T.C.
EGE ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

TEDARİK ZİNCİR YÖNETİM SİSTEMİNDE YENİ BİR BOYUT; İZLENEBİLİRLİK VE ŞEFFAFLIK İÇİN BLOK ZİNCİR TEKNOLOJİSİNİN KULLANIMI

Doktora Tezi

Bora Buğra SEZER

Matematik Anabilim Dalı

İzmir
2022

T.C.
EGE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TEDARİK ZİNCİR YÖNETİM SİSTEMİNDE YENİ BİR BOYUT; İZLENEBİLİRLİK VE ŞEFFAFLIK İÇİN BLOK ZİNCİR TEKNOLOJİSİNİN KULLANIMI

Bora Buğra SEZER

Tez Danışmanı: Prof. Dr. Urfat NURİYEV
İkinci Tez Danışmanı: Doç. Dr. Selçuk TOPAL

Matematik Anabilim Dalı
Bilgisayar Bilimleri Doktora Programı

İzmir 2022

EGE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

ETİK KURALLARA UYGUNLUK BEYANI

EÜ Lisansüstü Eğitim ve Öğretim Yönetmeliğinin ilgili hükümleri uyarınca Doktora Tezi olarak sunduğum " **Tedarik Zincir Yönetim Sisteminde Yeni Bir Boyut; İzlenebilirlik ve Şeffaflık İçin Blok Zincir Teknolojisinin Kullanımı**" başlıklı bu tezin kendi çalışmam olduğunu, sunduğum tüm sonuç, doküman, bilgi ve belgeleri bizzat ve bu tez çalışması kapsamında elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara atıf yaptığım ve bunları kaynaklar listesinde usulüne uygun olarak verdiğimi, tez çalışması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını, bu tezin herhangi bir bölümünü bu üniversite veya diğer bir üniversitede başka bir tez çalışması içinde sunmadığımı, bu tezin planlanmasından yazımına kadar bütün safhalarda bilimsel etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

/ / 2022

Bora Buğra SEZER

ÖZET

TEDARİK ZİNCİR YÖNETİM SİSTEMİNDE YENİ BİR BOYUT; İZLENEBİLİRLİK VE ŞEFFAFLIK İÇİN BLOK ZİNCİR TEKNOLOJİSİNİN KULLANIMI

SEZER, Bora Buğra

Doktora Tezi, Matematik Anabilim Dalı
Tez Danışmanı: Prof. Dr. Urfat NURİYEV
İkinci Tez Danışmanı: Doç.Dr. Selçuk TOPAL
Ağustos 2022, 79 sayfa

Tedarik zincir yönetimi sisteminde izlenebilirlik ve denetlenebilirlik sistemin en önemli temel yapılardır. Ayrıca, bu sistemlerde diğer önemli unsur ise güvendir ve mevcut merkezi sistemlerde üçüncü taraflara güven mecburidir. Tedarik zincirde sistem izlenebilirliği ve güvenliği için birçok mimari yapılmış olsa da bu mimarilerde güven, kullanıcı mahremiyeti, gerçek zamanlı bilgi ve zayıf izlenebilirlik gibi temel eksikliklere sahiptir. Bu tez çalışmasında, tedarik zincir izlenebilirliği için blokzincir-tabanlı mahremiyeti koruyan yeni bir çerçeve öneriyoruz. Mimarimiz, aktörler arasında mahremiyeti koruyan ve kriptografik protokoller ile kullanıcı dijital imza ve doğrulama entegre edilerek güvenlik sağlanmıştır. Ayrıca zincir dışı entegre sistemi ile performans sağlanarak yapılan testler sonucunda ölçeklenebilirlik için olumlu sonuçlar ortaya koyulmuştur. Dahası, kullanıcı isteğine bağlı olarak anonimlik ve izlenebilirlik arasında denge sağlanmıştır. Mimari ayrıca ilgili ürün kimliği ile tüm aşamalar şeffaf bir şekilde izlenebilir ve doğrulanabilir bir yapıya sahiptir.

Anahtar kelimeler: Tedarik zinciri, Mahremiyet, Blokzincir, Akıllı sözleşme, İzlenebilirlik

ABSTRACT

A NOVEL APPROACH IN THE SUPPLY CHAIN MANAGEMENT SYSTEM. USE OF BLOKZINCIR TECHNOLOGY FOR TRACEABILITY AND TRANSPARENCY

SEZER, Bora Buğra

PhD in Mathematics.
Supervisor: Prof. Dr. Urfat NURİYEV
Co-Supervisor: Assoc. Prof. Dr. Selçuk TOPAL
August 2022, 79 pages

Traceability and auditability in the supply chain management system are the essential basic structures of the system. In addition, another vital element in these systems is trust, and trust in third parties is mandatory in existing centralized systems. Although many architectures have been built for system traceability and security in the supply chain, these architectures have fundamental deficiencies such as trust, user privacy, real-time information, and poor traceability. In this thesis, we propose a new blokzincir-based framework that is privacy-preserving for supply chain traceability. The architecture has provided security by integrating user digital signature and authentication with cryptographic protocols, protecting privacy between actors. In addition, positive results for scalability were revealed as a result of the tests carried out by ensuring performance with the off-chain integrated system. Moreover, a balance has been achieved between anonymity and traceability based on user requests. The architecture also has a structure that can be monitored and verified transparently with the relevant product identity.

Keywords: Supply chain, Privacy, Blokzincir, Smart contract, Traceability

ÖNSÖZ

Doktora tez çalışmasında hedefim; Akıllı sözleşmeler kullanarak üçüncü taraflardan gizliliği koruyan tedarik zinciri izlenebilirliği için zincir dışı ve zincir üstü akıllı sözleşme entegrasyonunda mevcut kriptografik teknikler kullanılarak dijital imza ve doğrulama sağlayan bir çerçeve oluşturmaktır.

İZMİR 31/08/2022

Bora Buğra SEZER

İÇİNDEKİLER

Sayfa

İÇ KAPAK ii

KABUL ONAY SAYFASI iii

ETİK KURALLARA UYGUNLUK BEYANI v

ÖZET vii

ABSTRACT ix

ÖNSÖZ xi

İÇİNDEKİLER DİZİNİ xiii

ŞEKİLLER DİZİNİ xvii

TABLOLAR DİZİNİ xix

SİMGELER VE KISALTMALAR DİZİNİ xxi

1. GİRİŞ 1

1.1 Tedarik Zincir Yönetim Sistemi 4

1.1.1 Yapılan Çalışmalar 7

1.1.2 Tedarik Zincirde İzlenebilirlik 11

1.2 Blok Zincir Teknolojisi 12

1.2.1 İzinsiz Blok Zincir 14

İÇİNDEKİLER (devam)

Sayfa

1.2.2 İzinli Blok Zincir....14

2. GEREÇ VE YÖNTEM 15

2.1 Kriptografik Yapılar 15

2.1.1 Kriptografik Şifreleme Sistemleri....15

2.1.2 Eliptik Eğri Kriptografisi 16

2.1.3 Dijital İmza 18

2.2 Blokzincir Teknolojisinin Altyapısı 21

2.2.1 Blok Oluşumu 22

2.2.2 Fikir Birliği Protokolleri 25

2.2.3 Fikir Birliği Protokollerinin Hata Toleransı 30

2.2.4 Fikir Birliği Protokollerinin Tutarlılığı 32

2.2.5 Eşler Arası Ağların ve Fikir Birliği Protokollerin Güvenlik Açıklığı 32

2.2.6 Akıllı Sözleşmeler....36

2.2.7 Akıllı Sözleşmenin Güvenliği, Sebep ve Sonuçları 42

2.2.8 Zincir ve Zincir Dışı Veri İşleme 43

2.2.9 Anonimleştirme Teknikleri....44

İÇİNDEKİLER (devam)

Sayfa

3. ÇALIŞMA MODELİ 46

3.1 Çerçevenin İşlemler Detayı 48

3.1.1 Digital İmzalama 51

3.1.2 Doğrulama 52

3.2 Güvenlik Analizi 52

3.3 Karmaşıklık 53

3.3.1 Hesaplama Karmaşıklığı 54

3.3.2 İletişim Karmaşıklığı 55

4. DENEYSEL SONUÇLAR 56

4.1 Detaylar 62

5. SONUÇ 64

KAYNAKLAR DİZİNİ 65

TEŞEKKÜR 76

ÖZGEÇMİŞ 77

ŞEKİLLER DİZİNİ

Şekil Sayfa

1.1. Tedarik zincir izlenebilirliği 7

2.1 Açık anahtar şifrelemesi 16

2.2 Dijital imzalama 19

2.3 Eliptik Eğri *Q Ve* F_p Gösterimi 20

2.4 Eliptik eğri dijital imzalama algoritması uygulanması.....21

2.5 Zaman damgası (Timestamps) ve değişmezliği (Immutability).....23

2.6 İş kanıtı akışı.....28

2.7 Hisse kanıtı akışı.....29

2.8 Bizans Hata Toleransı'nın çalışma biçimi 30

2.9 Fikir birliği protokollerinde olası zafiyetler ve nedenleri.....36

2.10 Ethereum sanal makinesi'nde (Ethereum Virtual Machine (EVM)) akıllı sözleşme.....38

2.11 Akıllı sözleşme tabanlı çalışmaların sınıflandırılması 39

2.12 Akıllı sözleşme diyagramı 41

2.13 Akıllı sözleşme olası zafiyetler ve nedenleri 43

ŞEKİLLER DİZİNİ (DEVAM)

Şekil Sayfa

2.14 Zincir dışı (off-chain) ve zincir (on-chain) kullanımı 44

3.1 Blokzincir tabanlı tedarik zincir yönetim sisteminin kavramsal çerçevesi..... 46

3.2 Çerçevenin akıllı sözleşme mimarisi 47

3.3 Zincir dışında dijital imzalama ve doğrulama (basitleştirilmiş) 51

4.1 Sistem şeması, zincir dışı ve zincir üzerinde yürütülen blok zinciri uygulamasının test ekranı..... 58

4.2 Olay ve depolamaya tabanlı (event-storage-based) sözleşmelerin ortalama gaz maliyeti 59

4.3 İşlemin oluşturulması ve doğrulanmasının hesaplama süresi..... 61

4.4 Olay ve depolama tabanlı sözleşmenin iletişim maliyeti..... 61

TABLOLAR DİZİNİ

Tablo Sayfa

1.1 Dağıtık Defter Teknolojisinin Temel Özellikleri 13

2.1 Eliptik Eğri Üzerinde Açık- Özel Anahtar Çifti 18

2.2 Eliptik Eğri Digital İmzalamada Kulanılan Parametreler..... 20

2.3 İzinsiz, İzin Verilen Blokzincir ve Merkezi Bir Veri Tabanı Karşılaştırılması..... 25

2.4 Fikir Birliği Protokollerinin Genel Karşılaştırması 32

3.1 Çerçevenin Yapı Tablosu 49

3.2 Mimarinin Karmaşıklığı 55

SİMGELER VE KISALTMALAR DİZİNİ

Simgeler	Açıklama
B_i	Blok
H	Hash değeri
M	Aktörün üye sayısı
A_k	Herbir aktörün işlem sayısı
S_k	İlgili aktörün imzası
V_k	İlgili aktörün doğrulaması
N	Nonce değeri
k,q	açık-özel anahtar çifti
t, t_{ij}, t_i	İşlem süresi
a_{id}	Aktör kimliği
p_{id}	Ürün kimliği
p_{inf}	Ürün bilgileri
p_{idlist}	Ürün kimlik listesi
$h(ptx_i)$	Ürün bilgileri hash değeri
p_{time}	İşlem yürütme zamanı

SİMGELER VE KISALTMALAR DİZİNİ (DEVAM)

Simgeler	Açıklama
$h(ptx_{prev})$	Önceki işlem hash değeri
$sig_h\ (h(ptx_i))$	İmzalı hash değeri
$sign(h(ptx_i))$	İlgili aktör imzası
$verfy(sig(h(ptx_i)),sig_h(h(ptx_i)))$	İlgili aktör doğrulaması

Kısaltmalar

PoW	İş Kanıtı
PoS	Hisse kanıtı
PBFT	Bizans hata toleransı
RSA	Rivest, Shamir and Adleman (algoritma)
SHA	Güvenli hash algoritması
ECDSA	Eliptik eğri digital imzalama algoritması
JSON	JavaScript nesnesi gösterimi
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü
TX	İşlemler
EPC	Elektornik ürün kodu

SİMGELER VE KISALTMALAR DİZİNİ (DEVAM)

RFID	Radyo frekans tanımlama
DLT	Dağıtılmış defter teknolojisi
ISO	Uluslararası Standardizasyon Örgütü

1. GİRİŞ

Bu bölümde, tedarik zinciri yönetimi, blok zinciri teknolojisi, sistem ve değerlendirme yöntemleri araştırma alanındaki mevcut literatüre kısa bir genel bakış ve tanıtımı sağlanacaktır. Ayrıca, bu konularla ilgili literatürdeki araştırma boşlukları özetlenecek ve bu araştırmada kullanılan ilgili yöntem ve teknolojiler tanıtılacaktır.

Tedarik zinciri yönetim sistemi, ürün ve hizmetlerin tedarikçisinden son aşamada müşteriye kadar olan süreci kapsamaktadır. Bu yol üzerindeki tüm faaliyetleri, insan kaynaklarını, teknolojiyi, şirket yapılarını ve kaynakları kapsayan kavramın adı olarak açıklanabilir. Tedarik zinciri sürecinde gerçekleştirilen tüm faaliyetlerde yer alan her türlü kaynak ve bileşen, ürüne dönüştürülerek son aşamada müşteriye teslim edilir. Tedarik zinciri oluşturan ilişkiler ve bağlantılar bünyesinde tedarikçilere, distribütörlere, toptancılara, perakendecilere ve tüketicilere doğru bir yol vardır. Bu zincirin her halkası düzenli olarak birbirini takip etmektedir. Benzer şekilde iş süreçleri açısından da belirli aşamaları olduğunu söyleyebiliriz. Üretim, stok yönetimi, malzeme temini, dağıtım, satış, satın alma, müşteri ilişkileri yönetimi gibi değerli süreçler tedarik zincirin işleyişini sağlamaktadır. Son zamanlarda üretici ve nihai tüketici arasındaki aracıların sayısının artması nedeniyle malların üretimi karmaşık hale gelimiştir. Üretici ve tüketici arasında güvenin aynı zamanda tedarik zinciri performansının önemli bir unsuru olduğu ve maliyet düşüşlerini, daha yüksek esnekliği ve daha iyi ilişkisel yönetişimi desteklediği de söylenebilir (Kim and Chai, 2017). Tedarik zincirinde güven ve bilgi paylaşımının analizi söz konusu olduğunda, çalışmalar genellikle talep ve envanter verilerine odaklanmaktadır. Tedarik zincirindeki her oyuncunun kendi üretim planlaması, envanter kontrolü ve malzeme ihtiyaç planlama faaliyetleri için müşterilerinin taleplerini zamanında ve doğru bir şekilde tahmin etmesi gerekmektedir (Tsanos and Zografos, 2016). Tedarik zincirleri daha fazla talep odaklı hale geldikçe, veri doğruluğu çok önemlidir ve kuruluşlar, rekabet performanslarında güveni hayati bir faktör olarak algılamaktadırlar. Bununla birlikte, düşük güven senaryosunda, tedarik zinciri ortakları, özellikle aynı kademedeki şirketler olmak üzere, kendilerini giderek artan bir şekilde ortaklardan ziyade gelir için rekabet eden varlıklar olarak

gördükleri için diğer ortaklara bilgi sağlamaya isteksizdir. Oluşacak bir tahmin belirsizliği tedarik zinciri boyunca yayılacak ve bu süreç tedarik zincirinde sipariş-miktar değişkenliğini artıracaktır. Sonunda, satışların varyansını, aşırı güvenlik stokunu, artan lojistik maliyetlerini ve kaynakların verimsiz kullanımını aşan daha büyük bir üretim varyansına yol açacaktır. Ayrıca küreselleşme ve pazar genişlemesi, şirketleri yeni pazar gereksinimlerini karşılamak için ürün portföylerini ve yaşam döngülerini genişletmeye zorlamıştır. Zorluk sadece niceliksel değil, aynı zamanda niteliksel hale de gelmiştir. Tedarik zincirinin ana zorluğu, izlenebilirlik ve veri yönetim sistemi üzerinedir. Sağlık, finans, gıda ve eğitim başta olmak üzere çoğu sektörde bilgi sistemlerinin yönetimi merkezileştirilmiştir. Burada ilgili işlemler, karar verme ve depolama sistemi üçüncü taraf aracılar tarafından kontrol edilmektedir. Dahası, merkezi bir yönetim sistemi, veri bütünlüğü, kullanılabilirliği ve esnekliği için bir tehdit oluşturabilir ve sistemi dolandırıcılığına kadar ilerleme yapabilmektedir (Abeyratne and Monfared, 2016). Dolayısıyla Tedarikçiler ve müşterileri arasında güvenilir bir ekosistem oluşturulmalıdır. Bu, doğru veri toplama ve güvenli veri depolamanın gerekli olduğu durumlarda, ürün izlenebilirliğini sağlamak için zincirin şeffaflığına odaklanan bir politika ile sağlanır.

Blok zincir, sağladığı şeffaflık sayesinde birbirleriyle doğrudan güvene dayalı ilişkiler kurmamış farklı tarafları bir araya getirebilecek başka bir alternatif sunarken, tedarik zinciri yönetmeye yardımcı olacak bir teknolojidir. Blok zincir, ağdaki tüm tarafların, kronolojik olarak verilere eklenenler de dahil olmak üzere, aynı verilere erişimi paylaşabileceği bir yol sağlayarak, üçüncü taraflara veya aracılara olan ihtiyacı potansiyel olarak azaltarak, ağ üzerinde gerçekleşen her işlemi veya veri alışverişini depolamaktadır. Blokzincir'deki veriler kaldırılamaz veya değiştirilemez. Blok zinciri, her bir tarafın aynı verileri neredeyse gerçek zamanlı olarak görmesine izin vererek, günümüz dünyasındaki çoğu sistemin gerektirdiği karmaşık ve maliyetli veri fikir birliğini ortadan kaldırmaya yardımcı olabilir. Verileri ilgili taraflarla şüphesiz paylaşırken hem küresel hem de yerel olarak veri beyan etmek ve yayınlamak için mahremiyet ve şeffaflık sağlamaktadır.

Tedarik zincir yönetim sisteminde izlenebilirlik sağlanabilmesi için

doğrulanabilirliğin mahremiyetin ve güven ile ilgili sorunların istenilen düzeye getirebilmek için yeni bir çalışma yapılmalıdır. Bu tez çalışmasında amaç, tedarik zincir yönetimi persfektifinden merkezi bir otoritenin güvenine bağlı olmayan, merkezi olmayan bir bilgi sistemi oluşturmaktır. Bu sistem için gizlilik-korumayı ön planda tutarak yeni bir yaklaşım olan blok zincir teknolojisini kullanılmıştır. Blok zincir teknolojisi, tedarik zincirinin izlenebilirlik çözümleri için umut verici bir teknoloji olduğunu gösteriyor. Blok zincir teknolojisi sayesinde, bu yeni merkezi olmayan bilgi sistemi, tüm tedarik zinciri üyeleri için (devlet daireleri ve üçüncü taraf düzenleyiciler dahil) açıklık, şeffaflık, tarafsızlık ve güvenilirliğe dayalı bir bilgi platformu sağlayabilecek bir yenilik haline gelebilir. Gerçek zamanlı ürün takibi için izlenebilir bir sistem kurmak, bunu genel tedarik zinciri risk yönetimi yöntemleriyle entegre ederek bir güvenlik kontrol sistemi oluşturulabilinir. Ayrıca blokzincir teknolojisinin bağlantı özelliği sayesinde ürünlerin izlenebilirliği sağlanmaktadır. Dolayısıyla bu durum lojistik şirketlerinin performansını önemli ölçüde iyileştirmiş olacaktır. Bunların hepsi nihayetinde bir tedarik zincirinin güvenlik güvencesini artıracaktır.

Tedarik zinciri çalışmalarında önerilen sistemler şeffaflık ve izlenebilirlik sağlayabilir. Bu sistemlerde üreticiden tüketiciye kadar her adım görüntülenebilir ve doğrulanabilir. Ancak ilgili aktörlerin mahremiyeti konusundaki çalışmalara baktığımızda bu durum yeterince dikkate alınmamıştır. Blok zincirinin anonimliğini artırmak için farklı protokoller önerilmiştir (örneğin, Zerocash (Sasson et al., 2014)). Bununla birlikte, şeffaflık ve anonimlik arasında nasıl bir denge kurulacağına dair araştırma zorluğu devam etmektedir. Bu tez çalışmasında, kullanıcı isteklerine bağlı olarak şeffaflık ve anonimliği dengeleyen blok zinciri tabanlı bir çerçeve öneriyoruz. Çalışma, belirtilen sorunları ele almak için gizliliği koruyan izinli bir blok zinciri mimarisi kullanılarak yapılmıştır. Mevcut kriptografik protokoller (dijital imzalama, doğrulama) zincir dışı entegre edilerek gerçekleştirilmiştir. Çerçevede, aktörlerin mahremiyet eksikliğini gidermek için eliptik eğri dijital imza algoritması (ECDSA) kullanılmaktadır (Hankerson et al., 2006). Şifreleme sistemindeki verileri şifrelemek ve şifresini çözmek için bir açık-özel anahtar çifti kullanılmaktadır. RSA (Rivest et al., 1978) açık anahtarlı şifreleme sisteminde daha büyük anahtarlar kullanıldığından, bu dezavantajın üstesinden gelmek için NIST (Kerry and Director, 2013) onaylı ECDSA

önerilmiştir (Jansma and Arrendondo, 2004). Dijital imzalar, reddedilemezlik ve kimlik doğrulama bütünlüğüne sahiptir. Bu nedenle çalışmamızda akıllı sözleşmelerde eliptik eğri şifreleme algoritması kullanılarak dijital imzalama gerçekleştirilmiştir (Johnson et al., 2001). Ancak çerçeve sadece tedarik zinciri yönetimi için değil, IoT tabanlı akıllı tarım, akıllı şehirlerde veri güvenliği ve kullanıcı gizliliği, giyilebilir sensörlerden elde edilen verilerin izlenebilirliği, veri güvenliği ve kullanıcı gizliliği gibi birçok gizliliği koruyan uygulama alanlarında da kullanılabilirdir (Sezer vd., 2022). Ayrıca, mimarinin başlıca özellikleri şu şekilde açıklanmaktadır;

- Karmaşık bir dizi şifreleme işleminden kaçınan basit işlevselliğe sahip anonim bir tasarımdır.
- Hem veri gizliliğini hem de doğrulanabilirliği sağlayan bir veri iletim mimarisine sahiptir.
- Zincir içi ve zincir dışı kod performansını dikkate alan pratik ve gerçek zamanlı bir çalışmadır.
- Hyperledger gibi izinli blokzincirlerden farklı olarak, üzerinde işlem yoğunluğu gibi sorunları önlemek için sözleşmenin zincir-dışı olay-tabanlı sözleşme entegrasyonu ile hem kod performansını artıran hem de işlem ücretini önemli ölçüde azaltan bir performansa sahiptir.

