer and system sciences 37 (1988), no. 2, 156–189.

[BCC+16] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit, *Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting,* Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2016, pp. 327–357.

[BCD+14] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille, *Enabling blockchain innovations with pegged sidechains*, 2014.

[BCD+18] S. Barra, A. Castiglione, M. De Marsico, M. Nappi, and K. R. Choo, *Cloud-based biometrics (biometrics as a service) for smart cities, nations, and beyond*, IEEE Cloud Computing 5 (2018), no. 5, 92–100.

[BCG14] Dan Boneh and Henry Corrigan-Gibbs, *Bivariate polynomials modulo composites and their applications,* International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2014, pp. 42–62.

[BCI+13] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Omer Paneth, and Rafail Ostrovsky, *Succinct non-interactive arguments via linear interactive proofs,* Theory of Cryptography Conference, Springer, 2013, pp. 315–333.

[BDL+12] Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang, *High-speed high-security signatures,* Journal of Cryptographic Engineering 2 (2012), no. 2, 77–89.

[BDM93] Josh Benaloh and Michael De Mare, *One-way accumulators: A decentralized alternative to digital signatures,* Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1993, pp. 274–285.

[BDSMP91] Manuel Blum, Alfredo De Santis, Silvio Micali, and Giuseppe Persiano, *Noninteractive zero-knowledge,* SIAM Journal on Computing 20 (1991), no. 6, 1084–1118.

[BFLS91] L. Babai, L. Fortnow, L. Levin, and M. Szegedy, *Checking computations in polylogarithmic time,* Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 1991, pp. 21–31.

[BG18] Blockchain and GDPR, *How blockchain could address five areas associated with gdpr compliance,* 2018.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2003, pp. 416– 432.

[BGM17] Sean Bowe, Ariel Gabizon, and Ian Miers, *Scalable multi-party computation for zk-snark parameters in the random beacon model,* Cryptology ePrint Archive, Report 2017/1050, 2017, **https://eprint.iacr.org/2017/1050.**

[BH19] Düzenlemeler ve Kamu İlişkileri Çalışma Grubu BCTR Hukuk, *Kişisel verilerin korunması hukuku ve blokzincir teknolojisi raporu*, Kasım 2019.

[BK17] Alex Biryukov and Dmitry Khovratovich, *Equihash: Asymmetric proof-of-work based on the generalized birthday problem,* Ledger 2 (2017), 1–30.

[BLL02] Ahto Buldas, Peeter Laud, and Helger Lipmaa, Eliminating counterevidence with applications to accountable certificate management 1, Journal of Computer Security 10 (2002), no. 3, 273–296.

[Bol02] Alexandra Boldyreva, *Efficient threshold signature, multisignature and blind signature schemes based on the gap-diffie-hellman-group signature scheme,* Cryptology ePrint Archive, Report 2002/118, 2002, **https://eprint.iacr.org/2002/118.**

[BP97] Niko Barić and Birgit Pfitzmann, *Collision-free accumulators and fail-stop signature schemes without trees,* International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1997, pp. 480–494.

[BSBC+17] Eli Ben-Sasson, Iddo Bentov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, et al., *Computational integrity with a public random string from quasilinear pcps,* Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2017, pp. 551–579.

[BSCG+13] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza, *Snarks for c: Verifying program executions succinctly and in zero knowledge,* Annual Cryptology Conference, Springer, 2013, pp. 90–108.

[BSCTV14a] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza, *Scalable zero knowledge via cycles of elliptic curves,* Annual Cryptology Conference, Springer, 2014, pp. 276–294.

[BSCTV14b] _____, *Succinct non-interactive zero knowledge for a von neumann architecture,* 23rd USENIX Security Symposium USENIX Security 14), 2014, pp. 781–796.

[BtGDPR19] Blockchain and the General Data Protection Regulation, *Can distributed ledgers be squared with european data protection law?,* 2019.