Tezin geri kalanı şu şekilde organize edilmiştir: kısaca Tedarik zincir yönetim sistemi, blokzincir teknolojisi tanıtılmış ve ilgili alanda daha önce yapılmış çalışmaları gözden geçirerek çalışmalarımızın bir ön değerlendirmesi sunulmuştur. Daha sonra mimarimiz tanıtılmıştır. Deneysel sonuçlarla sistemimizin izlenebilirliği ve denetlenebilirliği detaylı olarak analiz edilmiştir. Doğrulama için açık anahtarlı şifrelemenin nasıl kullanıldığı sistemin gizliliği tartışılmıştır. Son olarak, sonuç sunulmuştur.

1.1 Tedarik zincir yönetim sistemi

Tedarik zincir yönetim sistemi işletmelerin ayrılmaz bir parçası ve üreticiden tüketiciye izlenebilirlik, şeffaflık, denetlenebilirlik sunan önemli bir

sistemdir. Sektörde çeşitli hastalıklardan gıda güvenliğine kadar ilgili verilerin izlenebilirliği denetlenebilirliği ve güvenliği sağlanır. Sistemde bir diğer önemli unsur ise şeffaflıktır. Çeşitli ülkelerde şeffaflığı artırmak ve tüketiciyi ürünün kalitesi, güvenliği ve sürdürülebilirliği gibi konularda bilgilendirmek için sertifikalar geliştirilmiştir (Grunert et al., 2014). Bu sertifikalar tedarik zincirde ürün ya da başka bileşenin sürdürülebilirliğine ve tüketicinin ilgili ürün ya da bileşenin güven duyarak ilgisinin artmasına olarak sağlar. Buda sistemdeki bileşenlerin gerekliliğini doğrular. Dolayısıyla tedarik zincirde yer alan aktörler, tüketicilere doğrulanabilirliği sağlayan ilgili sertifika ya da etiketler üzerine bir yapı oluşturulmasını gerektirir. Günümüzde ise ilgili endüstriler kendi bireysel sistemlerini kendileri merkezi sistemlerde inşa edip, minimum bilgiyi paylaşarak tedarik zinciri yönetim sistemi boyunca izlenebilirliği kısıtlamaktadır. Dahası aynı sistem üzerinde bulunan rakip işletmeler nedeniyle aktörler arasında gizlilik esas alınır. Sistemdeki ana amaç merkezi bir otoritenin yerine kontrolün kendilerinde olmalarını sağlamaktır.

Yapılan çalışmalara baktığımızda, Çin ve yabancı ülkeler arasındaki soğuk zincir endüstrisinin gelişim durumunun çalışmasına dayanan, tarımsal gıda soğuk zinciri için bir geliştirme stratejisi sunmuştur. Ayrıca (Chan et al., 2006), tüm soğuk zincirin performansını artırmak için ürünlerin, işlemlerin ve hizmetlerin performansının değerlendirilebileceği faktörlerin dikkate alınması gerektiğinde belirtmiştir. (Li et al., 2006), bir tarım-gıda tedarik zinciri için dinamik bir planlama yöntemi geliştirmiştir. Bu yöntem, aynı zamanda tarımsal gıda tedarik zinciri üyeleri için karı en üst düzeye çıkarırken, tarımsal gıda ürünlerinin kayıplarını en aza indirmeye planlamıştır. Dolayısıyla ilgili çalışmada analitik bir model kullanarak, tarımsal gıda tedarik zincirinden geçen gerçek zamanlı ürün bilgilerinin değerli bir şekilde kullanılabileceğini gösterdiler. Diğer birçok araştırmacı, tarımsal gıda kalitesi ve güvenliği üzerinde çalışmıştır (Trienekens and Zuurbier, 2008). Hükümet dairelerinin tarımsal gıda ürünlerinin kalite ve güvenliğini sağlamaya mevzuat ve düzenlemeler belirleyerek yanıt vermesi gerektiğini vurgulamıştır. Skandalların ardından tüketici güvenini yeniden tesis etmek için, tarımsal gıda tedariğinin şeffaflığı yoluyla kalite ve güvenlik kontrolünü garanti altına almak için üretim protokollerinin uygulanması veya tedarik zinciri yönetimi süreçlerinde bilgi teknolojisinin uygulanması gibi birçok

önlem de alınmaktadır (Akkerman et al., 2010).

Araştırmalara göre, tedarik zinciri dünya genelinde sürekli büyüyen bir sektör olmuştur. Sürdürülebilir bir rekabet ortamı oluşması sebebiyle müşteri değerini en üst düzeye çıkarmak için sistemdeki bileşenler faaliyetlerini aktif bir şekilde yönetmek zorundadırlar. Dünyadaki küreselleşme tedarik zinciri aktorlerinin dünyaya yayılmasını sağlayarak sistemdeki bileşenlerin daha güçlü düzenlemelere maruz kalması ve sonucunda da denetlenebilirlik için önemli bir adım süreci olarak görebiliriz.

Tedarik zinciri yönetim sistemi; tedarikçi, üretici, satıcı, perakendeci ve müşteri olmak üzere beş aktörden oluşmaktadır (Şekil 1.1). Bu sistem üreticiden tüketiciye kadar birden fazla tarafların işbirliğini gerektirmektedir. Ancak günümüz tedarik zinciri yapısında bazı temel sorunlar mevcuttur. Örneğin ürünlerdeki etiketler ürünlere basıldığı için kolayca sahtesi üretilebilir. Sahte etiketlerin yanı sıra, sahte veya kalitesiz malzeme ve bileşenler ve ticari markaların uygunsuz kullanımı, sahte malların ve fikri mülkiyet hırsızlığının tüketicilere ve şirketlere nasıl zarar verdiğini göstermektedir (J. Andino, 2014). Bu gibi olumsuzluklarda müşterilerin güven mekanizması sarsıldığı için şirketler üzerinde finansal sorunlara da sebep olabilmektedir. Ve yine merkezi sistemlerde sistemin kontrolü tek bir şirkette oluğu için, sistemdeki en ufak bir veri kaybı zincirdeki aktörlerin işlerini olumsuz etkileyebilir. Dolayısıyla tedarik zincirine katılan aktörlerin sisteme yazma izinleri almasına izin veren bir sistem gereklidir. Bununla birlikte, tüketiciler izlenebilirlik ve şeffaflık sağlamak için sistem hakkında fikir edinmelidir. Ürünlerdeki sertifikaların doğrulanması ve bu doğrulama sürecine uygun sistemlerin geliştirilmesi güven olmayan ortamda güven mekanizması çalıştırılması bu tarz sorunları çözebilecektir. Ayrıca tedarik zinciri ağında birbirine rakip taraflar olduğundan dolayı sistemde tüm veriler paylaşılamaz olur ve birbirinden bağımsız yerel ve özel sistemler ortaya çıkar. Yani sitemlerde izlenebilirlik sorun haline gelir. Bu nedenle taraflar arasındaki ilişkileri bozmayan tüm sistem boyunca izlenebilir bir sisteme ihtiyaç vardır.

Şekil 1.1 Tedarik Zincir İzlenebilirliği

1.1.1 Yapılan çalışmalar

Bu bölümde, tedarik zincir için blok zincir uygulamaları hakkındaki literatür de bulunan ilgili çalışmalar gözden geçirilmiş ve vurgulanmıştır. Araştırmalarımızda, (Tian, 2017), blokzincir kullanılarak Tehlike Analizi ve Kritik Kontrol Noktalarına (Hazard Analysis and Critical Control Points) dayalı bir gıda tedarik zinciri izlenebilirliği önermektedir. Daha önce (Tian, 2016) tarımsal gıda tedarik zinciri izlenebilirliği için Radyo Frekansı ile Tanımlama (Radio Frequency Identification (RFID)) ve blok zincirinin avantajlarını ve dezavantajları ile ilgili literatür çalışmaları yapmıştır. Bir başka çalışma da, değer zinciri boyunca gelen verileri entegre eden blok zinciri tabanlı bir izlenebilirlik çözümü sunmuştur (Caro et al., 2018). Tarladan ürün takibi için bir kullanım durumu geliştirilmiş ve Hyperledger aracılığıyla uygulama karşılaştırmaları yapmıştırlar. (Tse et al., 2017), blokzincir teknolojisinin gıda tedarik zincirine nasıl uygulanacağını yüksek düzeyde soyut bir düzeyde tartıştılar ve blokzincir tabanlı çözümü geleneksel çözümlerle karşılaştırdılar. Mahremiyetin korunması konusunda çeşitli çalışmalar yapılmıştır. Bunlardan biri kullanıcı kimliğini koruduğu için sanal halkaya (virtual ring) dayalı bir yapı önerilmiştir (Badra and Zeadally, 2014). Burada kullanıcı sanal halkayı kullanarak kontrol merkezine gönderir ve kontrol merkezi gelen kullanıcı kimliğini bilmeden kimlik doğrulama imzasıyla kimlik doğrulaması yapmaktadır. Ancak burada kullanılan sanal özelliğinden dolayı kontrol merkezine gelen sahte mesajı kimin gönderdiği bilinemez. Bu durum dezavantaj olarak kullanılabilir. Diğer bir çalışma ise anonimliğe dayalı olarak mahremiyetin korunmasını sağlamaktır (Efthymiou and Kalogridis, 2010; Zhou et al., 2017). Anonimlik, kullanıcı kimliklerini korumak için yaygın olarak kullanılan bir tekniktir. Kullanıcı bilgilerini hassas bilgi olarak tanımlayabiliriz. Ancak, anonimliği sağlayacak nitelik bilgisi yoksa kullanıcı kimliği ile hassas bilgiler arasındaki ilişkiyi bulmak için bazı tanımlayıcılar gözlemlenebilir. Blokzincir teknolojisinin kripto para sistemlerinde başarılı bir şekilde kullanılmasının

ardından bu teknolojinin farklı alanlarda kullanımı üzerine çeşitli araştırmalar yapılmıştır. Araştırma öncelikle işlem gizliliği üzerine olmuştur. Diğer bir deyişle, mevcut merkezi olmayan sistemlerden farklı olarak, finansal işlemlerin blok zincirinde net bir şekilde saklanamadığını ve işlem gizliliğinin kamu tarafından korunduğunu göstermiştir (Kosba et al., 2016). Kriptografik teknikler kullanılarak elde edilen bir diğer çalışma ise ZCash'tir. k-SNARK'lar (ZCash tarafından kullanılır) etkileşimli olmayan sıfır bilgi bilgi kanıtıdır. Bu protokol, inatçılığa ve bağlantısızlık temelinde anonimlik sağlamıştır. Burada işlemin aynı kişiye gönderildiğini kanıtlamak mümkün değildir. Ancak zk-SNARKs tekniğinde yüksek maliyet ve performans sınırlaması gibi nedenlerle istenilen verim elde edilememiştir (Sasson et al., 2014).

Son yıllarda gıda, eczacılık ve tarımsal gıda ürünleri gibi sektörlerde izlenebilirlik dikkat çekmeye başlamıştır (Expósito et al., 2013; Vo et al., 2016). Ayrıca ürünlerin izlenebilirliği açısından da önemli akademik çalışmalar yapılmıştır (Yan et al., 2018). Diğer çalışmalarda da ileri teknolojinin kullanıldığı tedarik zincirinde RFID teknolojisi uygulamaları yapılmıştır. Tedarik zincirinde RFID teknolojisi kullanımının aktörler arasında bir arada yaşamayı sağladığı ve daha verimli olduğu yapılan çalışmalarda gösterilmiştir (Wang et al., 2010). Ancak RFID teknolojisinin tedarik zincirinde merkezi bir sistemle çözülebileceği iddia edildi. Bu teknolojide kullanılan etiketler blok zincir teknolojisi ile birleştirilse de blok zincir teknolojisinin ayrı yönleri ve izlenebilirliğin ayrı yönleri tartışılmıştır. Performans, bütünlük ve uygulanabilirlik iddiaları, çalışmaların gösterdiği analiz sürecinde doğrulanmamaktadır (Tian, 2016). Başka bir çalışmada ise sistemde fiziksel olarak kullanılan etiketler yerine, aktörlerin kimliklerinin dijital olarak imzalanması, sertifika veren ilgili kuruluşlar tarafından yapılmaktadır (Abeyratne and Monfared, 2016). Ancak bu çalışmada kimlik, aktörlerin mahremiyeti olmadan ağa yayınlanmaktadır. (Salah et al., 2019)'de, ethereum blok zinciri ve akıllı sözleşme kullanarak tarımda tedarik zinciri izlenebilirliği ve şeffaflığı üzerine olmuştur. Önerilen yapı, merkezi otoriteler ve aracılar olmadan çalışmayı sağlamaktadır. (Lin et al., 2021)'de, DAC protokollerinin kimlik bilgisi gizliliği açısından esnek olduğu ve bu durum için menzil kanıtlarının (range-proof) kullanılabileceği belirtilmektedir. Çalışmada, akıllı şebekelerin gizliliğini korumak için dayanıklı protokol tabanlı bir SM2

dijital imza şeması önerilmiştir. (Zhang et al., 2021)'daki çalışmada, yazarlar, tıbbi uygulamalarda kullanıcı gizliliğini koruyan yeni bir 5G entegre blok zinciri tabanlı iletişim izleme planı önerdiler. (Xu et al., 2021) de, blokzincir'in temel özelliklerinden biri olan bilgi güvenliğinin SC'de şeffaflığı nasıl etkilediği üzerine bir çalışma yapılmıştır. (Caro et al., 2018) de, tarımsal gıda tedarik zincirinde IoT ve blok zincirine dayalı merkezi olmayan izlenebilirlik sunulmaktadır. Yazarlar, Ethereum ve Hyperledger Sawtooth olmak üzere iki farklı blok zinciri uygulaması kullandılar. Çalışma, blok zincirinde şeffaflık ve izlenebilirliği vurgulamasına rağmen, gizlilik yönü göz ardı edildi. Konsept olarak Nesnelerin İnterneti, akıllı şehirlerden SC'ye kadar birçok alanda önemli bir faktördür. Bununla birlikte, IoT'nin zorlu özellikleri nedeniyle güvenli bir ekosistemin oluşturulması da önemli bir yapı taşıdır. Bu noktada, çalışma (Abbas et al., 2021) akıllı ulaşım sistemleri için güvenli ve güvenilir bir mimari önermektedir. Bir diğer önemli kavram, kuantum bilgisayarlarda IoT tabanlı blok zinciridir. Kuantum bilgisayarlar, günümüz bilgisayar sistemlerinin performansının ötesinde bir performans sunar. Bu tür donanımların gerçekleştirilmesi kriptosistemler için önemli sonuçlara sahiptir. Ayrıca, IoT tabanlı sistemler de dahil olmak üzere birçok alan güvenlik ihlallerine karşı savunmasız hale geliyor. Çalışma (Abd El-Latif et al., 2021), klasik kripto hash fonksiyonları yerine kuantum hash fonksiyonlarını kullanan IoT cihazları arasında güvenli bir mimari önermektedir. Başka bir çalışmada (Nguyen et al., 2021), sağlık hizmetlerinde siber-fiziksel sistemler için veri toplama ile sensör cihazları kullanan blok zinciri tabanlı bir saldırı önleme sınıflandırma modeli önerilmiştir. (Ahmad et al., 2021)'te, havacılık ve savunmada operasyon yönetimi, sınır koruma, lojistik ve SC gibi çoklu senaryolarda bir blok zinciri çözümü tanıtılarak temel fırsatlar ele alındı. (Schmidt and Wagner, 2019)'da yazarlar, işlem maliyeti teorisi merceğinden blok zincirinin SC üzerindeki etkisini inceleyen ve işlem maliyetlerini azaltma potansiyelini araştıran bir çalışma yürütmüştür. (Rejeb et al., 2019)'de yazarlar, blok zinciri ve IoT'de SC verimliliğini artırmak ve kaliteyi iyileştirmek için özellikle ölçeklenebilirlik olmak üzere bazı önerilerde bulundular. Ayrıca, çalışmada (Min, 2019; Sunny et al., 2020), çeşitli blok zinciri tabanlı SC izlenebilirlik çözümleri hakkında bir literatür taraması bulunabilir.

Akıllı sözleşmeler, işlemlerin otomatik olarak çözülmesini ve bu durumun

kendi kendine fark edilmesini sağlamaktadır. Blokzincir'deki sisteme entegre edilen akıllı sözleşmeler, gelecekte daha potansiyel uygulamalardan biri olarak kabul edilebilir. Gizlilik içeren akıllı sözleşmeler üzerine yapılan çalışmalara baktığımızda, zkay (Steffen et al.,2019) akıllı sözleşmelerin şifrelenmiş verilerle yazıldığı görülmektedir. İşlemlerin doğruluğunu kanıtlamak için sıfır bilgi kullanılmaktadır. Ancak burada kullanıcı anonimliği ile ilgili bir çalışma yapılmamıştır. İteraktif olmayan sıfır bilgi (non-interactive zero knowledge (NIZK)) (Ma et al., 2020) modelinde, akıllı sözleşmeler için işlemleri korumak için homomorfik şifreleme kullanılmıştır. İşlemleri korumada başarılı olmasına rağmen gönderici ve alıcı gizlilik hassasiyeti sağlanamamaktadır. PPchain (Lin et al., 2020), ethereum tabanlı gizliliği içeren izinli bir blok zinciri mimarisidir. İçeriğinde akıllı sözleşmeleri desteklemektedir. Herhangi bir kullanıcıdan veri yayınlayarak şifreleme kullanılmıştır. Ancak doğrulama düğümleri veri olarak görülebildiğinden, bu mimaride kısmi gizlilik gerçekleştirilmiştir. Sistemdeki kötü niyetli işlemleri izlemek için bir yönetim süreci de gereklidir. (Dwivedi et al., 2020)'de, blok zinciri tabanlı farmasötik tedarik zincir'de akıllı sözleşmelerle güvenli bilgi paylaşımını içeren bir plan önerilmiştir. (Dietrich et al., 2021)'teki çalışmada, yazarlar tedarik zinciri ile blok zincirini birleştiren son çalışmaları araştırılmış ve bu çalışmaların karmaşıklıkları sınıflandırılmıştır. (Sunmola, 2021)'te, blok zinciri üzerinde sürdürülebilir bir tedarik zincir bağlam-farkındalık çalışması yürütülmüş ve mimarisi için bir peyzaj önerilmiştir. (Helo and Shamsuzzoha, 2020)'de, lojistik ve tedarik'deki verileri izlemek için blok zinciri tabanlı bir pilot sistem tasarlanmıştır. Yakın tarihli bir başka çalışmada, (Pan et al., 2021) yazarlar, blokzincir dahil olmak üzere genel Lojistik ve tedairk zincir'de dijital birlikte çalışabilirlik konusunda ilgili alanda yazılmış belirli sayıda makalenin seçimi ve tanıtımı hakkında editoryal araştırma yürütmüşlerdir.

Tedarik zincir modelinde blokzincir teknolojisinin kullanıldığı çalışmalar incelendiğinde, izlenebilirlik ve performans iyileştirmeleri yapılmasına rağmen kullanıcı veri gizliliği hassasiyetinin dikkate alınmadığı gözlemlenmiştir. Ayrıca, aktörler ve müşteriler için denetlenebilirlik ayrıntılı olarak tartışılmamaktadır. SC'nin bütünlüğü dikkate alınarak, şeffaflık, bütünlük, denetlenebilirlik ve izlenebilirlik parametreleri üzerine yapılan araştırmalar sonucunda iyileştirmeler ve öneriler tartışılmaktadır. Ancak, güvenlik ve mahremiyetin korunmasını

dikkate alan aktörler arasında tedarik zincir bütünlüğü konusunda herhangi bir çalışma yapılmamıştır. Dahası, yapılan çalışmalar incelendiğinde var olan çoğu çözüm literatür taraması olduğu uygulamalı çözümlerin ise yeterli mahremiyet ve güvenliği sağlamadığı gözlenmiştir.

1.1.2 Tedarik zincirde izlenebilirlik

Çeşitli kurum ve kuruluşlar izlenebilirlikle ilgili araştırmalar ve tanımlar yapmışlardır. Uluslararası Standardizasyon Örgütü (International Organisation for Standardization)(ISO), izlenebilirliği "Üretim, işleme ve dağıtımın belirli aşamalarında ürünlerin hareketini takip etme yeteneği" olarak tanımlamıştır (Khan et al.,2018). Radyo Frekansı Tanımlama (RFID) kullanmak isteyen şirketler için Elektronik Ürün Kodu (EPC) küresel izlenebilirlik standardı gibi çeşitli izlenebilirlik standartları da oluşturulmuştur (Amrioui et al., 2012). Tedarik zincirde izlenebilirlik mekanizmalarının benimsenmesinin arkasındaki ana güç, özellikle FSC'de güvenlik ve kalitedir (Pizzuti et al., 2017). İzlenebilirlik, ürün geri çağırmada aktif rol oynamıştır. Aynı zamanda işlem kontrolü ve üretim optimizasyonu da geliştirilmiştir (Karlsen et al., 2011). Genel olarak, izlenebilirlik faydaları şu kategorilerde gruplanabilir: piyasa faydaları, geri çağırma maliyetinin azaltılması, sorumluluk taleplerinin ve davaların azaltılması ve süreç iyileştirme (Mai et al., 2010). Sağlam izlenebilirlik mekanizmalarının kurulması, bir şirketin marka adını korur ve titizliğini son müşterilere iletmek için bir fırsat olarak hizmet eder (Oskarsdottir and Oddson, 2019). Dahası, izlenebilirlik mekanizmaları güven oluşturur ve farklı tedarik zincir ortakları arasında uzun vadeli ilişkilerin kurulmasını teşvik eder (Memon et al., 2015).

İzlenebilirlik dahili ve harici (interal and external) olarak iki kategoride incelenmiştir. Dahili izlenebilirlik, bir şirket veya üretim tesisinde bir ürünün, bileşenlerini ve ambalajını takip etme sürecini ifade eder. Yani herhangi bir aktördeki tedarik sürecin ne zaman ve nasıl yapıldığının tanımlanması ve izlenmesini içerir. Dahili izlenebilirlik, herbir aktörün kendi içinde maliyet, üretkenlik gibi kriterlerin performansını artırmayı amaçlar. Harici izlenebilirlik ise tedarik zincirin tamamını veya bir kısmını (Vo et al., 2016) ifade eder. Yani aktörler arasında fiziksel olarak aktarılan öğelerin izlenmesini içerir. Bu sistemde,

her bir aktör diğer aktörü doğrudan izleyebilir.

1.2 Blokzincir Teknolojisi

Blok zincir teknoloji, 2008 küresel krizde Satoshi Nakamoto olarak bilinen bir kişi ya da bir grup Bitcoin olarak bilinen, matematiksel temelini ortaya koyan dünyanın ilk eşler arası (peer to peer) (P2P) elektronik ödeme sistemini oluşturdu (Nakamoto and Bitcoin, 2008). Dağıtılmış Defter Teknolojisi (Distributed Ledger Technology (DTL)) olarakta bilinen blokzincir teknolojisi kavramı, merkezi bir otoriteden herhangi bir aracılık olmaksızın değer işlemleri için dağıtılmış bir eşler arası sistem sağlamak olarak da tanımlanmaktadır. DLT'nin en belirgin türü, kökeni eşler arası kripto para birimi Bitcoin'de bulunan blok zinciridir. Bitcoin, iş kanıtı fikirbirliği algoritması ile ilk kez çift harcama sorununu çözmüştür. Burada ana fikir ise, işlemlerin ve çalışma kanıtlarının, iş kanıtını yeniden yapmadan değiştirilemeyecek sıralı bir kayda (zincir olarak da adlandırılır) hash ederek zaman damgasını eklemektir. Ağı kontrol eden ve iş kanıtını gerçekleştiren düğümler, ağa saldırmak için işbirliği yapmadıkları sürece, bu doğal sistem özellikleri, katılımcıların işlem geçmişinin doğru olduğuna güvenmelerini sağlamaktadır. Bu özelliklere dağıtılmış defter teknolojisinin “temel özellikleri” denir (Tablo 1.1)(Xu et al., 2017).

Merkezi olmayan sistem olan blok zincir teknolojisi üzerine kurulan elektronik ödeme sistemi üçüncü kuruluşları ortadan kaldırarak kişiler arasında direk para transferi yapılmasını sağladı. Getirdiği yenilik sayesinden sistem şeffaf denetlenebilir ve güven olmayan bir ortamda güveni sağlamıştır. Burada yapılan bir işlem doğruluğu geleneksel yapı olan bir banka tarafından değil de altyapıda kriptografik olarak çalıştırılan bir sistem sayesinde ispatlanmıştır. Birçok banka, ticaret finansmanı ve uluslararası ödemeler için blok zinciri uygulayan küresel konsorsiyum şirketler dahil olmak üzere birçok şirket blok zinciri teknolojisi denemelerine katılmaktadır. Bir blokzincir servisi sağlayıcısı olarak Microsoft Azure ve IBM, ekosisteminin hızlı gelişimini, blok zinciri teknolojisine olan geniş ilginin altını çizmektedir. Bu teknoloji, merkezi olmayan uygulamalar oluşturmak ve birlikte çalışabilirliği sağlamak için açık bir altyapı haline gelmiştir. Bir blok zincirindeki tüm işlemler, ağdaki tüm tarafların sahip olduğu dağıtılmış bir

defterde saklanır. Sistemin o anki durumu benzersiz bir şekilde genel muhasebe tarafından belirlenir (Zheng et al., 2018). Blokzincir teknolojisi, 2008 yılında Satoshi Nakamoto tarafından "uçtan uca elektronik ödeme sistemi" adlı makele ile ortaya çıkan Bitcoin'in temelini oluşturan sistemdir (Nakamoto and Bitcoin, 2008). Bu teknoloji güven olmayan ortamda bize güveni sağlayan, merkezi otoriteye gerek duymadan merkezi olmayan bir sistemi mümkün kılar. Sistemde yapılan bir işlemin ispatı kriptografik protokoller ile kanıtlanır. Blokzincir teknolojisinin ana noktaları şunlardır:

(I) merkezi olmayan bir sistem,
(II) verilerin değiştirilemezliği,
(III) güven olmayan bir ortamda güven sağlanması (Guegan, 2017)

Tablo 1.1 Dağıtık Defter Teknolojisinin Temel Özellikleri

Temel Özellik	**Açıklama**
Değişmezlik	İşlemler eklendikten sonra defter değiştirilemez.
Reddedilemezlik	Her işlem, deftere yalnızca bir kez eklenir.
Bütünlük	Verilerinin eksiksiz olduğu ve deftere ilk yazıldığı gibi doğrulanabilir.
Şeffaflık	İşlemler ve veriler herkes tarafından görülebilir.
Eşit Haklar	Herkesin işlemleri okuma ve yazma imkânı vardır.

Özetlemek gerekirse, DLT'nin temel özellikleri, işlem yapan taraflar ve cihazlar arasında güven inşasının yanı sıra işlemlerin uzlaşma süresini artırma ve aracılarla ilişkili maliyetleri azaltma potansiyelini sağlamaktır. Akıllı sözleşmelerle birlikte, blokzincir teknolojisinin toplum ve endüstrideki potansiyel uygulamaları çok çeşitlidir. Finansal hizmetler, sigorta ve tedarik zinciri gibi sektörler, Bu sektörlerin nasıl etkileşime girdiği ve işlem yaptığı konusunda gelecekte oyunun kurallarını değiştireceğini öngörüyor. Bu teknolojiyi kullanan gelecekteki eşler arası etkileşimler ve süreç otomasyonu, geleneksel uygulamalara kıyasla daha güvenilir ve şeffaf olabilir. Blokzincir tekolojisi kriptopara

sistemlerinde başarıyla kullanılmasından sonra, bu teknolojinin farklı alanlarda da kullanılabilitesi için birçok başarılı araştırma yapılmıştır. Yapılan araştırmalar öncelik işlem gizliliği üzerine olmuştur. Yani mevcut merkezi olmayan sistemlerden farklı olarak finansal işlemlerin blokzincirde saklanamayacağı ve işlem gizliliği açık bir şekilde korunur görüşü yapılmıştır (Kosba et al.,2016).

Bu teknoloji izinli ve izinsiz blok zincir (Permissioned-Permissionless blockhain) olarak 2 kısımdan oluşmaktadır.

1.2.1 İzinsiz Blokzincir

Bitcoin (Nakamoto and Bitcoin, 2008) ve Ethereum (Buterin, 2014), açık ve merkezi olmayan izinsiz blok zincir (permissionless blokzincir) örnekleridir. İzinsiz blok zincir de bir akran (peer), ağa herhangi bir zamanda okuyucu ve yazar olarak katılabilir ve ayrılabilir. Ayrıca, sistemi yöneten veya yasaklayabilecek merkezi bir varlık yoktur. Bununla birlikte, Zerocash (Li et al., 2006) örneğinde olduğu gibi kriptografik protokoller ile, gizlilikle ilgili bilgileri gizleyen izinsiz bir blok zinciri tasarlamak teknik olarak mümkündür.

1.2.2 İzinli Blokzincir

Burada, merkezi bir varlık, bireysel eşlerin blok zincirinin yazma veya okuma işlemlerine katılma hakkına karar verir. Gizlilik sağlamak için, okuyucu ve yazar ayrıca birbirine bağlı ayrı paralel blok zincirlerinde de çalışabilir. İzin verilen blok zincirlerinin (permissioned blokzincir) en yaygın bilinen örneği Hyperledger Fabric ve R3 Corda'dır (Akkerman et al., 2010).

2. GEREÇ VE YÖNTEM

Bu bölümde çalışmamızda kullanılan tekniklerin içerikleri ve özellikleri tartışılacaktır.

2.1 Kriptografik Yapılar

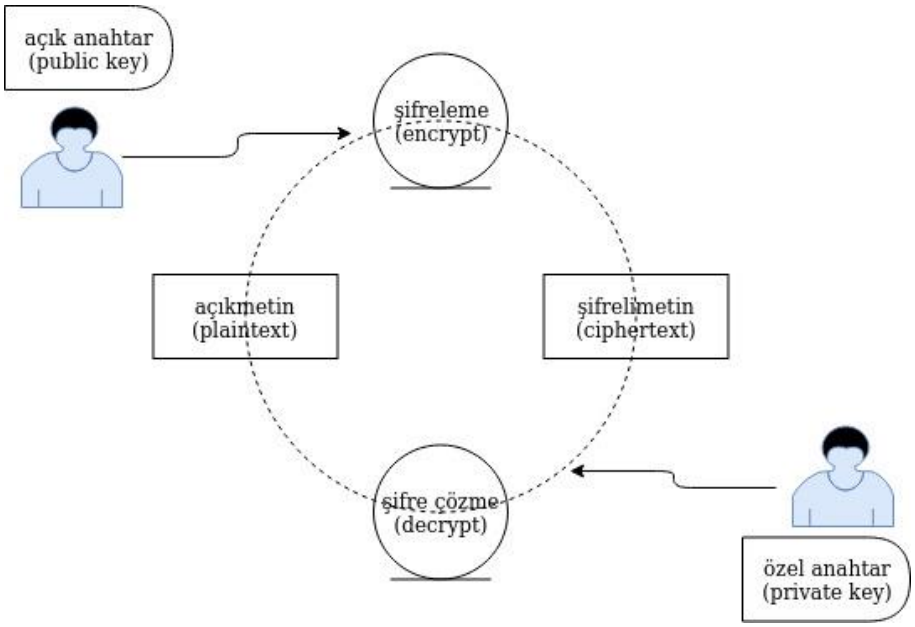
Bu bölümde çalışmamızda kullandığımız kriptografik yapıları ve bunların özellikleri açıklanmıştır.

2.1.1 Kriptografik Şifreleme Sistemleri

Kriptografik şifreleme simetrik (symmetric) ve asimetrik (asymmetric) şifreleme sistemi olarak iki kısımdan oluşmaktadır. Simetrik şifrelemede aynı anahtar hem şifrelemede hem de şifre çözmede kullanılır. Asimetrik şifrelemede ise bir açık anahtar bir özel anahtar vardır. Şifreleme ve şifre çözmede farklı anahtarlar kullanılır (Simmons, 1979)

Simetrik şifrelemede k anahtar olarak tanımlarsak E_k şifreleme olarak gösterilir ve bir c şifreli metin elde edilir. Yani $c=E_k(m)$ olarak gösterilir. Yine aynı k anahtarını kullanarak bir c şifresinin çözmesi ise D_k, yani $m=D_k(c)$ olarak gösterilir.

Asimetrik şifrelemede bir pk açık anahtar (public key) birde sk özel anahtar (private key) çifti vardır. Herhangi bir A kişisi mesaj göndermesi için kendisine verilen pk açık anahtar ile m mesajını şifreler. Oluşan c şifresi $c=E_{pk}(m)$ ile gösterilir. Şifreli c mesajının çözülebilmesi için sk özel anahtarı kullanılarak m mesajı elde edilir ve $m=D_{sk}(c)$ ile gösterilir (şekil 2).



Şekil 2.1 Açık Anahtar Şifrelemesi

Bu tez çalışmasında digital imza ve doğrulamada asimetrik şifreleme sistemi olan Eliptik Eğri Kriptografi (Elliptic Curve Cryptography) (Miller, 1985) kullanılmıştır. Daha küçük anahtar boyutu ile RSA açık anahtar şifrelemesine göre eşit düzeyde güvenlik ve performans sağladığı için tercih edilmiştir.

2.1.2 Eliptik Eğri Kriptografisi

Eliptik eğri kriptografisi (Elliptic Curve Cryptography), temelinde açık anahtar şifreleme sistemi yapısında olan ve trapdoor fonksiyonuna dayanan alternatif olarak oluşturulmuş bir şifreleme sistemidir. Yani sonlu alanlar üzerindeki eliptik eğrilerin cebirsel yapılarına dayanmaktadır (Miller, 1985). Diffie-hellman (Boneh, 1998) ve RSA gibi şifreleme yapılarının zorluğu asal çarpanlara ayırma (prime factorization) çözümü zorluğuna dayanmaktadır. Asal çarpanlarına ayırma zorluğu Trapdoor fonksiyon yapısını anlatan örnek bir çalışmadır diyebiliriz.

Tanım: *Eliptik eğri aşağıdaki denklem ile tanımlanan bir düzlem eğrisidir.*

$$y^2 = x^3 + ax + b, \text{ burada } (x, y) \in Z_p \qquad (2.1)$$

Eliptik bir eğri üzerindeki aritmetik işlemleri ve bir anahtar çiftinin oluşturulmasını tanımlamamız gerekmektedir.

Öncelikle eğri üzerinde *(p,q)* iki nokta arasında temel işlemlerden toplama işlemi yapılır ve *r* oluşan üçüncü nokta yine eğri üzerindedir *(r=p+q)*. Bu işlem aşağıdaki formül ile gösterilmektedir.

$$\begin{aligned} \lambda &= (y_q - y_p)/(x_q - x_p) \\ x_r &= \lambda^2 - x_p - x_q \\ y_r &= \lambda (x_p - x_r) - y_p \end{aligned} \qquad (2.2)$$

Ancak aşağıdaki formül ile gösterilen, eğri üzerinde özel durum olarak noktanın kendi üzerinde toplanmasıdır (double point).

$$\lambda = (3x_p^2 + a)/(2y_p) \qquad (2.3)$$

Buradaki aritmetik işlemlerin basitliğine rağmen, çözülmesinin ve hasaplanmasının bir o kadar zorluğu aşikârdır. Herhangi bir saldırgan ilgili noktadaki açık anahtarı bilmesi, sistemi çözmesine yeterli olmamaktadır. Başlangıç noktasındaki yeri ve çarpanı bilmesi gerekmektedir. Bu değerleri bulabilmesi için bütün değerleri denemesi gerekmektedir. Eğer saldırgan başlangıç noktasını bilse bile bu değerleri elde edebilecek çarpanı bulması için açık anahtar olan noktadan bulduğu başlangıç noktasına kadar değerleri çıkarması gerekmektedir. Burada eğri üzerindeki herhangi bir *q* noktası açık anahtar (public key) , bir diğer nokta sabit *g* noktası "generator point" dır. Sabit *g* noktanın çarpımı olan bir *k* çarpanı ise özel anahtar (private key) dır (Tablo 2.1).

Tablo 2.1 Eliptik Eğri Üzerinde Açık- Özel Anahtar Çifti

Özel anahtar (private key)	$k, \quad k \in R\ [1, n - 1]$
Açık anahtar (public key)	$q \leftarrow kg$, *g sabit nokta*
Açık- özel anahtar çifti (public-private key pair)	(q,k)

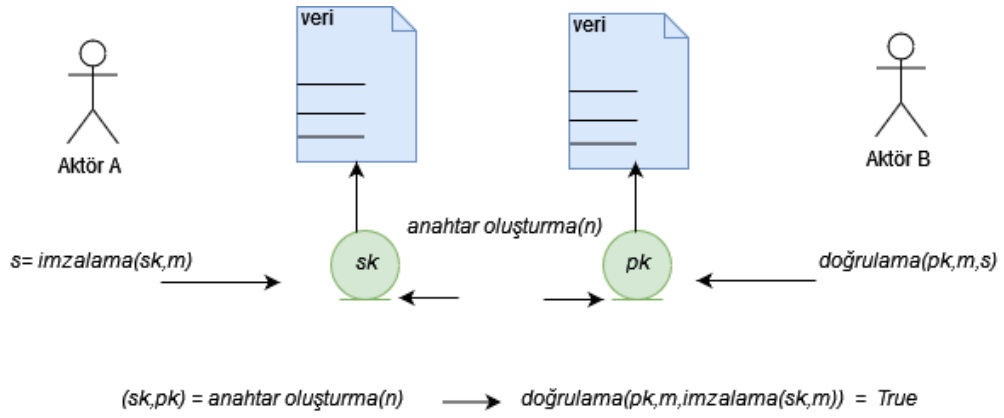
Dolayısıyla eliptik eğri güvenliği zor bir problem (NP-hard) olarak kabul edilen ayrık logaritma (discrete logarithm) problemi çözmenin zorluğuna dayanmaktadır (Naor, 2003).

2.1.3 Dijital İmza

Dijital imza (digital signature), kaynak doğrulama ve veri bütünlüğü hizmetlerini sağlayan ve imzalayanın reddedilmemesini destekleyebilen verilerin kriptografik dönüşümü olarak tanımlamaktadır. Yani dijital ortamda bulunan verilerin ve/veya belgelerin geçerliliğini göstermek için matematiksel temellere dayanan şekillerdir. Kimlik doğrulama, inkâr etmeme ve bütünlüğü sağlayan, asimetrik kriptografi kullanımı ile mümkün hale gelen yapıdır da diyebiliriz.

Dijital imzaların iki yönü vardır. bir belgenin bütünlüğünü garanti ederler. İkinci olarak, gerçekliği garanti ederler. Bir dijital imza, bir sertifika yetkilisi kullanılarak belirli bir kişi veya kuruma kadar izlenebilir. Bu şekilde, belgenin belirtilen yazar tarafından oluşturulduğundan ve belgenin yasal olarak bağlayıcı bir sözleşme olarak kullanılabileceğinden emin olunabilir. Digital imzanın birinci tarafı zamandan bağımsızdır. Yani söz konusu belgenin hash değerini yeniden hesaplayarak ve bunu dijital imzadaki ile karşılaştırarak her zaman ilgili belgenin uygun imzaya sahip olduğu doğrulanabilir. Bununla birlikte, ikinci durum zamana bağlıdır. Çoğu dijital sertifikanın süresi dolar ve sahipleri, yani belge oluşturanlar tarafından yenilenmedikçe onaylanamaz. Ayrıca, hala faaliyette olan sertifika yetkilisi kurumlarına da güveniyorlar. Bazı sertifika yetkililerinin iflas edebileceği veya kapanabileceği düşünülebilir. Bu gerçekleştiğinde, sertifikalarının gerçek olduğunu onaylamak imkânsız olacaktır. Şu anda çoğu arşiv, eski dijital imzaların

doğrulanması için güvene dayanmaktadır. İmzanın arşivleme sırasında geçerli olduğuna ve belgenin tahrif edilmediğine dair belgeyi koruyan arşive (veya başka bir kuruma) güvenmek gerekir. Dolayısıyla üçüncü kuruluş olmadan güven mekanizmasının işlenmesi gerekmektedir.



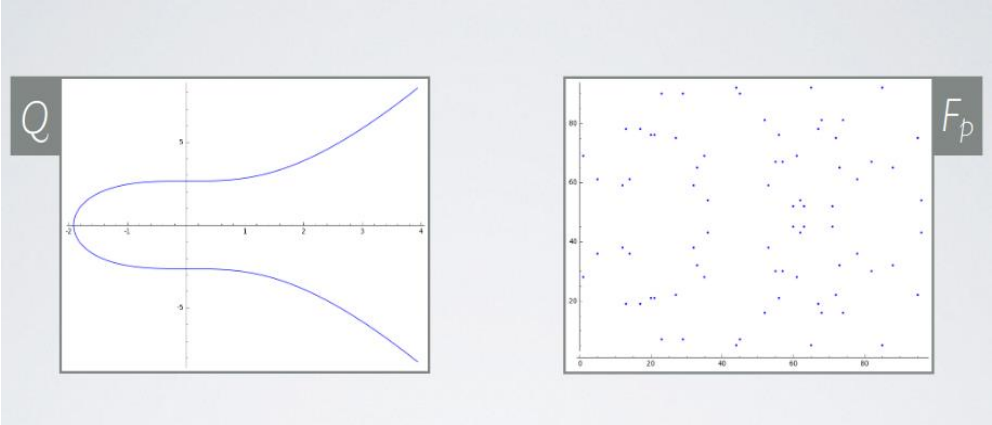
Şekil 2.2 Dijital İmzalama

Dijital imzada, bir *m* mesajı ilk önce güvenli bir tek yönlü fonksiyon (one-way) kullanılarak *h* hash değeri alınır. *h* daha sonra imzalayanın özel anahtarı *(sk)* ile birlikte imzalama algoritmasında dijital bir imza oluşturmak için kullanılır. Doğrulamada ise, aynı hash algoritması kullanılarak m yeniden hash alınır ve h^I elde edilir. Doğrulama algoritması, orijinal dosya hash elde etmek için imzalayanın (*pk)* açık anahtarı kullanılarak gerçekleştirilir ve h^I, *h*-'ye eşitse işlem başarılıdır (Şekil 2.2).