[But14] Vitalik Buterin, *Ethereum: A next generation smart contract and decentralized application platform,* Online, White Paper 2014, **http://www.the-blockchain.com/docs/Ethereum_white_paper-a_ next_ generation_smart_contract_and_decentralized_application_ platform-vitalik-buterin.pdf**

[Cha81] David L. Chaum., *Untraceable electronic mail, return addresses, and digital pseudonyms,* Commun. ACM 24 (1981), no. 2, 84–90.

[CHKO08] Philippe Camacho, Alejandro Hevia, Marcos Kiwi, and Roberto Opazo, *Strong accumulators from collision-resistant hashing,* International Conference on Information Security, Springer, 2008, pp. 471–486.

[CKS09] Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente, *An accumulator based on bilinear maps and efficient revocation for anonymous credentials,* International Workshop on Public Key Cryptography, Springer, 2009, pp. 481–500.

[CL02] Jan Camenisch and Anna Lysyanskaya, *Dynamic accumulators and application to efficient revocation of anonymous credentials,* Annual International Cryptology Conference, Springer, 2002, pp. 61–76.

[Cos18] *Cosmos Network:,* 2018, **https://cosmos.network/docs/.**

[CZJ+17] Ethan Cecchetti, Fan Zhang, Yan Ji, Ahmed E. Kosba, Ari Juels, and Elaine Shi, Solidus: *Confidential distributed ledger transactions via PVORM,* ACM CCS'17, ACM, 2017, pp. 701–717.

[CZK+18] Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller, and Dawn Song, Ekiden: *A platform for confidentiality-preserving, trustworthy, and performant smart contract execution,* CoRR abs/1804.05141 (2018).

[Dam91] Ivan Damgård, Towards *practical public key systems secure against chosen ciphertext attacks,* Annual International Cryptology Conference, Springer, 1991, pp. 445–456.

[Dam98] _____, *Commitment schemes and zero-knowledge protocols,* School organized by the European Educational Forum, Springer, 1998, pp. 63–86.

[DFGK14] George Danezis, Cédric Fournet, Jens Groth, and Markulf Kohlweiss, *Square span programs with applications to succinct nizk arguments,* International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2014, pp. 532–550.

[DH76] Whitfield Diffie and Martin Hellman, New directions in cryptography, IEEE transactions on Information Theory 22 (1976), no. 6, 644–654.

[DHS15] David Derler, Christian Hanser, and Daniel Slamanig, *Revisiting cryptographic accumulators, additional properties and relations to other primitives,* Cryptographers' Track at the RSA Conference, Springer, 2015, pp. 127–144.

[DM16] George Danezis and Sarah Meiklejohn, *Centrally banked cryptocurrencies,* NDSS'16, The Internet Society, 2016.

[DPW+16] Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, and Mark Friedenbach, Strong federations: *An interoperable blockchain solution to centralized third party risks,* CoRR (2016), **http://arxiv.org/abs/ 1612.05491**

[DT08] Ivan Damgard and Nikos Triandopoulos, *Supporting non-membership proofs with bilinear-map accumulators,* Cryptology ePrint Archive, Report 2008/538, 2008, **https://eprint.iacr.org/2008/538.**

[Dwo15] Morris J Dworkin, *Sha-3 standard: Permutation-based hash and extendable-output functions,* Tech. report, 2015.

[EJN17] Steve Ellis, Ari Juels, and Sergey Nazarov, *ChainLink A Decentralized Oracle Network – Whitepaper,* September 2017, **https://link.smartcontract.com/ whitepaper.**

[Fin18] Michéle Finck, *Blockchains and data protection in the european union,* 2018, Version 0.5, Accessed: 2019-11-10.

[FS86] Amos Fiat and Adi Shamir, How to prove yourself: *Practical solutions to identification and signature problems,* Conference on the Theory and Application of Cryptographic Techniques, Springer, 1986, pp. 186–194.

[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova, *Quadratic span programs and succinct nizks without pcps*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2013, pp. 626–645.