Tez çalışmasında Tablo 2.2 'de gösterdiğimiz eliptik eğri dijital imzalama algoritması (elliptic curve digital signature algorithm (ECDSA)) kullanarak bir imzanın oluşturulması parametreleri gösterilmiştir.

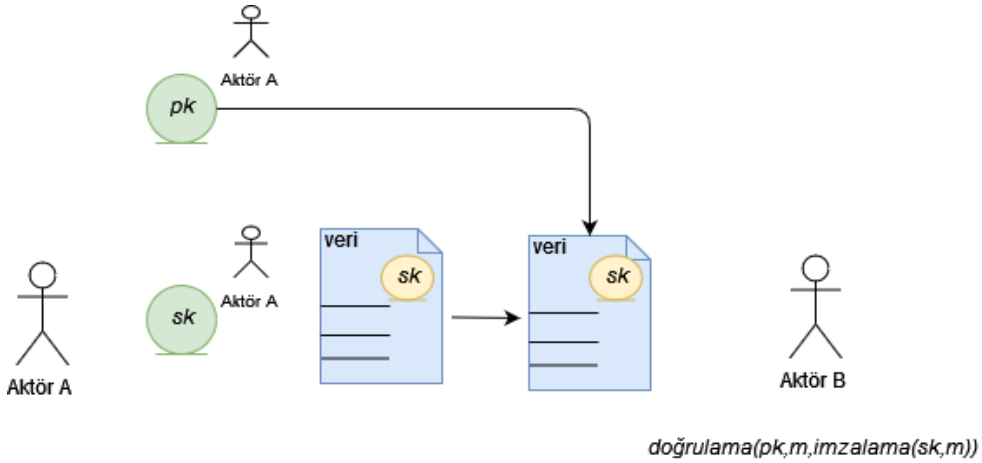
Tablo 2.2 Eliptik Eğri Digital İmzalamada Kulanılan Parametreler

Parametreler	Format	Aralık (Range)	Anahtarboyutu (Bit-size)
sk	*random*	*Zq*	*256*
pk	*sk x G*	*E(Fp)*	*512*
m	*hash(M)*	*Zq*	*256*
Sign	*(r, s)*	*Zq x Zq*	*512*



Şekil 2.3 Eliptik Eğri *Q Ve* F_p Gösterimi

ECDSA blok zincirde *E(Fp) : { (x,y) in Fp x Fp | y2 = x3 + 7 }*, denkleminde a=0, b=7 dir ve secp256k1 olarak kullanılır. Burada *G* eliptik eğri taban noktası (generate point) olup, secp256k1 de *p* asal sayısı p = 2^{256}-2^{32}-2^9-2^8-2^7-2^6-2^4-1, şekil 2.3'te görüldüğü üzere Fp karmaşık nokta yığını secp256k1 de istenilen tüm özellikleri barındırır. Şekil 2.4 ise eliptik eğri dijital imzalama uygulaması gösterilmiştir.



Şekil 2.4 Eliptik Eğri Dijital İmzalama Algoritması Uygulanması

2.2 Blokzincir Teknolojisinin Altyapısı

Nakamoto'nun blok zinciri ile çözdüğü sorun, dağıtılmış bir sisteme güven oluşturmaktır diyebiliriz. Daha spesifik olarak, hiçbir tarafın verinin içeriğini veya zaman damgalarını (timestamps) algılamadan kurcalayamayacağı, zaman damgalı belgelerin dağıtılmış bir deposunu oluşturma sorunudur. Bu sorunun, dijital imza ile kimlik doğrulama, bütünlük ve reddedilmeme sorunlarına bir çözümdür diyebiliriz. Bir taraf bir belge için dijital imza oluşturursa, taraf ile belge arasında yalnızca doğrulanabilir bir bağlantı kurulmaktadır. Geçerli bir dijital imzanın varlığı, tarafın gerçekten belgeyi imzalamayı amaçladığını ve belgenin değiştirilmediğini kanıtlar. Yine de dijital imza, belgenin imzalandığı zamanla ilgili hiçbir şeyi garanti etmez: zaman damgası, onu imzalayan tarafa güvenmeyi gerektirir. Mali işlemler ve diğer yasal sözleşme biçimleri söz konusu olduğunda, zaman esastır ve bu mali işlemlerin sırasının denetlenebilir olması için bağımsız olarak onaylanması gerekir. Bitcoin örneğinden yola çıkalım, bir bitcoin birimi bir sayıdır, ancak yalnızca bazı sayılar geçerli bitcoinlerdir diyebiliriz. Bu sayılar iyi tanımlanmış bir denklemin çözümleridir ve yeni bir çözüm bulan ona sayıya sahip olur. Bu aşamaya madencilik denilmektedir. Biraz daha detaylandıracak olursak; Bir bitcoin bulunduktan sonra, defterde saklanan işlemlerle takas edilebilirdir. İşlemler, inkâr edilemezliği (nonrepudiation) önlemek için satıcının kimlik bilgileriyle dijital olarak imzalanır. Kullanıcılar bir deftere güvenmeyeceğinden ve hepsini tek bir yerde depolamak için çok fazla işlem olduğundan, merkezi bir

defter yoktur. Bu nedenle, bitcoin ve diğer kripto para birimleri, belirli bir madeni paranın (coin) (veya bir madeni paranın bir kısmının) işlemine dahil olan her bilgisayarın o madeni paranın işlemlerinin geçmişinin bir kopyasını tuttuğu dağıtılmış bir defter sağlamaktadır. Blokzincir teknolojisi, bu geçmişi saklayan hiçbir tarafın tespit edilmeden bulunmamasını sağlamaktadır.

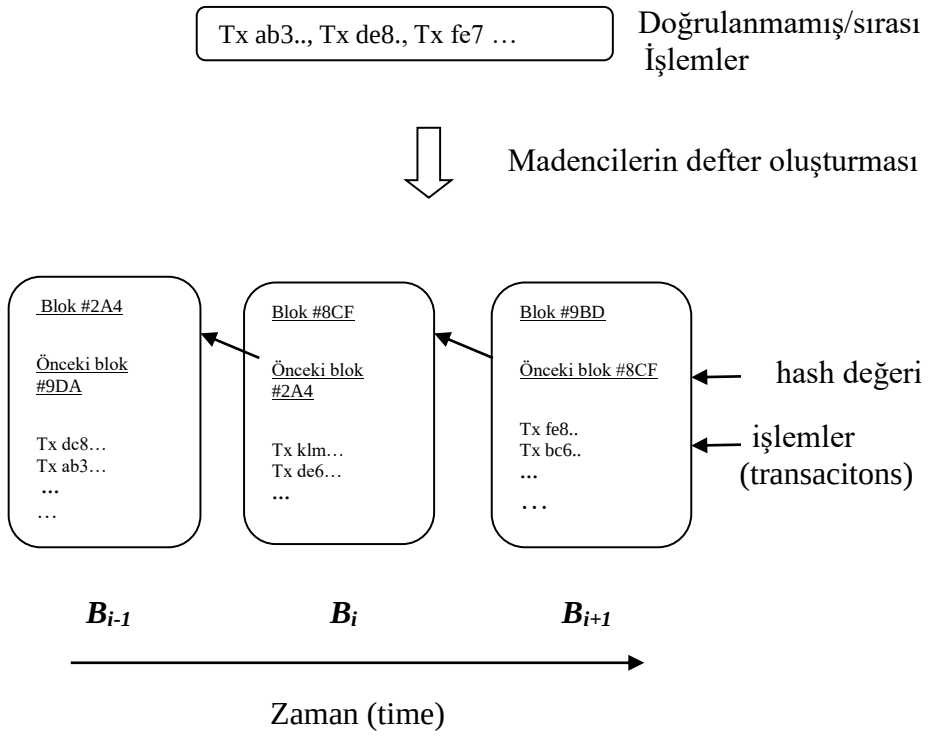
2.2.1 Blok Oluşumu

Blok zincir teknolojisinin başarılı olarak çalışan örneği olan Bitcoin'nin yapısına bakarak blok oluşumunu incelemekteyiz. Bitcoin de madenciler olarak adlandırılan node lar yeni bloklar oluşturur ve kriptografik bulmacaları çözerek ağdaki zincire ekler; bu süreç iş ispatı (proof of work (PoW)) olarak bilinir (Nakamoto and Bitcoin, 2008). Bloklar, kanıt sağlayan değişmez zaman damgalarını içerir. Önceki blok bilgileri doğrulanmazsa, yeni bloklar mevcut zincirin yeni parçalarını oluşturamaz ve reddedilir. Sonuç olarak, ağ üzerinde yapılan her işlemin şeffaf ve dağıtılmış bir muhasebe defteri bizlere bu güveni verir (Şekil 2.5). İşlemler, işlem ayrıntılarını ve bir zaman damgasını içeren veri birimleridir. Blok zinciri, her satırın ayrı bir işlemi temsil ettiği, ilk sütunun işlemin zaman damgasını, ikinci sütunun işlemin ayrıntılarını ve üçüncü sütunun mevcut işlemin bir karmasını sakladığı üç sütunlu bir tablo olarak düşünülebilir. Bir blok zincirine yeni bir kayıt eklendiğinde, hesaplanan son hash tüm ağda yayınlanır (broadcasted). Ağdaki her node sahibinde tüm işlem geçmişinin bir kopyasını tutması gerekli değildir - birkaç tarafın tutması yeterlidir. Herkes son hash bildiği için, farklı ve dolayısıyla geçersiz bir hash elde etmenin imkânsız olacağından, herkes verilerin değiştirilmediğini doğrulayabilir. Hash değerini korurken verileri değiştirebilmenin tek yolu verilerde bir çakışma (collusion) bulmaktır ve bu hesaplama açısından imkânsızdır. O kadar çok bilgi işlem gücü gerektirir ki, pratikte ekonomik değildir.

Matematiksel olarak, iki önemli özelliği olması gereken bir *f* fonksiyonu tarafından bir hash üretilir: girdi uzayının ve çıktı uzayının boyutu büyük olmalıdır; çakışmaları, yani aynı çıktıyı $f(x_1)=f(x_2)$ üreten x_1 ve x_2 girdilerini bulmak pratikte imkânsızdır. Hash işlevlerinin tipik bir uygulaması, parola depolamadır - bir web sitesine kaydolduğunuzda, sitenin parolanızı kendi

veritabanında saklamasını istemezsiniz, aksi takdirde, veritabanına erişimi olan herkes onu okuyabilir. Web sitesi, *f(p)=y* parolasının hash değerini saklamalıdır. Giriş yaptığınızda, giriş şifresi *p* tekrar hashlenir ve saklanan değer olan *f(p)=y* ile karşılaştırılır. Gerçek parola ile aynı *y* hash değerini üreten yanlış bir parola bulma olasılığı sıfırdır.

Hash fonksiyonlarına örnek olarak, güvenli hash algoritmaları (SHA1, SHA128, SHA256 SHA512 vb.) verilebilir. Herhangi bir dizeyi girdi olarak alınır ve her zaman işlevin çıktı numarasının sabit sayıda basamaklı onaltılık gösterimi olan bir çıktı dizesi üretilir.



Şekil 2.5 Zaman Damgası (Timestamps) ve Değişmezliği (İmmutability)

Bu yapıyı incelediğimizde; İlk n-bit 0 olacak şekilde 256 bit hash değeri (Dhumwad et al., 2017) için madenciler iş ispatı yaparak verileri bloklara ekler. Bulunan özel hash değeri için geçen zaman ise (timehold) 2^n dir. Her bir blok oluşumu için ortalama geçen süre ise 10 dakikadır.

Tanım 1*: İlk n bit sıfır 0 olacak şekilde elde edilen 256 bit hash değeri ile (PoW), önceki bloğun hash değerinden elde edilen yeni blok oluşumunda geçen zaman;* 2^n *den küçüktür (* Sezer ve Nuriyev, 2020).

$$H_{ab}=H(H_a, H_b)$$

$$H_a=SHA256(Tx_a) \qquad H_b=SHA256(Tx_b) \qquad \text{Merkle Ağacı} \quad (2.4)$$

$$H(B_i)= H(N,Tx_{1,\dots}\ Tx_n, H(B_{i-1})) < Timehold = 2^n \sim 10\ dak. \qquad (2.5)$$

Burada B_i blok, N nonce değeri, H hash, Tx_n değeri işlem (transaction) geçen zaman ise *Timehold* dur.

Blokzincir teknolojisi, kötü amaçlı yazılımlara ve bilgisayar korsanlarının saldırılarına karşı geleneksel bilgi teknolojileri altyapılarından çok daha sağlam ve daha az zayıf yönleri vardır. Tablo 2.3' de, izinsiz ve izin verilen blokzincir' nin bazı özellikleri ve merkezi bir veri tabanı karşılaştırılmıştır. Merkezi bir sistemde, gecikme (latency) ve verim açısından performans genellikle blokzincir sistemlerinden çok daha iyidir, çünkü blokzincir sistemi mutabakat mekanizması aracılığıyla ek karmaşıklık katmıştır. Örneğin, Visa gibi merkezi bir sistem saniyede 2000-3000 den fazla işlemi işleyebilirken, Bitcoin şu anda saniyede yaklaşık yedi işlem gerçekleştirebiliyor.

Tablo 2.3: İzinsiz, İzin Verilen Blokzincir Ve Merkezi Bir Veri Tabanı Karşılaştırılması (Peck, 2017)

	İzinsiz (Permissionless) Blokzincir	**İzinli (Permissioned) Blokzincir**	**Merkezi Veritabanı (Central Database)**
Verimlilik (Throughput)	Düşük	Yüksek	Çok Yüksek
Gecikme (Latency)	Düşük	Orta	Hızlı
Güven Vermeyen (Untrusted) Yazıcı Sayısı	Yüksek	Düşük	Yok
Mutabakat (Consensus)	PoW, Bazı PoS	BFT Protokolü (PBFT [19])	Yok
Merkezi Yönetim	Hayır	Evet	Evet

Blok zincirin teknik sınırlamaları vardır. Bir blok zinciri hakkındaki bilgiler tüm katılımcılara açık olduğu için gizlilikten etkilenmektedir. Verim ölçeklenebilirliği için, genel açık blok zincirler saniyede yalnızca ortalama 3-20 işlemi işleyebilirken, VISA gibi ana ödeme hizmetleri saniyede ortalama 1.700 işlemi işleyebilirdir. Bir yazılım bağlayıcısı olarak blok zinciri, karmaşık bir içyapıya sahiptir ve birçok konfigürasyona ve varyanta sahiptir (Xu et al., 2016). 2008'de Bitcoin'in ortaya çıkışından bu yana, çok çeşitli blok zincirleri ortaya çıkmıştır. Bu nedenle, blok zincirler, örneğin gerçek zamanlı uygulamalarda tüm kullanım senaryolarının gereksinimlerini tek başına karşılayamaz. Blok zincirlere dayalı uygulamalar oluştururken, blok zincirlerinin özelliklerini ve konfigürasyonlarını sistematik olarak göz önünde bulundurmamız ve bunların genel sistemler için kalite nitelikleri üzerindeki etkilerini değerlendirmemiz gerekir. Uygulamada, güvenilir teknoloji değerlendirme kaynaklarının eksikliği karşılaştırmayı çok zorlaştırmaktadır.

2.2.2 Fikir birliği protokolleri

Blokzincir teknolojisinde, yeni bir blok oluşturma, merkezi bir düğüm yerine birden çok düğümün (node) bir araya gelerek fikir birliği (consensus)

sonrasında ortaya çıkmaktadır. Burada fikir birliği sürecine dâhil olan tüm temel yapılar, eşler arası (peer-to-peer network (P2P)) ağlarını ve fikir birliği protokollerini içermektedir. Eşler arası ağ, görevleri ve iş yüklerini eşler arasında tahsis etmek için dağıtılmış bir uygulama mimarisidir (Schollmeier, 2001). Bu ağda merkezi bir yetkili düğüm yoktur ve ağdaki düğümler, yeni düğümlerin keşfi, ağın yönlendirilmesi ve ağda yayılan verilerin doğrulanması gibi görevleri üstlenmektedir. Bu özelliğe dayanarak, blok zincir teknolojisi fikir birliği sürecine katılmak ve farklı fiziksel konumlardaki düğümleri birleştirmek için eşler arası ağını kullanmaktadır. Ağın merkezi olmayan ve düğüm adreslerinin yapısal olup olmadığına bağlı olarak, merkezileştirilmiş, merkezi olmayan yapılandırılmamış, merkezi olmayan yapılandırılmış ve yarı dağıtılmış eşler arası ağ olmak üzere dört kategoride incelenmektedir. Son üç kategori, Bitcoin, Ethereum ve Hyperledger Fabric blok zinciri platformları tarafından benimsenmiştir.

Blok zincirdeki her bir düğüm'ün aynı durumda olması ve üzerinde anlaşabilmesi için sistem üzerinde bir fikir birliğine varılması gerekmektedir. Düğümlerin durum geçişini nasıl işlediğini tanımlayan algoritmaya fikir birliği denir. Bir fikir birliği algoritmasının 3 temel özelliği bulunmaktadır (Baliga, 2017).

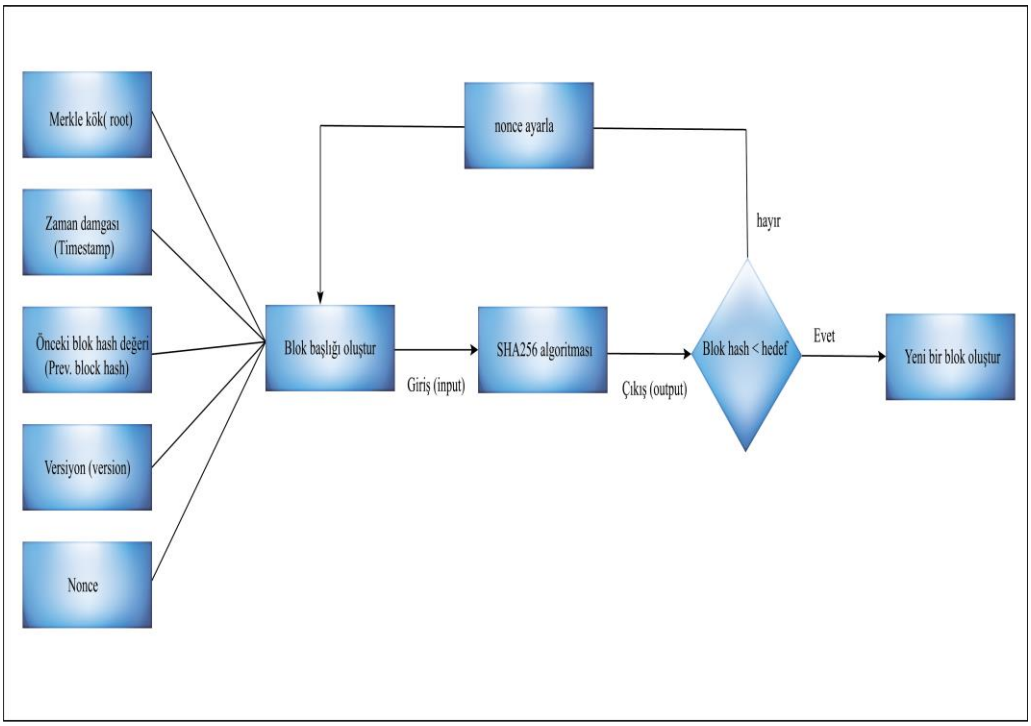
1. Güvenlik (security): Tüm düğümler, blok zincirinin tutarlı bir durumunu sağlayarak geçerli çıktılar üretir.
2. Süreklilik (liveness): fikir birliğine katılan tüm hatalı olmayan düğümler sonunda bir çıktı üretir.
3. Hata toleransı (fault tolerance): protokolün kendini fikir birliğine katılan bir düğümün başarısızlığından kurtarılması.

Dağıtık sistemlerde mükemmel bir fikir birliği protokolü yoktur. Fikir birliği protokolünün tutarlılık (consistency), kullanılabilirlik (availability) ve bölüm hata toleransı (partition fault tolerance) (CAP) arasında bir değiş-tokuş (trade-off) yapması gerekmektedir (Gilbert and Lynch, 2002). Ayrıca, fikir birliği protokolünün, fikir birliği sürecini kasıtlı olarak baltalayan bazı kötü niyetli düğümlerin olacağını ve bunun içinde var olan protokollere ek Bizans Generalleri Problemini de ele alınması gerekmektedir (Akkerman et al., 2010). Fikir birliği

protokolünde iş kanıtı, hisse kanıtı (Proof-of-Stake (POS)) ve Bizans Hata Toleransı (Practical Byzantine Fault Tolerance) olarak üç temel protokol bulunmaktadır.

İş kanıtı

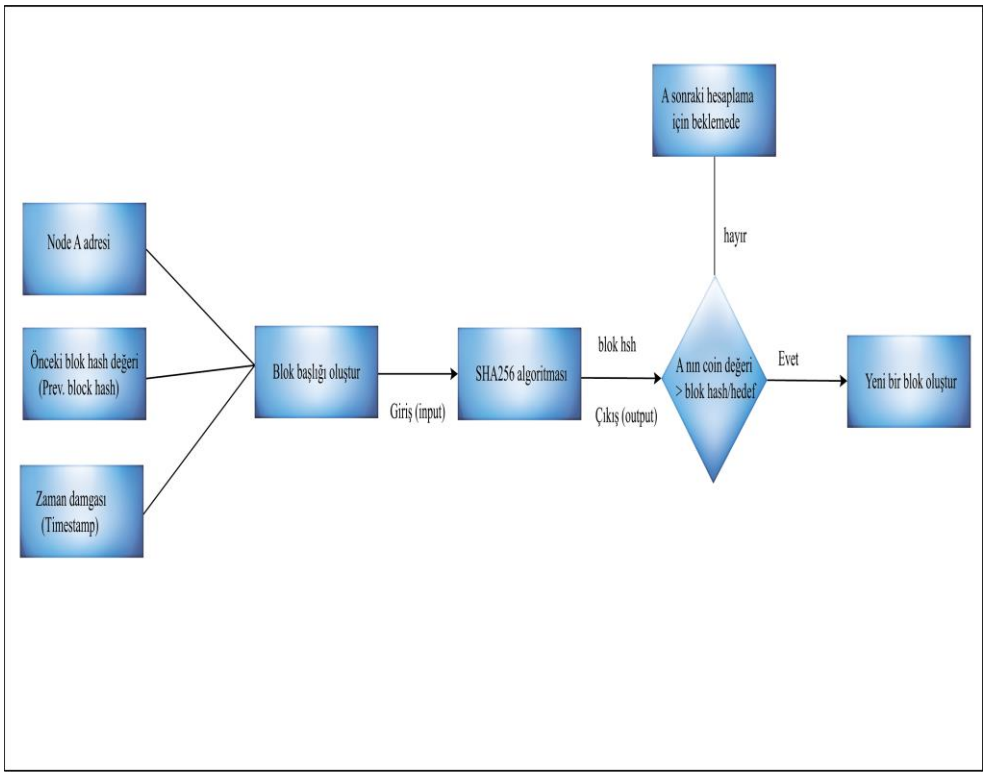
Adından da anlaşılacağı üzere, PoW algoritması, yaptıkları işi kanıtlamak için CPU/GPU kaynaklarını kullanan düğümlere dayanmaktadır. Bir bloğun oluşturulmasında, nonce veri alanı dışındaki tüm veri alanları statiktir. Bloğun geçerliliğini kanıtlamak için, nonce değeri üzerinden bloğun hash değeri hesaplanır. Protokolde tanımlandığı gibi zorluk koşulu sağlandığında blok geçerlidir denir. Bloklar geçerli olduğu kanıtlandıktan sonra önceki bloklara bağlı olduğundan dolayı pratikte değişmezdir. Burada PoW, hesaplamalı güç rekabeti ile her fikir birliği turunda yeni bir blok oluşturmak için bir düğüm seçer. Yarışmada, katılan düğümlerin bir kriptografik bulmacayı çözmeleri gerekiyor. Bulmacayı ilk ele alan düğüm, yeni bir blok oluşturma hakkına sahip olabilir (Şekil 2.6). Bir B bloğunun içeriğini değiştirmek isteyen kötü niyetli kişi, B bloklarının tüm çalışma kanıtını en son bloğa kadar yeniden yapmak zorunda kalacaktır. Bu durum, önemli miktarda kaynak gerektirecektir ve ekonomik olarak uygun olmadığı da ispatlanmıştır.



Şekil 2.6 İş Kanıtı Akışı

Hisse kanıtı

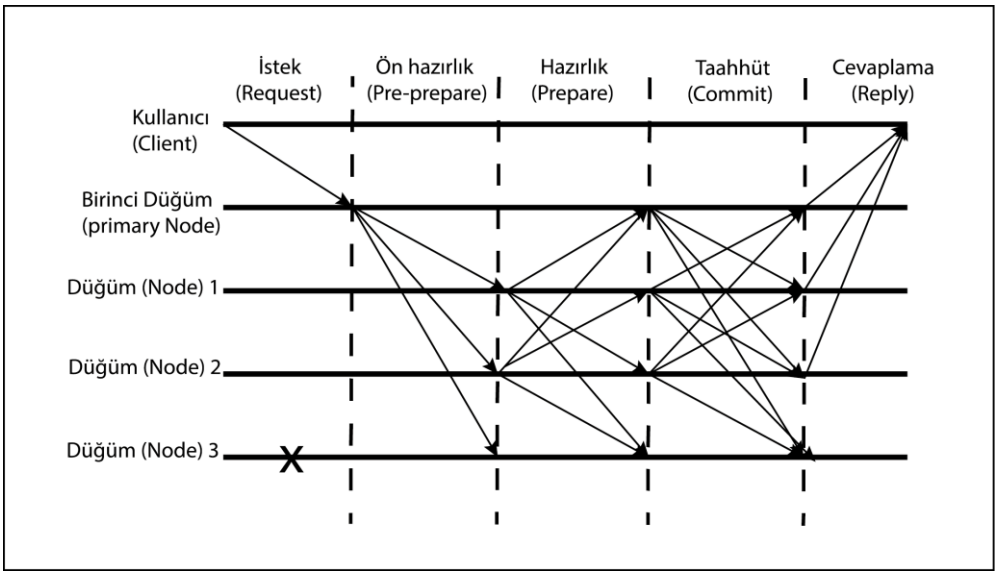
PoW algoritmasının aksine, bir PoS algoritması, kullanıcıların blokların geçerliliğini belirlemek için bir miktar kripto para birimini stake ederek doğrulayıcı olarak hareket etmesini sağlar (Van Wingerde, 2017). Yani PoS'ta, yeni bir blok oluşturan düğümlerin her turunu seçmek, hesaplama gücünden ziyade elde tutulan hisseye bağlıdır. POS algoritmasında, doğrulayıcılar fonlarını bir adrese kilitler ve algoritma periyodik olarak (örneğin her on saniyede bir) hangi doğrulayıcının yeni bir blok oluşturma hakkı kazandığını belirler (Şekil 2.7). PoS'un PoW'a göre en büyük avantajı, PoS ile madenciliğin fiziksel değil sanal olmasıdır. PoS, işlerini kanıtlamak için elektrik tüketen donanıma sahip olmak yerine, kullanıcıların sanal para birimlerini paylaşmalarına izin verir. Bu nedenle PoS, fikir birliğine varmak için çok fazla hesaplama gücü tüketmek yerine dâhili para teşvikinin bir yolunu kullanan, enerji tasarrufu sağlayan bir fikir birliği protokolüdür. 'Paydaşlar' PoS ile önemli ölçüde daha az elektrik kullandıklarından, ağın enflasyonunu azaltan blok ödülleri şeklinde katılmak için daha az teşvike ihtiyaç duyarlar.



Şekil 2.7 Hisse Kanıtı Akışı

Bizans Hata Toleransı

PBFT, dağıtık sistemlerde düşük algoritma karmaşıklığına ve yüksek pratikliğe sahip bir Bizans Hata Toleransı protokolüdür (Castro and Liskov, 1999). PBFT beş aşamadan oluşur: istek (request), ön hazırlık (pre-prepare), hazırlık (prepare), taahhüt etmek (commit) ve cevaplama (reply). Şekil 2.8 PBFT'nin nasıl çalıştığını açıklamaktadır. Birincil düğüm, istemci tarafından gönderilen mesajı diğer üç düğüme iletir. Düğüm 3'ün çökmesi durumunda, bu düğümler arasında bir fikir birliğine varmak için bir mesaj beş aşamadan geçer. Son olarak, bu düğümler istemciye yanıt vererek bir konsensüs turunu tamamlar. PBFT, düğümlerin ortak bir durumu korumasını ve her konsensüs turunda tutarlı eylemde bulunmasını garanti eder. PBFT, güçlü tutarlılık hedefine ulaşır, bu nedenle bir mutlak kesinlik konsensüs protokolüdür.



Şekil 2.8 Bizans Hata Toleransı'nın Çalışma Biçimi

2.2.3 Fikir birliği protokollerinin hata toleransı

PoW ve PoS olasılıklı-kesinlik (probabilistic-finality) protokolleridir ve saldırganların iyi bir zincirin yerini alacak uzun bir özel zincir oluşturmak için büyük miktarda hesaplama gücü veya hisse biriktirmeleri gerekir. Blok zinciri ayarında kesinlik (finality), iyi biçimlendirilmiş tüm blokların blok zincirine bağlandıktan sonra iptal edilmeyeceğinin onaylanmasıdır. Kullanıcılar işlem yaparken, işlemleri tamamlandıktan sonra işlemlerin keyfi olarak değiştirilemeyeceğinden veya geri alınamayacağından emin olmak isterler. Bu nedenle, bir blok zinciri fikir birliği protokolü tasarlarken kesinlik hayati derecede önem arz etmektedir.

Mevcut Nakamoto fikir birliği tabanlı sistemlerde, %51 saldırıları ve kötü niyetli madencilik, blokların iptal edilme olasılığına izin vererek sistemin sağlığını tehdit edebilir. Bu protokoller olasılıksal kesinlik sunarken, diğerleri mutlak kesinlik (Absolute-finality) sunmaktadır. Örneğin, Bitcoin'de, bir saldırganın çift harcamalı (double spending) bir saldırıyı başarıyla tamamlamak için daha uzun bir özel zincir oluşturması için hesaplama gücünün %51'i yeterlidir (Nakamoto and Bitcoin, 2008). Bu nedenle, saldırganın hesaplama gücünün (computational power) oranı %51 veya daha fazlaysa, blok zinciri ağı zayıflatılacaktır. PoW gibi, PoS yalnızca sahip olunan hissenin %51'inden daha azına sahip olan paydaşın

varlığına izin verebilmektedir. PBFT' de ise ağda toplam 3f+1 düğüm varsa normal düğüm sayısı 2f+1'i geçmelidir, yani kötü niyetli veya çöken düğüm sayısı f'den az olmalıdır. Bu nedenle, PBFT' nin hata toleransı 1/3'tür (Castro and Liskov, 1999).

Olasılıklı-kesinlik

Zincir tabanlı protokoller (örn. Bitcoin'in Nakamoto konsensüsü) tarafından sağlanan kesinlik türünü ifade eder; burada bir işlemin geri alınmama olasılığı, bu işlemi içeren blok zincirin kesinliğine ve yoğunluğuna göre artar. Blok ne kadar yoğunsa (yani ana blok gibi), o bloğu içeren çatalın en uzun zincir olma olasılığı o kadar yüksektir. Bu nedenle, bir işlemin geri döndürülme olasılığının çok düşük olduğundan emin olmak için, bir işlemi takip etmeden önce yaklaşık bir saat süren Bitcoin blok zincirinde 6 blok onaylanmasına kadar bir işlemin beklenmesi önerilmektedir.

Mutlak-kesinlik

PBFT tabanlı protokoller tarafından sağlanan ve bir bloğa dâhil edildikten ve blok zincirine eklendikten sonra bir işlemin hemen tamamlanmış olarak kabul edildiği kesinlik türünü ifade eder. Bu durumda, bir lider bir blok teklif edecek ve bir onaylayıcılar komitesinin yeterli bir kısmının bloğu onaylaması gerekecektir.

Bölüm 2.2.3'te bahsettiğimiz fikir birliği protokollerinin hata toleransı, türü ve uygulama senaryoları açısından genel analiz ve karşılaştırma sonuçları Tablo 2.4'te özetlenmiştir.

Tablo 2.4 Fikir Birliği Protokollerinin Genel Karşılaştırması

Özellik	PoW	PoS	PBFT
Tür	Olasılıksal-kesinlik	Olasılıksal-kesinlik	Mutlak-kesinlik
Hata Toleransı	%51	%51	%33
Enerji Tüketimi	Fazla	Az	İhmal edilebilir
Uygulanabilirliği	Açık	Açık	İzinli

2.2.4 Fikir birliği protokollerinin tutarlılığı

Blok zincir teknolojisinde tutarlılık (consistency), eşler-arası ağda tüm düğümlerin zincirin aynı kopyasına sahip olması gerekliliğini ifade etmektedir (Bano et al., 2019). Burada, yeni oluşturulan blok, tüm düğümler tarafından dağıtılmakta ve doğrulanmaktadır. Blok zincirinin tüm kopyaları, fikir birliği protokolü tarafından öngörülen doğrulama kuralları aracılığıyla tutarlı hale gelmektedir. Dolayısıyla tutarlılık, blok zincirinin uygulamasında kabul edilen fikir birliği protokolüne bağlıdır. Örneğin, PoW tabanlı blok zinciri zayıf bir tutarlılık sağlar; çünkü blok zincirde bazı okuma/yazma istekleri eski verileri döndürebilse de, her düğümdeki blok zincirinin kopyasının sonunda tutarlı hale geldiği anlamına gelir (Zhang et al., 2019) FBFT tabanlı blok zinciri, tüm düğümlerin aynı anda blok zincirinin aynı kopyasına sahip olduğu anlamına gelen güçlü bir tutarlılık sağlamaktadır.

2.2.5 Eşler arası ağların ve fikir birliği protokollerin güvenlik açıklığı

Bölüm 2.1.3 ve 2.2.4'te sunduğumuz güvenlik gereksinimleri, eşler arası ağların ve fikir birliği protokollerin güvenliğinde önemli bir rol oynadığını göstermektedir. Bu ağlarının ve protokollerin tasarımı veya uygulanmasındaki eksiklikler, yukarıda bahsettiğimiz güvenlik gereksinimlerini ihlal ederek, kötü niyetli saldırganlar tarafından saldırı gerçekleştirmek suretiyle farklı güvenlik açıklarına neden olabilmektedir. Eşler arası ağlarda güvenlik açıkları çoklu kimliklerin oluşturulması, yönlendirme müdahalesi ve iletişim kapasitesi olmak üzere 3 ana kısımdan oluşmaktadır (Cao et al., 2022).

Çoklu kimliklerin oluşturulması: Eşler arası ağda, her düğüm benzersiz bir kimliğe (yani genel anahtar) sahiptir. Ancak saldırganlar, bu ağa katılmak için aynı makinede sahte birden çok kimlikten yararlanabilir. Sybil saldırısı (Douceur, 2002) ile saldırganlar çoklu kimlikler oluşturarak ağda kalan düğümler hakkında yönlendirme bilgilerini elde edebilir ve seçtiği bir düğümün ağ yönlendirmesini yanlış yönlendirip ağ kaynaklarını tüketebilmektedirler (Kolb et al., 2020)

Yönlendirme müdahalesi: Bu güvenlik açığı, bir saldırganın, seçtiği

düğümlerinin bağlantılarını ele geçirerek veya protokoldeki doğrulama kurallarının eksikliğini kullanarak, bu düğümlerin ağda ayırt edilmesine izin verir. Ayırt etme işlemi başarılı olduktan sonra, saldırgan artık seçtiği bu düğümlerin yönlendirmesini kontrol edebilir ve diğer düğümlerle olan etkileşimini daha da etkileyebilir. Benzer şekilde, Ethereum'a karşı önerilen Ortadaki-Adam (Man-in-the-Middle) saldırısı (Ekparinya et al., 2018), bir saldırganın bir Sınır Ağ Geçidi Protokolünün (Border Gateway Protocol) yolunu ele geçirerek düğümler arasındaki iletişim gecikmesini manipüle edebileceğini göstermektedir. Saldırgan iletişim gecikmesini kontrol altına aldığında, başka saldırılar da başlatabilmektedir.

İletişim kapasitesi: Ağ bağlantısı, farklı bölgelerde önemli ölçüde farklılıklar göstermektedir. Yüksek bağlantılı bir bölgede bulunan düğümler ile daha az bağlantılı bir bölgedeki düğümleri karşılaştırdığımızda, yüksek bağlantılı bölgede bulunan düğümlerin blokları daha hızlı oluşturup diğer düğümlere göndermesi işkardır (Xiao et al.,2020). Ayrıca düğümlerin bir bloğa sığdırdığı işlem sayısındaki farklılık da farklı iletişim gecikmelerine neden olurmaktadır (Xiong et al.,2018). Dolayısıyla, farklı düğümlerin farklı iletişim kapasiteleri vardır, yani düğümlerin bloklarını tüm ağa yayması farklı gecikmeler oluşturmaktadır. Saldırganlar bir saldırı başlatmak için bu güvenlik açığından daha fazla yararlanabilir ve fikir birliğinin güvenliğini baltalayabilir.

Eşler arası ağların güvenlik sorunlarını inceledikten sonra fikir birliği protokollerindeki güvenlik açıkları, esas olarak bu protokollerin hataya dayanıklı kapasitesi ile değişen ortam arasındaki tutarsızlıktan kaynaklanabilmektedir. Düğümdeki oy yetkisinin merkezileştirilmesi, karlı stratejiler düşünülmesi, özel düğümlere bağımlılığın artması ve düşük hata toleransı seviyesi gibi temel hatalardan oluşan güvenlik açıkları bulunmaktadır.

Merkezileşme: Blok zincir teknolojisinde, her düğüm kendi oylama gücüyle (örneğin, PoW' daki işlem gücü veya PoS' deki hisse) blok üretmek için ağdaki diğer düğümlerle bir rekabet içindedir. Yarışmaya daha fazla düğüm katıldıkça, tek bir düğümün tüm ağdaki oylama gücünün çoğunluğunu kontrol etmesi zordur. Bu duırum protokol için bir güvenlik garantisi olarak kabul

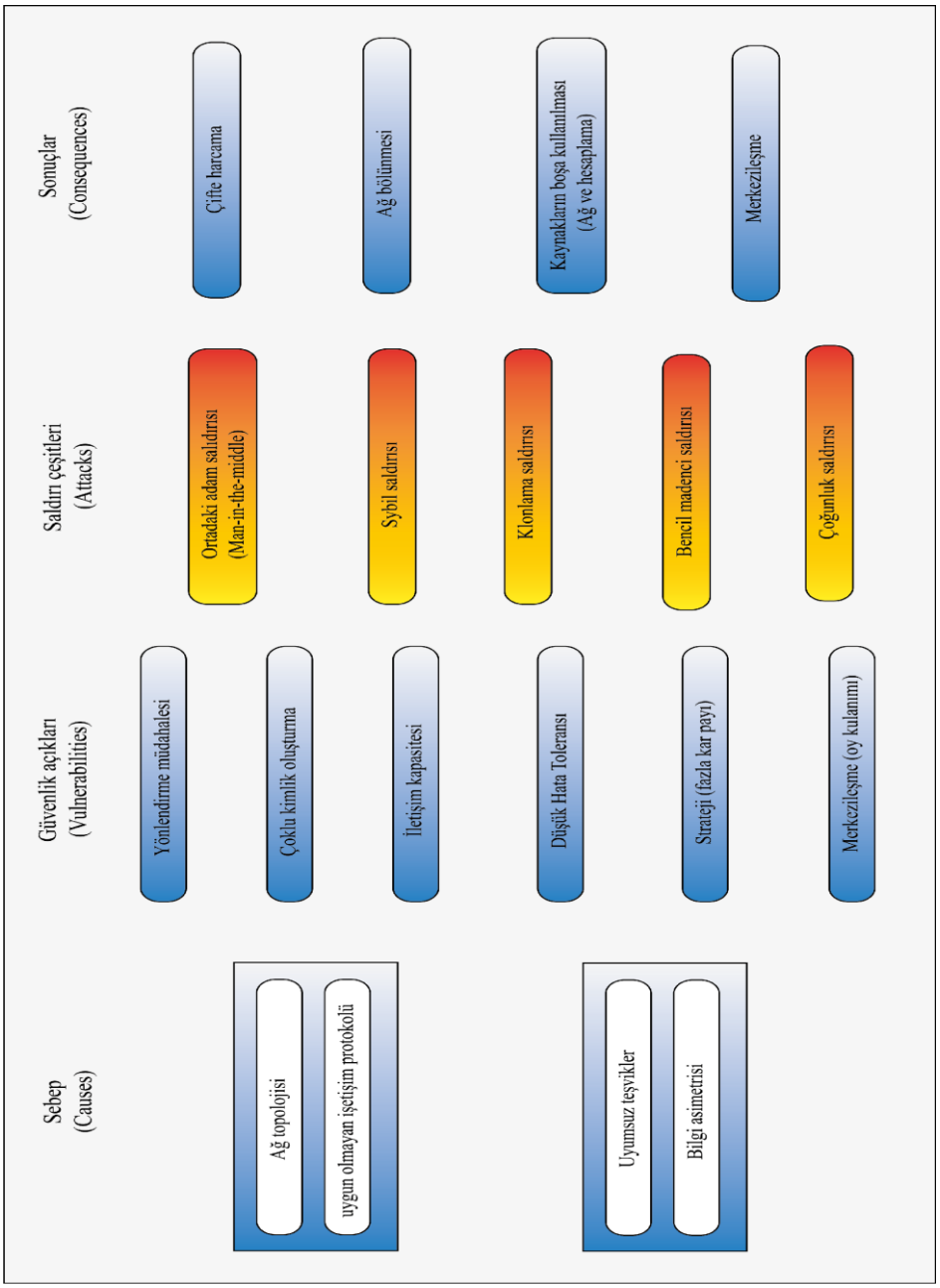
edilmektedir (Nakamoto, 2008). Ayrıca, sistem birden çok düğüm oylama güçlerini bir araya getirebilir ve bir konsorsiyum (yani, "havuz") biçiminde diğer düğümlerle rekabet edebilmesine olanak tanımaktadır (Eyal and Sirer, 2014). Dolayısıyla, bir havuz sistemi, bir tek düğüme kıyasla oylama gücünün çoğunluğunu kontrol etmeye eğilimlidir ve bir çoğunluk saldırısı (yani, %51 saldırısı (Saad et al., 2020)) başlatabilir. Bu durumda, olası senaryolardan biri blok zincirinin yanlış geçmişe sahip alternatif bir kopyasını oluşturmaktır. Bu durum arzu edilen bir durum değildir. Ancak günümüzde, halka açık blok zinciri platformlarında havuzlar çok yaygındır ve blok oluşturmada baskın bir rol oynayarak ağın kademeli olarak merkezlenmesine neden olmaktadır (Bitcoinmining, 2016).