[GKP17] Juan A. Garay, Aggelos Kiayias, and Giorgos Panagiotakos, *Proofs of work for blockchain protocols,* Cryptology ePrint Archive, Report 2017/775, 2017, **https: //eprint.iacr.org/2017/775.pdf.**

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, *The knowledge complexity of interactive proof systems,* SIAM Journal on computing 18 (1989), no. 1, 186–208.

[Gro10] Jens Groth, *Short pairing-based non-interactive zero-knowledge arguments,* International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2010, pp. 321–340.

[Gro16] _____, *On the size of pairing-based non-interactive arguments,* Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2016, pp. 305–326.

[GV18] Alberto Garoffolo and Robert Viglione, *Sidechains: Decoupled consensus between chains,* 2018.

[Har19] Jason Hart, Gdpr one year anniversary: *A risk-based approach to gdpr is key for achieving compliance,* 2019.

[Hea16] Mike Hearn, Corda: *A distributed ledger,* Nov 2016, Version 0.5, Accessed: 2019-11-10.

[Hel12] Lipmaa Helger, *Secure accumulators from euclidean rings without trusted setup,* International Conference on Applied Cryptography and Network Security, Springer, 2012, pp. 224–240.

[HLX17] Xuan Han, Yamin Liu, and Haixia Xu, *A user-friendly centrally banked cryptocurrency,* ISPEC'17, LNCS, vol. 10701, Springer, 2017, pp. 25–42.

[Kil92] Joe Kilian, *A note on efficient zero-knowledge proofs and arguments,* Proceedings of the twenty-fourth annual ACM symposium on Theory of computing, ACM, 1992, pp. 723–732.

[KMS+16] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,* 2016 IEEE Symposium on Security and Privacy (SP), May 2016, pp. 839–858.

[KVK18] KVKK, *Data protection in turkey,* 2018.

[KZG10] Aniket Kate, Gregory M Zaverucha, and Ian Goldberg, *Constant-size commitments to polynomials and their applications,* International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2010, pp. 177–194.

[Lam79] Leslie Lamport, *Constructing digital signatures from a one-way function*, Tech. report, Technical Report CSL-98, SRI International Palo Alto, 1979.

[Lip13] Helger Lipmaa, *Succinct non-interactive zero knowledge arguments from span programs and linear error-correcting codes,* International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2013, pp. 41–60.

[LLNW16] Benoit Libert, San Ling, Khoa Nguyen, and Huaxiong Wang, *Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors,* Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2016, pp. 1–31.

[LLX07] Jiangtao Li, Ninghui Li, and Rui Xue, *Universal accumulators with efficient nonmembership proofs,* International Conference on Applied Cryptography and Network Security, Springer, 2007, pp. 253–269.

[LRY16] Benoît Libert, Somindu C. Ramanna, and Moti Yung, *Functional commitment schemes: From polynomial commitments to pairing-based accumulators from simple assumptions,* Cryptology ePrint Archive, Report 2016/766, 2016, https://eprint.iacr.org/2016/766.

[LSY+19] Y. Li, W. Susilo, G. Yang, Y. Yu, X. Du, D. Liu, and N. Guizani, *Toward privacy and regulation in blockchain-based cryptocurrencies,* IEEE Network (2019), 1–7.

[LWW04] Joseph K Liu, Victor K Wei, and Duncan S Wong, *Linkable spontaneous anonymous group signature for ad hoc groups,* Australasian Conference on Information Security and Privacy, Springer, 2004, pp. 325–335.

[LYL+19] Jack Lu, Boris Yang, Zane Liang, Ying Zhang, Eric Swartz, and Lizzie Lu, *Building super financial markets for the new digital economy wanchain white-paper* – version 0.9.1, 2019, https://wanchain.org/files/ Wanchain-Whitepaper-EN-version.pdf.

[McD13] Mindi McDowell, *Understanding denial-of-service attacks,* 2013.

[MDH+17] Shunli Ma, Yi Deng, Debiao He, Jiang Zhang, and Xiang Xie, *An efficient nizk scheme for privacy-preserving transactions over account-model blockchain,* Cryptology ePrint Archive, Report 2017/1239, 2017, https://eprint.iacr.org/2017/ 1239.

[MGGR13a] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin, *Zerocoin: Anonymous distributed e-cash from bitcoin,* 2013 IEEE Symposium on Security and Privacy, May 2013, pp. 397–411

[MGGR13b] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin, *Zerocoin: Anonymous distributed e-cash from bitcoin,* 2013 IEEE Symposium on Security and Privacy, May 2013, pp. 397–411.

[MOR01] Silvio Micali, Kazuo Ohta, and Leonid Reyzin, *Accountable-subgroup multisignatures,* Proceedings of the 8th ACM conference on Computer and Communications Security, ACM, 2001, pp. 245–254.

[MP15] Gregory Maxwell and Andrew *Poelstra, Borromean ring signatures,* 2015.

[MPR11] Hemanta K Maji, Manoj Prabhakaran, and Mike Rosulek, *Attribute-based signatures,* Cryptographers' track at the RSA conference, Springer, 2011, pp. 376–392.

[MV13] Atefeh Mashatan and Serge Vaudenay, *A fully dynamic universal accumulator,* Proceedings Of The Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science 14 (2013), no. ARTICLE, 269–285.

[Nak09] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system.*

[Ngu05] Lan Nguyen, *Accumulators from bilinear pairings and applications,* Cryptographers' Track at the RSA Conference, Springer, 2005, pp. 275–292.

[NVV18] Neha Narula, Willy Vasquez, and Madars Virza, *zkledger: Privacy-preserving auditing for distributed ledgers*, NSDI'18, USENIX Association, 2018, pp. 65–80.

[Nyb96] Kaisa Nyberg, *Fast accumulated hashing,* International Workshop on Fast Software Encryption, Springer, 1996, pp. 83–87.

[Oka88] Tatsuaki Okamoto, *A digital multisignature scheme using bijective public-key cryptosystems,* ACM Transactions on Computer Systems (TOCS) 6 (1988), no. 4, 432–441.

[OO99] Kazuo Ohta and Tatsuaki Okamoto, *Multi-signature schemes secure against active insider attacks,* IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 82 (1999), no. 1, 21–31.

[PB17] Joseph Poon and Vitalik Buterin, *Plasma: Scalable autonomous smart contracts,* Aug 2017, Accessed: 2017-08-10.

[Ped91] Torben Pryds Pedersen, *Non-interactive and information-theoretic secure verifiable secret sharing,* Annual International Cryptology Conference, Springer, 1991, pp. 129–140.

[Per09] Colin Percival, *Stronger key derivation via sequential memory-hard functions,* 2009.

[PHGR13] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova, *Pinocchio: Nearly practical verifiable computation,* 2013 IEEE Symposium on Security and Privacy, IEEE, 2013, pp. 238–252.

[Rad12] Shirley Radack, *Secure hash standard: Updated specifications approved and issued as federal information processing standard (fips) 180-4,* Tech. report, National Institute of Standards and Technology, 2012.

[RGB16] Ian Grigg Mike Hearn Richard Gendal Brown, James Carlyle, Corda: *An introduction, August 2016,* Accessed: 2019-11-10.

[Ric14] Silas Richelson, *Cryptographic protocols with strong security: Non-malleable commitments, concurrent zero-knowledge and topology-hiding multi-party computation,* Ph.D. thesis, UCLA, 2014.

[rip] Ripple., **https://ripple.com/files/ripple_solutions_overview.pdf,** Accessed 17-04-2019.

[Sab13] N. V. Saberhagen, *Cryptonote v 2.0.,* 2013.

[SALY17] Shi-Feng Sun, Man Ho Au, Joseph K Liu, and Tsz Hon Yuen, *Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero,* European Symposium on Research in Computer Security, Springer, 2017, pp. 456–474.