Strateji (daha fazla kar payı): Adil bir sistemde düğümler yeni oluşturulan bloğu diğer düğümlere yaydığında ve tüm ağdaki oylama gücü oranıyla eşleşen blok ödülünü alması diyebiliriz. Ancak bazı strateji ile saldırganlar adil paylarından daha fazla gelir elde etmek için yeni oluşturulan bloğu geçici olarak gizleyebilir bu durum kaynak israfına ve ağın kademeli olarak merkezileşmesine yol açabilmektedir (Eyal and Sirer,2014). Bu tür stratejiler veya bunların bir kombinasyonu, saldırganların başka saldırılar başlatmasına sebep olmaktadır. Ancak, bu tür stratejileri tespit etmek ve hatta uygulanabilir karşı önlemler bulmak zordur (Eyal, 2015) Şu anda, bu stratejilerden kaynaklanan güvenlik açığı, açık bir araştırma sorunu olmaya devam etmektedir.

Düşük hata toleransı: Fikir birliği protokolünün doğası gereği düşük düzeyde hata toleransı veya düşük düzeyde hata toleransı haline gelen bir güvenlik açığı bulunmaktadır. Örneğin, kötü niyetli düğümlere PBFT de %33'e kadar, PoW veya PoS orijinal olarak %51'e kadar tolerans gösterecek şekilde tasarlanmıştır. Oylama gücünün merkezileştirilmesi ve daha karlı stratejiler nedeniyle bu eşik düşürülebilirken muhtemelen, daha düşük bir hata toleransı seviyesi, başarılı saldırılar için gereken koşulları daha da azaltarak, güvensiz bir fikir birliğine yol açabilmektedir.

Yukarıda bahsettiğimiz güvenlik açıkları veya saldırılar, güvenlik gereksinimlerinin birkaç idealist varsayıma dayanması sebebiyle pratikte garanti

edilemediğini göstermektedir (Xiao et al., 2020). Bu varsayımlar düğümlerin aynı iletişim özelliğine sahip olduğunu, düğümlerin işlemleri ve blokları ağ boyunca eşit hızda yayılabildiği gibi gereksinimlerdir (Garay et al., 2015). Ancak düğümlerin alabileceği teşvik ödülü mekanizması giderek artan yoğun rekabet nedeniyle azaltılır, bu durum düğümleri karlarını başka yollarla (örneğin, havuzlar veya farklı kar oranı yüksek stratejiler) maksimize etmeye itebilmektedir (Sapirshtein et al., 2016). Ek olarak, Şekil 2.9'da fikir birliği ile ilgili nedenler-zafiyetler-saldırılar-sonuçları gösteren genel bir veri tablosu ile gösterilmiştir (Cao et al., 2022).



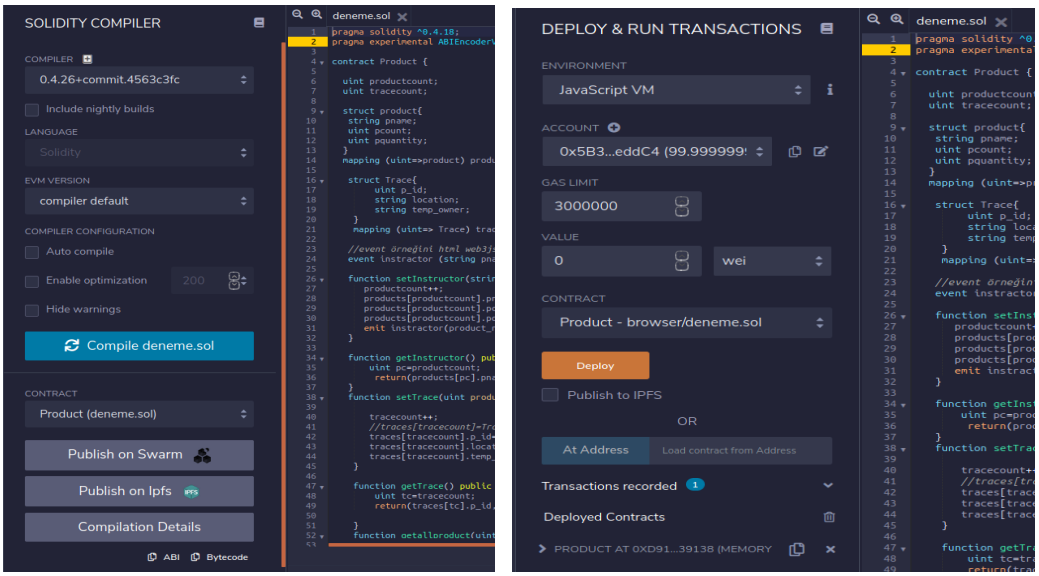
Şekil 2.9 Fikir Birliği Protokollerinde Olası Zafiyetler Ve Nedenleri

2.2.6 Akıllı Sözleşmeler

Blokzincir teknolojisinde kullanılan akıllı sözleşmeler (smart contracts) ilk olarak Nick Szabo tarafından ortaya atılmıştır (Szabo,1994). Akıllı sözleşme, iki veya daha fazla taraf arasında ortak bir anlaşmadır. Önceden tanımlanmış işlevleri sayesinde bilgileri depolar, girdileri işler ve çıktıları yazar (Buterin, 2014). Örneğin, akıllı sözleşme, akıllı sözleşme oluşturmayı sağlayan yapıcı işlevini tanımlayabilir. Blok zincirde yeni bir akıllı sözleşmenin oluşması, akıllı sözleşme

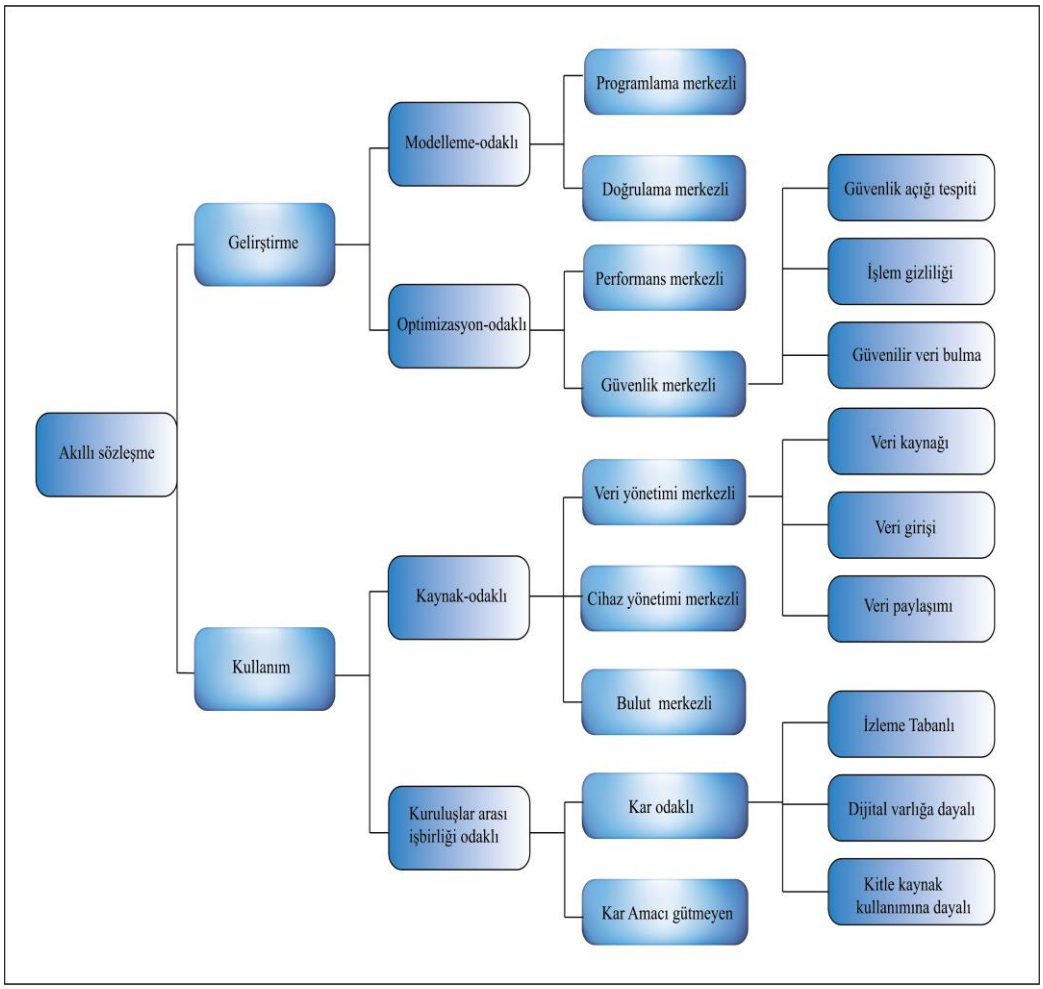
sahibi olan bir işlem aracılığıyla yapıcı işlevi çağrılarak etkinleştirilir. Kendi kendini imha etme işlevi, akıllı bir sözleşmede tanımlanabilecek işlevlerin başka bir örneğidir. Yanlızca ilgili akıllı sözleşme sahibi bu işlevi çağırarak sözleşmeyi yok edebilmektedir. Akıllı bir sözleşmenin, sözleşme şartlarına göre ilgili olayları ve eylemleri yürütmesi ve kontrol etmesi amaçlanan durum değişkenleri (state variables), fonksiyonlar, fonksiyon değiştiricileri (function modifiers), olaylar (events) ve yapılar (structures) (Buterin, 2014) içeren bir sınıftır. Bitcoin blok zincirinde, çok imzalı hesaplar (multi-signature wallets) gibi kullanım durumlarını kolaylaştıran bir komut dosyası sistemi aracılığıyla akıllı sözleşmelerin temel bir sürümü uygulanmıştır. Akıllı sözleşmeler blok zincir teknolojisine fazladan bir katman (layer) eklemektedir. Yani sadece A kişisinden B kişisine para göndermek değil de akıllı sözleşmeler sayesinde ağdaki işlemlere programlama yeteneği de sağlanmış oldu. Akıllı sözleşmeler, aslında bir blok zincirindeki fikir birliği mekanizmasının doğru şekilde yürütülmesini sağladığı bir yazılım kodu parçasıdır. Akıllı sözleşmeler sayesinde üçüncü bir taraf olmadan ilgili kurallar sisteme işlenmektedir. Blok zincir özellikli akıllı sözleşmelerin sınıflandırma çalışması şekil 2.11 de gösterilmiştir.

Her akıllı sözleşme de, durumlar ve işlevler bulunmaktadır. İlki, bazı verileri veya sahibinin cüzdan adresini (yani akıllı sözleşmenin konuşlandırıldığı adres) tutan değişkenlerdir. Asla değiştirilemeyen sabit durumlar ve blok zincirindeki durumları kaydeden yazılabilir durumlar olmak üzere iki durum tipi arasında ayrım yapabiliriz. İkincisi, durumları okuyabilen veya değiştirebilen kod parçalarıdır. Durum geçişlerinin blok zincirinin yeni bir bloğunda kodlanması gerektiğinden, gaz ücreti gerektiren işlevler, çalıştırmak ve yazmak için gaz gerektirmeyen salt okunur işlevler olmak üzere iki işlev türü vardır. Burada, sonsuz döngüde akıllı sözleşmenin çalışmasını önlemek için ise ödeme para birimi (yani gaz ücreti (gas fee))gereklidir (Şekil 2.10).



Şekil 2.10 Ethereum Sanal Makinesi'nde (Ethereum Virtual Machine (EVM)) Akıllı Sözleşme

Akıllı sözleşmeler, farklı blok zinciri platformlarında (örneğin, Ethereum ve Hyperledger Fabric) geliştirilebilir ve uygulanabilirdir. Birkaç platform, sözleşme programlama dilleri, sözleşme kodu yürütme ve güvenlik seviyeleri dâhil olmak üzere akıllı sözleşmeler geliştirmek için ayırt edici özellikler sunmaktadır. Bazı platformlar ise, akıllı sözleşmeler geliştirmek için üst düzey programlama dillerini desteklemektedir. Bitcoin (Nakamoto and Bitcoin, 2008) kripto para birimi işlemlerini işlemek için kullanılabilen, ancak çok sınırlı bir bilgi işlem kabiliyetine sahip, açık bir blok zinciri platformu olduğu için yığın tabanlı (stack-based bytecode) komut dosyası dili kullanmaktadır. Bitcoin komut dosyası (scripting) dilini kullanarak zengin mantıkla akıllı bir sözleşme oluşturma yeteneği çok sınırlıdır. Bitcoin'in blok zincirinde uygun akıllı sözleşmeleri etkinleştirmek için hem madencilik işlevlerinde hem de madenciliği teşvik planlarında büyük değişiklikler yapılması gerekecektir (Lewis., A, 2016).



Şekil 2.11 Akıllı Sözleşme Tabanlı Çalışmaların Sınıflandırılması

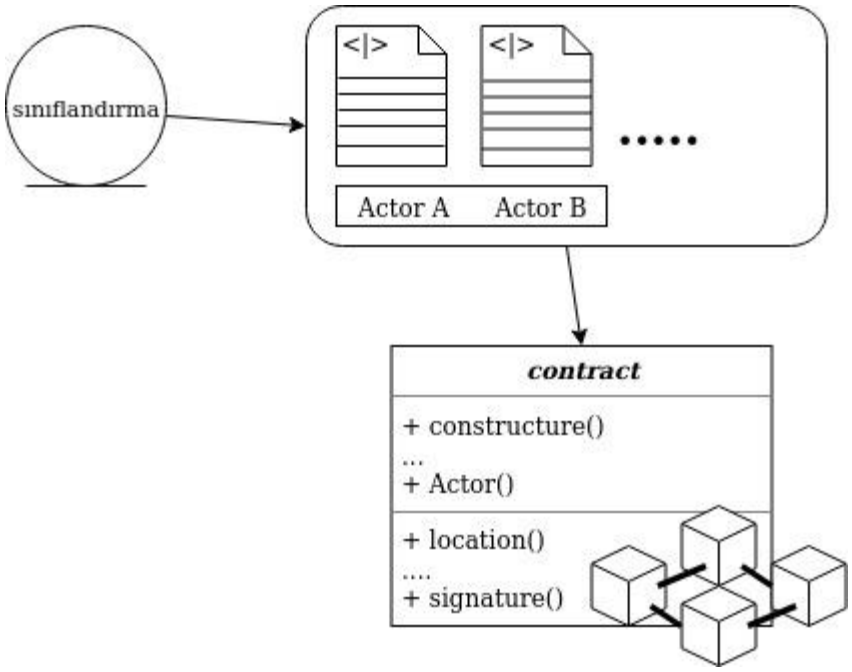
Blok zincir teknolojisinin ilerlemesi ve Ethereum blok zincirinin (Buterin, 2014) ortaya çıkmasından sonra, Ethereum Sanal Makinesi'nde (Ethereum Virtual Machine(EVM)) genel bir amaç ve tam akıllı sözleşme sisteminin sunulması sağlanmıştır. EVM Turing-tam bir sanal makinenin yardımıyla gelişmiş ve özelleştirilmiş akıllı sözleşmeleri destekler. EVM, akıllı sözleşmeler için çalışma zamanı ortamıdır ve Ethereum ağındaki her düğüm, bir EVM uygulamasını çalıştırır ve aynı talimatları yürütür. Solidity, üst düzey bir programlama dili olarak, akıllı sözleşmeler yazmak için kullanılır ve sözleşme kodu, EVM bayt koduna derlenir ve yürütme için blok zincirinde konuşlandırılır. Ethereum şu anda akıllı sözleşmeler için en popüler geliştirme platformudur ve çeşitli alanlarda çeşitli türlerde merkezi olmayan uygulamalar (DApp'ler) tasarlamak için kullanılabilirdir. Ethereum'da bir sözleşme uygulandığında (deploy), adresi bir miktar Ether verilir, özel bir depoya sahiptir ve kod ile ilişkilendirilir (Luu et al,

2016). Bir sözleşmeyle etkileşim kurmak isteyen kullanıcılar genellikle iki tür bilgi gönderir. İlk olarak sözleşme adresine "gaz" verilir. Ethereum'da gas, ağın sözleşmeyi yürütmesi için kullanıcının kullanmak istediği Ether miktarını belirtir. İkinci olarak, sözleşmeye yapılan işlemde, sözleşmenin kodu için bir girdi görevi gören bir veri alanı sağlanır (Şekil 2.11).

Bitcoin ve Ethereum gibi halka açık blok zinciri yerine, izinli bir blok zincir olan Hyperledger Fabric (Androulaki et al., 2018), bir üyelik hizmet sağlayıcısı aracılığıyla da yalnızca işle ilgili kuruluşların katılabileceği ağ oluşturulabilmektedir. Hyperledger Fabric, IBM tarafından önerilen ve akıllı sözleşmeleri destekleyen, açık kaynaklı, kurumsal düzeyde dağıtılmış bir defter teknolojisi platformudur. Çok çeşitli endüstri kullanım durumları için modülerlik ve çok yönlülük sunar. Hyperledger Fabric için modüler mimari, tak ve çalıştır bileşenleri aracılığıyla kurumsal kullanım durumlarının çeşitliliğini barındırmaktadır.

Ethereum ve Hyperledger Fabric akıllı sözleşmeleri birçok açıdan farklılık göstermektedir. Solidity, Ethereum akıllı sözleşmeleri yazmak için kullanılan iyi bilinen programlama dildir. Hyperledger Fabric Go, Java ve Javascript (Androulaki et al., 2018) gibi çok dilli akıllı sözleşmeleri desteklemektedir. Sözleşme kodunun yürütülmesi için, Ethereum'daki sözleşme kodu, eşler arası ağda yayılan bir işleme dâhil edilir ve bu işlemi alan herhangi bir madenci, onu yerel sanal makinesinde yürütebilir (Buterin, 2014). Hyperledger Fabric'te, uygulama tarafından bir işlem oluşturulduğunda, işlem yalnızca belirtilen eşler (onaylayan eşler) tarafından yürütülür ve imzalanır. Uygulamanın işlem teklifini aldıktan sonra, bu onaylayan eşlerin her biri işlemin atıfta bulunduğu zincir kodunu çağırarak bağımsız olarak yürütür (Androulaki et al., 2018). Güvenlik için, zincir kod, izolasyon için bir kapsayıcı ortamında (örneğin Docker) çalışmaktadır.

Bu tez çalışmasında akıllı sözleşmeleri destekleyen ethereum sanal makinesinde (EVM) solidity programlama kullanarak uygulamalar yapılmıştır (Buterin, 2014) (Şekil 2.12).



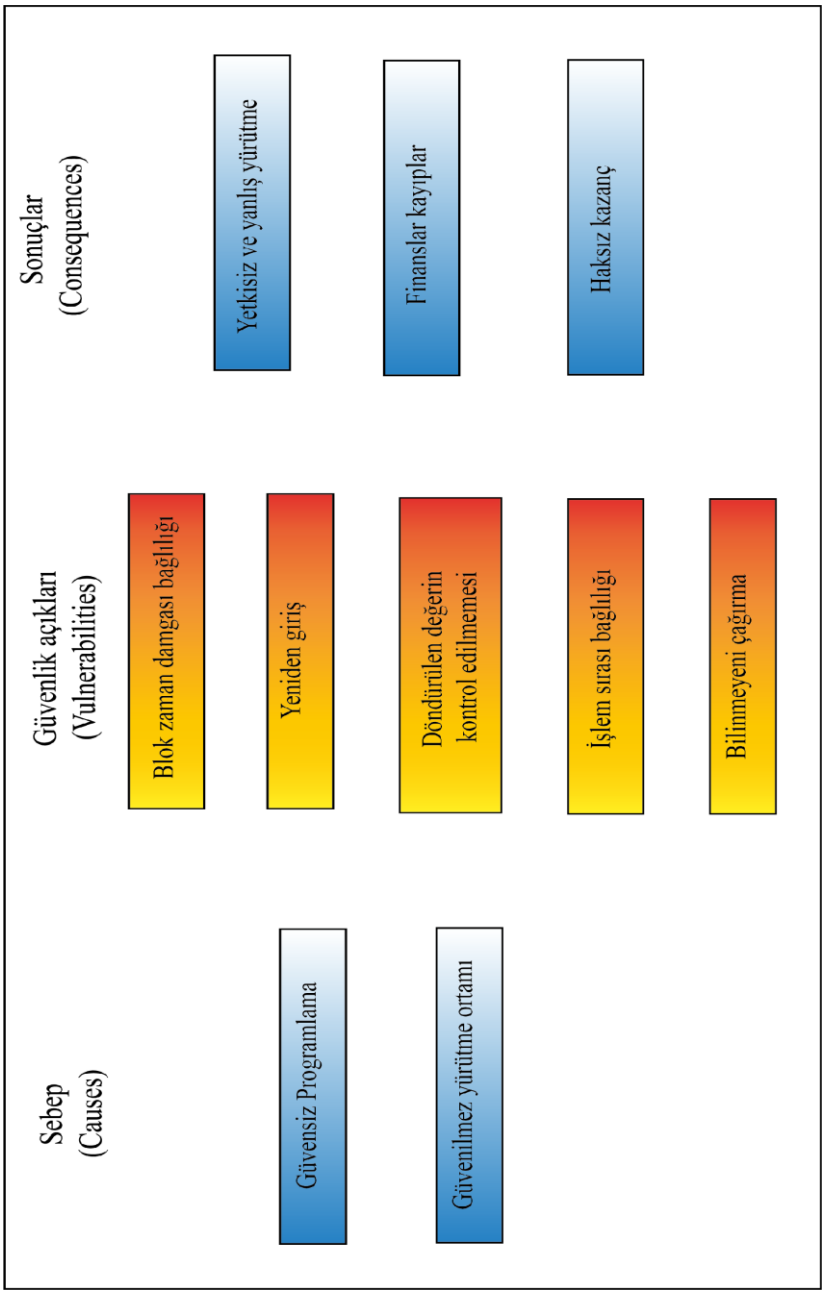
Şekil 2.12 Akıllı Sözleşme Diyagramı

Akıllı sözleşmeler, son yıllarda (Cao et al., 2022) hem hırsızlık hem de mali kayıplarla sonuçlanan çoklu güvenlik açıklarından zarar görmektedir. Ayrıca Akıllı sözleşmelerin geleneksel iş süreçlerini yeniden şekillendirme konusunda büyük potansiyelleri olmasına rağmen, çözülmesi gereken bir takım zorluklar bulunmaktadır. Örneğin, yazılan akıllı sözleşme ile tarafların belirli bir anonimliği sağlansa bile, tüm işlemler küresel olarak erişilebilir olduğundan, tüm sözleşme uygulamasının gizliliği korunmayabilir. Ayrıca, bilgisayar programlarının hatalara ve arızalara karşı zafiyetleri nedeniyle akıllı sözleşmelerin doğruluğunu sağlamak zordur (Zheng et al., 2020). Bu nedenle güvenli akıllı sözleşmelerin tasarlanması ve uygulanması, uyarlanabilir yazılım mühendisliği teknolojileri ve ağ oluşturma, programlama dilleri ve kriptografi gibi birden çok araştırma alanından uzmanlık gerektirmektedir.

2.2.7 Akıllı sözleşmelerin güvenliği, sebep ve sonuçları

Önceki bölümlerde akıllı sözleşmelerin, büyük miktarda dijital varlık veya veri işleyebilir olduğundan ve yüksek riskli finansal ortamlarda kuralların uygulanması için kullanılabilir olduğundan bahsettik. Akıllı sözleşmelerin güvenlik yönünü göz önünde bulundurmak çok önemlidir, çünkü küçük bir hata

bile çok fazla veri kaybı veya gizlilik sızıntısı gibi önemli sorunlara yol açabilir. Bu nedenle kötü niyetli saldırganlar için çekici bir hedef haline gelmektedir. Akıllı sözleşmeler, blok zincirinin değişmezlik özelliği nedeniyle blok zincirine yerleştirildikten sonra değişmez hale gelmektedir. Kötü niyetli saldırganlar, kâr elde etmek veya sözleşmelerin doğru yürütülmesini sabote etmek için akıllı sözleşmelerde gizlenen güvenlik açıklarından yararlanabilir. Bu güvenlik açıklarından çoğu, Bölüm 2.2.6'da belirtilen güvenlik gereksinimlerinin ihlal edilmesinden kaynaklanmaktadır. Ayrıca, akıllı sözleşmelerde işlem sırası, zaman damgası, yanlış kullanılan istisnalar, yeniden giriş güvenlik açıkları gibi başka güvenlik zafiyeti de bulunmaktadır. Şekil 2.13'te akıllı sözleşmelerde güvenlik açığı oluşan sebepler ve sonuç üzerine genel bir sınıflandırma yapılmıştır (Cao et al., 2022). Ethereum blok zincirinde işlem yürütme sırası madencilere bağlıdır ve müşterilerin bunlar üzerinde herhangi bir kontrolü yoktur. Bu sorun, aynı sözleşme tarafından çağrılan birden fazla işlem olduğunda ortaya çıkabilir ve bu işlemlerin sırası blok zincirinin yeni durumunu etkileyebilir. Zaman damgası ile tetiklenen koşulları içeren akıllı sözleşmelerin güvenlik zafiyeti oluşabilir. Blok zaman damgaları, madenciler tarafından yerel sistem saatlerine göre belirlenir ve böylece bir düşman tarafından manipüle edilebilirler. Bu durumda blok indeksi kullanılabilir. Yanlış kullanılan istisnalarda ise, başka bir sözleşmeyi çağrılan sözleşmede herhangi bir istisna oluşursa, feshedilir ve arayan sözleşmeye bildirimde bulunmayabilir. Dahası bir sözleşme başka bir sözleşmeyi çağırdığında, mevcut sözleşmenin yürütülmesi, aranan sözleşme bitene kadar bekler. Bu, düşmana, arayan sözleşmenin aracı durumundan yararlanma fırsatı sağlayabilir. Yeniden giriş güvenlik açığı orijinal çağrı tamamlanmadan önce başka bir akıllı sözleşme tarafından tekrar tekrar çağrıldığında oluşur. Bu güvenlik açığı, akıllı sözleşmelerin çağrı bütünlüğünü ihlal etmesinden kaynaklanır ve akıllı sözleşmeyi yeniden giriş noktasında tutarsızlık oluşturarak beklenmeyen davranışlara neden olabilir (Rouhani and Deters,2019; Atzei et al., 2017).



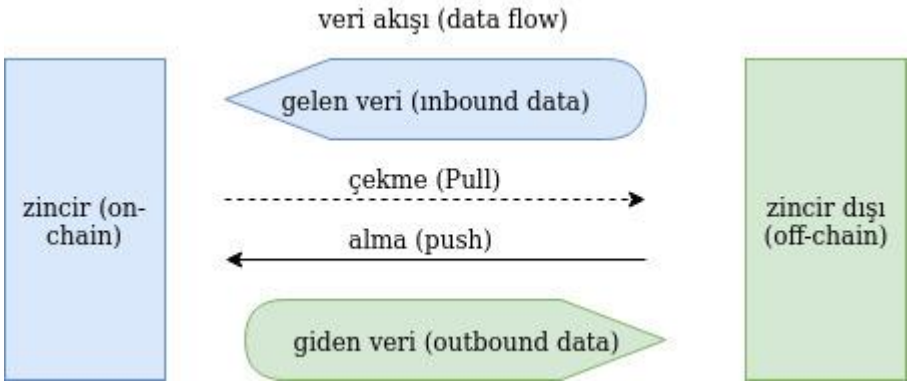
Şekil 2.13 Akıllı Sözleşme Olası Zafiyetler Ve Nedenleri

2.2.8 Zincir ve Zincir dışı veri işleme

Son yıllarda, blokzincir tabanlı uygulama prototiplerinin kavram kanıtı (proof-of-concept) uygulamaları sırasında kapsamlı deneyimler kazanıldı. Merkezi olmayan sistemler yüksek düzeyde güvenlik ve gizlilik sağlamasına rağmen, maliyetli ve yavaştırlar. Dolayısıyla blok zincir teknolojisi üzerinde işlenen smart contract ile hangi verilerin zincir üzerinde hangi verilerin zincir dışında saklanacağı ve çalıştırılması son derece önemlidir. Zincir dışı (off-chain)

kullanım, ilgili sorunlara da çözüm getirilebilmektedir. Bununla birlikte, akıllı sözleşmeler çok iyi harici veri beslemelerine ihtiyaç duyabilir. Gerçek dünyadaki olayları bulup doğrulayan ve bu bilgiyi bir blok zincirine gönderen Oracles, akıllı sözleşmelere veri besleyebilen zincir dışı çözümlerdir (Eberhardt and Tai,2017) (Şekil 2.14).

Tez çalışmasında zincir üzerinde(on-chain) yazılan akıllı sözleşmeler ile zincir dışı (off-chain) kullanılarak, gerek sözleşme üzerinde maliyet sorunu gerekse ölçeklenebilirliği üzerine işlemler yapılmış ve optimize edilmiştir.



Şekil 2.14 Zincir Dışı (Off-Chain) ve Zincir (On-Chain) Kullanımı

2.2.9 Anonimleştirme teknikleri

Blok zincirlere uygulanabilir birtakım anonimleştirme teknikleri (anonmization techniques) bulunmaktadır. Bu teknikler ZCash (Sasson et al., 2014), DASH (Duffield and Diaz, 2018) ve Monero (Nicolas, 2013) gibi protokollerde kullanılmaktadır. Bu tez çalışması ve anonimleştirme teknikleri için önemli olan iki önemli özellik vardır;

- **Takip edilemezlik (Untraceability):** Gelen her işlem için tüm olası göndericiler eşit olasılıklıdır.
- **Bağlantısızlık (Unlinkability)**: Herhangi iki giden işlemin aynı kişiye gönderildiğini kanıtlamak imkânsızdır.

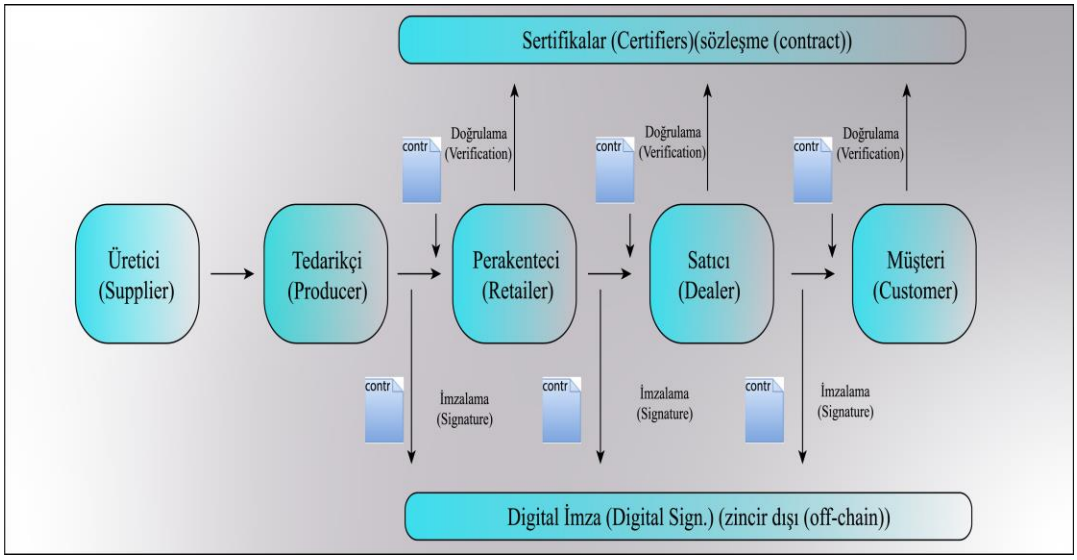
ZCash: zkSNARKs, işlemlerin geçerliliğini garanti etmek ve anonimleştirme sağlamak için sıfır bilgi kanıtlarını (Zero-knowledge-proof) kullanır. Kullanılan sıfır bilgi ispatlı yapıya zk-SNARK denir, "sıfır bilgi ile karşındakinin sen olduğunu ispatlama" anlamına gelmektedir. Yani "Sıfır bilgi" ispatları, ispatlayanın doğrulayıcıya herhangi bir ifadenin doğruluğunu ispat etmesine, ifadenin kendisinin geçerliliğinin ötesinde herhangi bir bilgi ifşa etmeden ispatlamasına denir. Örneğin, rastgele bir sayının hash değeri verildiğinde, kanıtlayıcı doğrulayıcıyı, bu hash değerine sahip bir sayının gerçekten var olduğuna, ne olduğunu açıklamadan ikna edebilir.

DASH tarafından kullanılan protokolde amaç, işlemlerin kullanıcıların (gönderici ve alıcı) hesap bakiyesini anonim hale getirmektir. Mimarideki bu işlem, Masternodes adı verilen merkezi olmayan bir sunucu ağı kullanan bir karıştırma protokolü aracılığıyla yapılır. Ayrıca Masternode aracılığıyla, sistemin bütünlüğünü tehlikeye atabilecek güvenilir bir üçüncü taraf ihtiyacını ortadan kaldırırken ağın anonimleştirme sağlamasına izin veren iki katmanlı bir ağ da sunmaktadır.

Tez çalışmasında, mimarimiz kullanıcının isteğine bağlı olarak, anonimlik ve şeffaflık arasında denge kuracak şekilde oluşturulmuştur.

3. ÇALIŞMA MODELİ

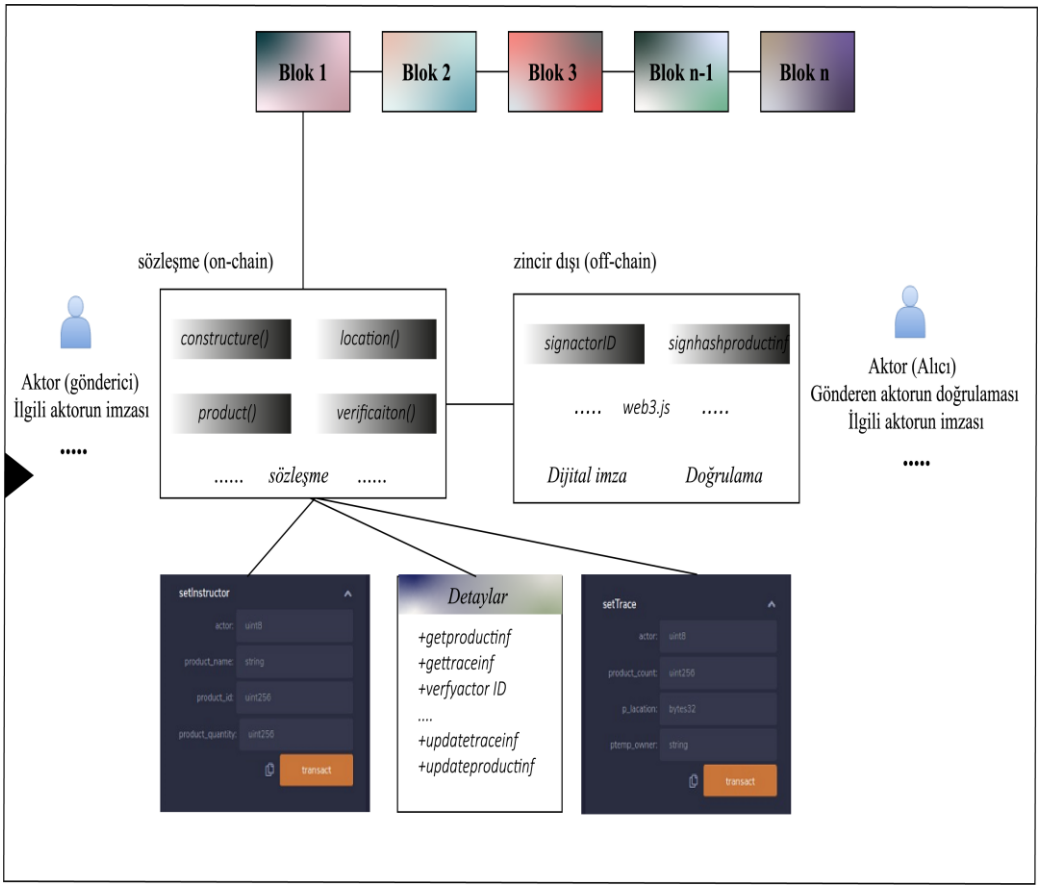
Bu tez çalışmasında akıllı sözleşmelere dayalı, merkezi olmayan, açık ağda özel değerler üzerine yani açık-gizli-blokzincir (public-permissioned) tabanlı bir sistem modeli öneriyoruz. Kavram ispatı (proof-of-consept) (PoC) mimarimiz kullanıcının isteğine bağlı olarak, anonimlik ve şeffaflık arasında denge kuracak şekilde oluşturulmuştur. Mimari 5 aktörden oluşmaktadır: tedarikçi, üretici, satıcı, perakendeci ve müşteri. Mimaride yönetilen her ürün türü aktörler tarafından işlenir ve bunlar akıllı bir sözleşme dâhilinde gerçekleştirilir. Mimarinin en önemli yapısı olan dijital imzalama zincir dışı entegre sistemi kullanılarak gerçekleştirilmiştir. Bu nedenle, ölçeklenebilirlik açısından zincir dışı kullanım daha iyi performans göstermiştir. Digital imzalama işleminden sonra doğrulama işlemi sözleşme üzerinde yapılmaktadır. Mimarideki üretici ürünü oluşturduğunu ve taşıyıcı aracılığıyla perakendeciye ilettiğini, perakendeci ise satıcıya daha sonra nihai hedef müşteriye iletildiğini varsayalım. Kavramsal mimarimiz Şekil 3.1 'da verilmiştir.



Şekil 3.1 Blokzincir Tabanlı Tedarik Zincir Yönetim Sisteminin Kavramsal Çerçevesi.

Çerçevemizin bir kısmı, akıllı sözleşmeleri destekleyen Ethereum Sanal Makinesi'nde (EVM) solidity programlama kullanılarak zincir üzerinde

oluşturulmuştur (Buterin, 2014). EVM, geliştiriciler için iyi uygulama arayüzü (API) 'lerine sahiptir. Burada HTML, CSS ve javascript ön uç (front-end), akıllı sözleşme (solidity prog.) arka uç (back-end) olarak adlandırılmaktadır. Uygulama, ön uç web sayfası ve arka uç akıllı sözleşmenin birleştirilmesiyle geliştirildi, olay-tabanlı doğrulama (Event-based verification), görüldüğü gibi mevcut klasik akıllı sözleşme ve zincir dışı ile entegrasyon üzerine kuruludur. Ürün, ilgili aktörler tarafından akıllı sözleşmeye (ürün bilgisi, mevcut lokasyon vb.) işlenir ve bu işlem sözleşme de gerçekleştirilir. Sözleşmemizin ana noktalarından biri, akıllı sözleşmemizin performansını iyileştirmek için zincir dışı entegrasyonudur. Sözleşme ile zincir dışı bir köprü görevi gören web3 kullanılarak, ilgili aktör dijital imzası için aktör kimliği imzası, ürün bilgisi imzalı hash değeri gibi işlemler gerçekleştirilir. Bu entegrasyonun bir özeti Şekil 3.2'de gösterilmektedir. Pilot uygulamada, akıllı sözleşmenin solidity prog. ile nasıl uygulandığı basit bir şekilde gösterilmektedir.



Şekil 3.2 Çerçevenin Akıllı Sözleşme Mimarisi

Kavramsal çerçevede, sistemin ana işlemi, dijital imza sonrasında ilgili aktörün ürün verilerinin doğrulanması ve başka bir aktöre gönderilmesidir. Tedarikçinin ürünü oluşturup nakliye yoluyla üreticiye göndermesi durumunda, üretici perakendeciye, perakendeci de bayi ve nihai müşteriye iletilir. Ürün bilgileri sistemdeki aktörler tarafından oluşturulur ve işlemler ağdaki EVM'nin düğümlerine yayınlanır. İşlemler daha sonra ağdaki tüm düğümler tarafından doğrulanır. Ancak mimarideki imza ve doğrulama, ilgili aktörlerin ürünle ilgili işlemlerinde bir sonraki aktöre mahremiyet sağlanarak yapılır. Sistemdeki şeffaflık ve anonimlik, ilgili aktörün talebine göre değişiklik göstermektedir. Bu işlemler hem zincir içi akıllı sözleşmelerle hem de zincir dışı işlemlerle entegre edilmiştir (Şekil 3.1).

3.1 Çerçevenin işlemler detayı

Mimaride her aktörün a_{id} ile gösterilen kendi aktör kimliği (ID) vardır. Her ürün için p_{id} ile gösterilen bir ürün kimliği vardır. Bir ürün kimliği listesi (p_{idlist}), sistemdeki her bir aktörün tüm ürün kimliklerini içerir. Burada yeni kayıt edilen ürünün ürün ID 'sinin benzersiz olup olmadığı tutulan listeden kontrol edilir. Her bir ürüne ait ürün bilgisi p_{inf} ile gösterilmektedir. İlgili ürün verilerinin hash değeri $h(ptx_i)$, ürün alım-satım işleminin tarih ve saati □□□□□, önceki işlemin hash değeri $h(ptx_{prev})$ ile gösterilir. İlgili aktörün dijital imzası ve doğrulaması $sign(h(ptx_i))$, $verfy(sign(h(ptxi)))$, $sig_h(h(ptx_i))$ ile gösterilmiştir (tablo 3.1).

Burada işlem hash değeri denklem 1 ile gösterilmiştir.

$$h(ptxi) = \{a_{id}\ ,\ p_{id}\ ,\ p_{idlist},\ p_{inf}\ ,\ p_{time},\ h(ptx_{prev})\}. \qquad (3.1)$$

Tablo 3.1 Çerçevenin Yapı Tablosu

Sembol	Açıklama
a_{id}	Aktör kimliği (Actor ID)
p_{id}	Ürün kimliği (Product ID)
p_{inf}	Ürün bilgileri (Product information (lokasyon vd.))
p_{idlist}	Ürün kimlik listesi (Product ID list)
$h(ptx_i)$	Ürün Bilgileri Hash Değeri (Hash of Product Inf.)
p_{time}	İlgili işlemin oluşturma ve yürütme zamanı (Time of transaction)
$h(ptx_{prev})$	Önceki işlemleri hash değeri (Hash of prev. Transaction)
$sig_h(h(ptx_i))$	Ürün bilgileri hash değerinin imzalı hash değeri (Sign hash of hash)
$sign(h(ptx_i))$	İlgili aktör imzası (Signature of actor)
$verfy(sig(h(ptx_i)),sig_h(h(ptx_i)))$	İlgili Aktor doğrulaması (Verification of actor)

Kısaca mimarinin çalışma şeklini açıklayalım. Üretici, ürün bilgilerini (pinf) sisteme girer ve ürün için benzersiz bir tanımlama kodu oluşturulur. Yeni ürün girişi için benzersiz ürün kimliği kontrolünden sonra, işlemler üretici tarafından doğrulanır ve bir sonraki adıma geçilir. Ürün bilgilerinin doğrulanmasının ardından üretici, dijital imzayı gerçekleştirir ve perakendeciye gönderir. Perakendeci, üreticilerin ilgili ürünü ele aldığı işlemleri doğrular. Diğer aktörlerin (satıcı ve müşteri) her aşamasında aynı doğrulama yapılmaktadır. Satıcı, perakendeciden gelen işlemlerin bilgilerini doğruladıktan sonra, satış yapmak için

ürün depolama ve ürün satış bilgilerini içeren yeni ürün bilgilerini imzalar. Daha sonra satıcı tarafından müşteriye kimlik bilgileri ve veri gizliliği korunarak satış yapılır. Müşteri, satıcıdan gelen verilerin doğruluğunu ispatlar ve sistemden doğru ürün bilgilerini şeffaf bir şekilde izleyebilir. Böylece, kullanıcı verilerinin gizliliği, her bir aktörün tedarik süreci boyunca korunur. Algoritma 1 de genel olarak mimarinin çalışma şekli açıklanmıştır (Sezer vd., 2022).