[San99] Tomas Sander, *Efficient accumulators without trapdoor extended abstract,* International Conference on Information and Communications Security, Springer, 1999, pp. 252–262.

[SCG+14a] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, *Zerocash: Decentralized anonymous payments from bitcoin*, 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 459–474.

[SCG+14b] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza, Zerocash: *Decentralized anonymous payments from bitcoin,* 2014 IEEE Symposium on Security and Privacy, IEEE, 2014, pp. 459–474.

[Sch91] Claus-Peter Schnorr, *Efficient signature generation by smart cards*, Journal of cryptology 4 (1991), no. 3, 161–174.

[Ser20] İsa Sertkaya, *Kripto para sistemleri,* Bİlgem Teknoloji (2020), no. 8, 26–29.

[ST18] E Schwartz S Thomas, *A Protocol for Interledger Payments*, 2018, **https:// interledger.org/interledger.pdf.**

[Szt15] P. Sztorc, *Drivechain - the simple two way peg, November 2015*, **http://www. truthcoin.info/blog/drivechain/.**

[Tea19a] Fabric Team, *Hyperledger fabric documents,* 2019, Accessed: 2019-11-10.

[Tea19b] _____, *Hyperledger fabric tutorials,* 2019, Accessed: 2019-11-10.

[Tea19c] Quorum Team, *How tessera works,* 2019, Accessed: 2019-11-10.

[Tea19d] _____, *Quorum - enterprise ethereum client,* 2019, Accessed: 2019-11-10.

[TK19a] Matthijs van den Bos Cees van Wijk Aleksei Koren Tommy Koens, Scott King, *Solutions for the corda security and privacy trade-off: Having your cake and eating it,* October 2019, **https://mondovisione.com/_assets/files/Corda_ DoSt_v1.6.pdf.**

[TK19b] Scott King Tommy Koens, *Solutions for the corda security and privacy tradeoff: Having your cake and eating it*, October 2019, **https://mondovisione.com/ _assets/files/Corda_DoSt_v1.6.pdf.**

[Vee17] Meilof Veeningen, *Pinocchio-based adaptive zk-snarks and secure/correct adaptive function evaluation,* International Conference on Cryptology in Africa, Springer, 2017, pp. 21–39.

[VTPM18] Gilbert Verdian, Paolo Tasca, Colin Paterson, and Gaetano Mondelli, *Quant overledger – whitepaper,* January 2018, **https://www.quant.network/wp-content/ uploads/2018/09/Quant_ Overledger_Whitepaper-Sep.pdf.**

[W+14] Gavin Wood et al., *Ethereum: A secure decentralised generalised transaction ledger,* Ethereum project yellow paper 151 (2014), no. 2014, 1–32.

[WKCC18] Karl Wüst, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun, *Prcash: Centrally-issued digital currency with privacy and regulation,* IACR Cryptology ePrint Archive 2018 (2018), 412.

[Woo17] Gavin Wood, *Polkadot: Vision for a heterogeneous multi-chain framework,* 2017, **https://polkadot.network/PolkaDotPaper.pdf.**

[XWZ+18] Jian Xu, Laiwen Wei, Yu Zhang, Andi Wang, Fucai Zhou, and Chong-zhi Gao, *Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures,* Journal of Network and Computer Applications 107 (2018), 113–124.

[ZXL19] Rui Zhang, Rui Xue, and Ling Liu, *Security and privacy on blockchain,* ACM Comput. Surv. 52 (2019), no. 3, 51:1–51:34.

belgem.io
Herkes için Blokzincir

Blokzincir
Almanağı 2019

Blockchain 101

Sorularla
Blockchain

Keşif: Blockchain'in
Sırları

Yayınlara, yanlarında yer alan karekodu okutarak ya da tıklayarak ulaşabilirsiniz.


BKM
BANKALARARASI
KART MERKEZİ


TÜBİTAK
BİLGEM


BLOKZiNCiR
Araştırma Laboratuvarı