Pseudocode : Algoritma 1 *Aktor Ürün Bilgileri, İmzalama ve Doğrulama*

function valid_*product*

+ check p_{gb}*=0 ret. h(*p_{gb}*), if not ret. h(*$ptx_{prev.}$*) (*p_{gb} *genesis block)*

+ check $p_{id} \notin p_{idlist}$*, if not ret. false*

+ check $p_{info} \neq 0$*, if not ret. false*

+ if $np_{idlist} \neq p_{idlist}$ *then* $p_{idlist} \leftarrow np_{idlist}$ *(Ürün listesi güncelemesi konum satış bilg vb.)*

+ end if

+ check $a_{id} \neq 0$*, if not ret. false*

+ check $p_{id} \neq 0$*, if not ret. false*

+ $h(ptx_i) \leftarrow hash\ (a_{id}, p_{id}, p_{inf}, p_{time}, h(ptx_{prev.}))$

+ $sign(h(ptx_i)) \leftarrow$ *Eliptik eğri digital imzalama alg. ile imzalama (ECDSA)* $(h(ptx_i))$

+ if $sign(h(ptx_i))$ *is valid then signactor =true, else ret. false*

+ end if

+ check signactor =true, if not ret. false

+ $sig_h(h(ptx_i)) \leftarrow$*signature hash of* $h(ptx_i)$ *(Ürün hash değerinin imzalı hash değeri)*

+ $s_{adr} \leftarrow$*sender actor adress*

+ $verfy(a_{adr}) \leftarrow$*verify* $sig(h(ptx_i))$, $sig_h(h(ptx_i))$

+ if $vefy(a_{adr}) \neq s_{adr}$ *then ret. false*

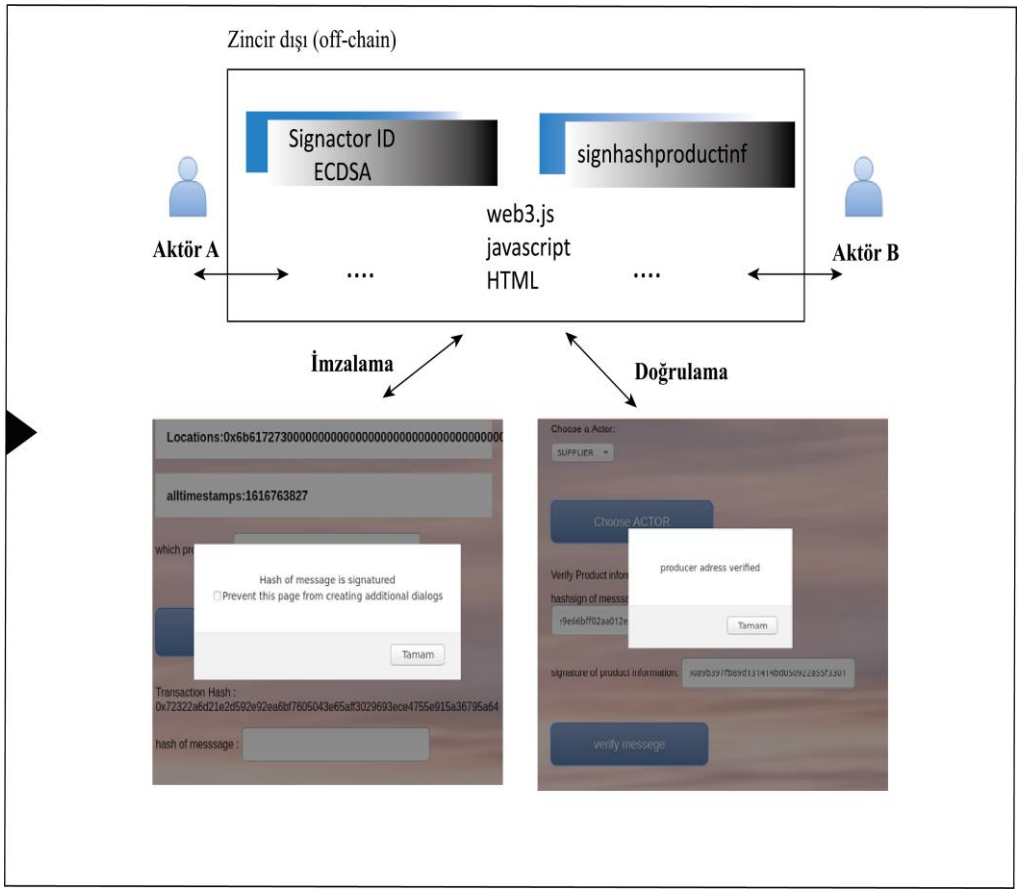
+ end if

+ return true

end function

3.1.1 Dijital İmzalama

Dijital imza, aktörlerin birbirleriyle olan işlem alış-veriş'ini doğrulamak için kullanılmaktadır. Djital imzada kullanılan eliptik eğri digital imza algoritmasında (ECDSA) her aktörün bir açık-özel anahtar çifti vardır. İlgili aktör, zincir dışındaki açık anahtarı ile verilerini sözleşmeye kaydettikten sonra elde ettiği hash değerinin imzasını gerçekleştirmiştir. Şekil 3.3'de gösterilen imzalama, ilgili aktörün kimliğine dayalı olarak kanıtlanmış bir ECDSA ile zincir dışında gerçekleştirilmiştir. İlgili aktörün zincir üzerindeki verilerinin hash değeri ile imzalanmış hash değeri alınır (Tablo 3.1). Bu değer, doğrulama için kullanılacak imzalı hash değerdir. Ayrıca, imzalama test ekranı, sözleşme ve zincir dışı HTML üzerinde ayrıntılı olarak gösterilmiştir.



Şekil 3.3 Zincir Dışında Dijital İmzalama ve Doğrulama (Basitleştirilmiş)

3.1.2 Doğrulama

İşlemlerin geçerliliğinin kanıtlanması, gizliliğin korunması ve dolandırıcılığın önlenmesi amacıyla dijital imza kullanılmış ve sistemdeki her işlemin hash değeri ilgili aktör tarafından imzalanmıştır. Ardından, sözleşmede ürünün hash değerinin imzalı hash değeri üretilir. İmzalı hash değer, zincir dışında ilgili aktörün açık anahtarı ile elde edilir ve imzalı hash değerinin hash değeri ($(sig_h(h(ptx_i)))$) doğrulama için kullanılacak veridir. Doğrulama hem zincir dışı hem de zincir üzerinde gerçekleştirilir. Yani zincir dışında elde edilen imzalı hash değeri ve imza, doğrulama için zincire gönderilir. İlgili aktör, gönderen aktörün adresini özel anahtarla (yani imzalı hash'in hash'i) doğrulayarak işlemi doğrular (Şekil 3.3).

Kısaca, sözleşme Algoritması 1'deki eliptik eğri algoritması ile aktörün imzası ve ürünlerin imzalanmış hash değeri kullanılarak kimlik doğrulama gerçekleştirilir.

3.2 Güvenlik analizi

Mimarimizde mahremiyetin korunmasını iki açıdan özetliyoruz; Birincisi, aktörlerin kimliğini korumak (anonimlik), diğeri ise aktörlerin işlemlerini korumaya odaklanmaktır. Çerçevemizin güvenliği, eliptik eğri kriptografisine (Hankerson et al., 2006) dayanmaktadır. Eliptik eğri kriptografisi, açık anahtar şifreleme sistemine ve ayrıca sonlu bir alan üzerindeki eliptik eğrilerin cebirsel yapılarına dayanan bir şifreleme sistemidir. İşlemlerin güvenliği keccak-256 ($h(ptx_i)$) (Bertoni et al., 2011) kullanılarak sağlanmıştır. Dijital imza (ECDSA) $sign(h(ptx_i))$ zincir dışı aktörler tarafından gerçekleştirilmiştir.

Çalışmamızda açık anahtar, ilgili aktör tarafından imzalanan değerdir ($(sign(h(ptx_i)))$). Özel anahtar, ilgili aktörün ürün bilgisi özet değerinin imzalı özet değeridir ($(sig_h(h(ptx_i)))$).

Tanım 2 Eliptik eğri dijital imza algoritmasını (ECDSA) kısaca hatırlayacak olursak**;** Sonlu alan Fp üzerinde E eliptik eğri olsun, öyle ki $p, q \in E(Fp)$ iki

nokta ve $k \in R$ [1, $n-1$] öyle ki $p = kq$ olsun. Polinom zamanda k sayısını bulmak imkânsızdır (Hankerson et al., 2006).

Aritmetik işlemlerin basitliğine rağmen, çözme ve hesaplama işlemi zordur. Saldırganın sistemi çözebilmesi için ilgili noktada açık anahtarı bilmesi yeterli değildir. Saldırganın başlangıç noktasındaki yeri ve çarpanı bilmesi gerekir. Bu değerleri bulmak için saldırganın tüm değerleri test etmesi gerekir. Saldırgan başlangıç noktasını bilse bile, bu değerleri elde edebilecek çarpanı bulmak için bulduğu başlangıç noktasına kadar açık anahtar noktasından değerleri çıkarması gerekir. Bu durum polinom zamanda gerçekleşememektedir. Bu nedenle, mimarinin güvenliği de ECDSA güvenliğine dayanmaktadır.

Lemma 1 Mimaride, bir saldırgan tarafından polinom zamanda herhangi bir aktörün kimliğini (ID) belirlemek mümkün değildir.

İspat Saldırganın herhangi bir aktör tarafından imzalanan ($sign(h(ptx_i))$) imzalı hash değerini bildiğini varsayalım. Saldırganın aktör kimliğini bilmesi için ayrıca imzalı hash değerinin imzasına $sig_h(h(ptx_i))$ sahip olması ve bu değerleri test etmesi gerekir. ECDLP ve tek yönlü hash fonksiyonu nedeniyle, aktörün kimliğini (a_{adr}) bulmak mümkün değildir. Bu durum anonimlik sağlamaktadır. Sonuç olarak, güvenliğin sadece ECDLP üzerinden tartışılabileceğini söylüyoruz (Hankerson et al., 2006; Silverman and Suzuki, 1998).

Mimaride önemli bir noktanın hatırlatmasını yapalım; aktörün talebine bağlı olarak izlenebilirlik ve anonimlik gerçekleştirilmektedir. Aktörün isteğine bağlı olarak ilgili anahtarlar ile izlenebilirlik sağlanırsa anonimlik ve mahremiyetin sağlanamayacağı unutulmamalıdır.

3.3. Karmaşıklık

Karmaşıklığı (Complexity) hesaplamak için ağdaki aktörlerin sayısı, aktörler tarafından gerçekleştirilen girdi-çıktı işlemlerinin sayısı, dijital imza için kullanılacak anahtarın boyutu gibi terimlere ihtiyacımız bulunmaktadır. Çerçevede ana nokta, aktörler tarafından oluşturulan işlemler ve bu işlemlerin dijital

imzasıdır. Bir diğer nokta da dijital imza sonrası yapılan işlemlerin aktörler tarafından doğrulanmasıdır. Mimaride karmaşıklığı iki açıdan değerlendirebiliriz; Birincisi, hesaplama karmaşıklığıdır (computational complexity). İkincisi ise iletişim karmaşıklığıdır (communication complexity).

3.3.1 Hesaplama karmaşıklığı

Mimaride ağ üzerinde aktörler olduğunu varsayıyoruz. Algoritmadaki her protokol için, işlem başına (per transaction) karmaşıklık, karşılık gelen değişkende doğrusal olarak büyümektedir. Ek olarak, aktörün ağa katılması ve işlemleri sürdürmesi için mevcut protokolleri (imzalama ve doğrulama) kullanmanın hesaplama karmaşıklığı, eliptik eğri algoritmasının anahtar uzunluğuna bağlı olarak doğrusaldır. Ayrıca, bir işlemin hesaplama karmaşıklığına imza protokolü hâkimdir. Algoritmadaki protokollerin hesaplama karmaşıklığı Tablo 3.2'de özetlenmiştir (Sezer vd., 2022).

Tablo 3.2 Mimarinin Karmaşıklığı

Sembol	Açıklama	Detaylar (çerçevedeki protokoller)	Karmaşıklık
N	Aktör sayısı	--	--
K	Anahtar bit uzunluğu (eliptik eğri)	--	--
M	Her aktörün üye sayısı	--	--
A_k	*İşlemlerin sayısı (her aktör için)*	*İşlemlerin oluşturulması*	$O(A_k \times M)$
S_k	*Herbir aktör'ün Imzalaması*	*Dijital imzalama (zincir dışı)* $(sign(h(ptx_i))$	$O(S_k \times M)$
V_k	*Herbir aktör'ün doğrulaması*	*Doğrulama (sözleşmede)* $(verfy(a_{adr}))$	$O(V_k \times M)$

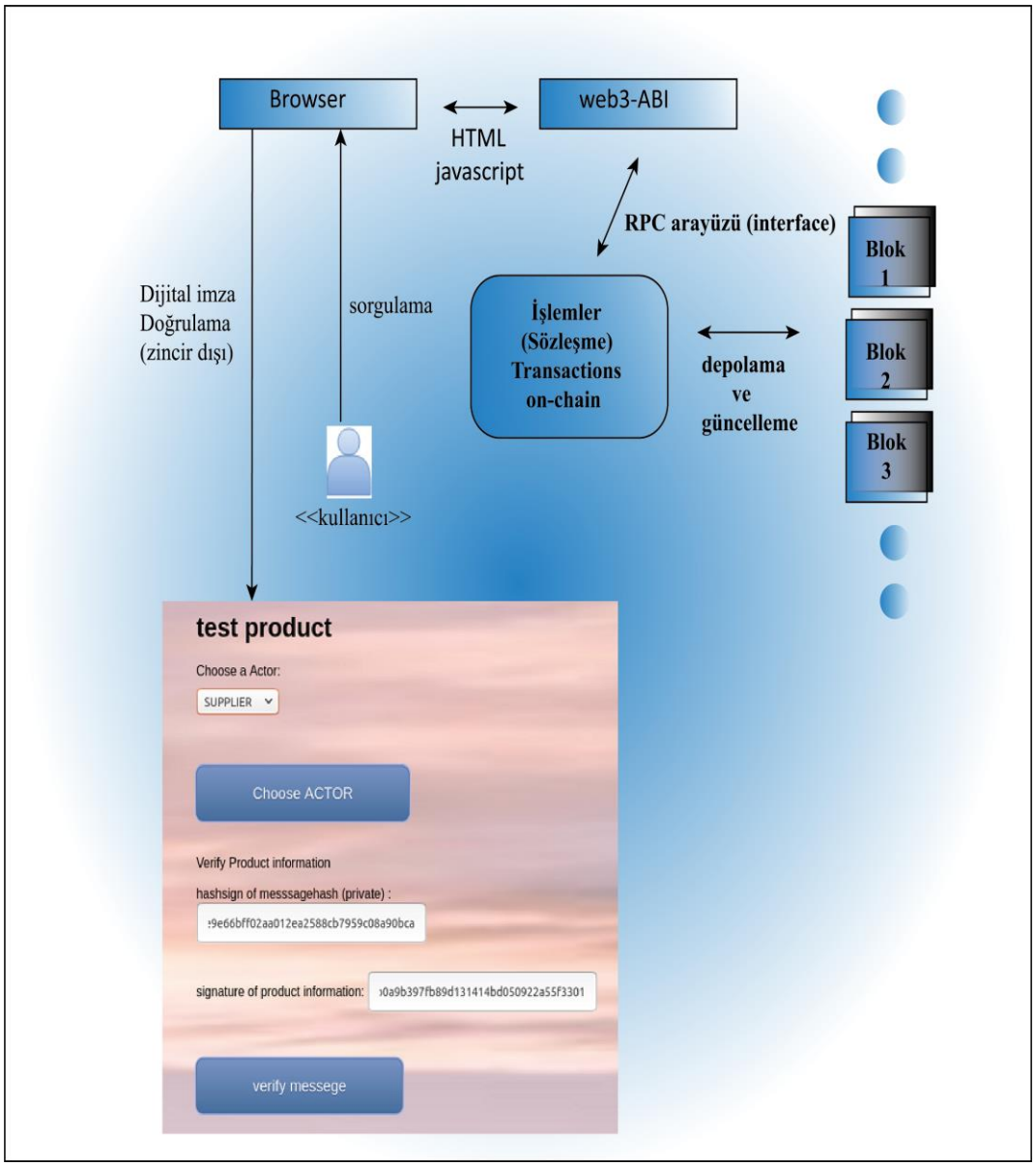
3.3.2 İletişim karmaşıklığı

Ağdaki aktörün, iletişim kurmak istediği diğer aktörlerin adresini elinde tuttuğunu varsayıyoruz. Burada işlemler kullanılan fikirbirliği modeline göre değişiklik göstermektedir. Fikirbirliği modeli, ağdaki düğüm sayısını ve saniyedeki işlem sayısını (tps) temel alır. Zincir üzerinde bir EVM ağı kullandığımız için, fikir birliği modelinin iletişim karmaşıklığı $O(N)$ (Vukolić, 2015; Dinh et al., 2017)'dir. Ek olarak, zincir dışı aktörün zincir üzerindeki her bir işlemi doğrulaması, ağdaki aktörlerin sayısına N ve kimlik doğrulama protokolüne V bağlıdır. Bu nedenle, iletişim karmaşıklığı $O(NxV)$'dir (Sezer vd., 2022).

4. DENEYSEL SONUÇLAR

Bu tez çalışmasında çerçevemizde ürünle ilgili bilgiler üreticiden tüketiciye izlenebilir ve denetlenebilir niteliktedir. Sistemdeki herhangi bir aktör ürün kimliği ile doğrulama ve izlenebilirlik yapılabilmektedir. Aktörlerin kendilerine ait bir adresleri olduğu varsayılmaktadır. Dijital imzalama ve diğer kriptografik işlemler için NIST tarafından güvenli kabul edilen $256 - bit$ anahtar uzunluğu kullanılmaktadır. Sözleşmedeki iş yükünü azaltmak için ise zincir dışı entegrasyonu sağlanmıştır. Blok zincirindeki işlemler değişmez olduğu için dolandırıcılık ve değişiklik mümkün değildir. Çerçevemizin uygulanabilirliğini sağlamak için truffle-ganache-cli, web3 javascript programlama ve web tabanlı (HTML) arayüz kullanılmıştır. Çalışmamız 10 GB ram, 3.0 GHz Intel işlemci üzerinde ubuntu 18.04 işletim sistemi çalıştıran yerel bir bilgisayarda gerçekleştirilmiştir. İncelemeyi kolaylaştıran bir kavram kanıtı (proof-of concept) oluşturulmuştur. Ölçümlerin doğruluğu için algoritma ve protokolleri (Dijital imza, doğrulama) 1000 kez test edilmiştir. Zincir dışındaki güvenlik seviyesini 128 bit, k = 256 (eliptik bir eğri için) olarak belirlenmiştir. Hash fonksiyonu olarak *keccak-256* kullanılmıştır. Önerdiğimiz çerçeveyi entegre köprüler oluşturarak mevcut akıllı sözleşme ile tanımlanan bileşenleri harmanladık. Komut dosyası oluşturma özelliğini düşündüğümüzde Mimarimiz, üst düzey dil desteğine (yani Solidity) sahiptir. Akıllı sözleşmemizi, Ethereum'daki (Wood, 2014) (EVM) uyumlu blok zincirinde konuşlandırılabilen solidity dilinde yazdık. Ethereum platformunda ana programlama dili olan Solidity, sözleşme programları yazmak için tasarlanmış nesne yönelimli bir dildir. Burada, tüm işlemlerin token tabanlı bir para birimi olan ether üzerinden bir maliyeti vardır. Buna gaz ücreti denir. EVM'nin her işlem için bir gaz ücreti vardır. EVM'de gaz maliyeti pahalı bir işlemdir. Ayrıca detayların zincir üzerinde kullanılması ve saklanması da gaz ücretini artırır. Artan gaz maliyetleri ölçeklenebilirlik açısından olumsuzluklara neden olmaktadır. Ayrıca, Ethereum'da yeni blok oluşturma ve mevcut blokların doğrulanması işlemi, ağ durumuna bağlı olarak 15-30 saniye arasında değişmektedir. Bu durumda çalışmamızda gaz ücretinin optimize edilmesi ölçeklenebilirlik açısından olumlu sonuçlar getirecektir.

Ölçeklenebilirlik, genel veya izin defteri (permission-ledger) kullanımı, erişilebilirlik (accessibility) ve gizlilik (privacy) gibi birçok değişkene bağlıdır. Bir açık defter (public-ledger) kullanımında, ölçeklenebilirlik büyük ölçüde gaz maliyetlerine (gas fee) bağlıdır. Ayrıca blok zincirindeki işlem oranlarındaki artış, işlem ücretlerini ve yanıt süresini olumsuz etkilemektedir (Ahmad et al., 2021). Test ekranında, zincir dışında yeni bir ürün eklemek ve zincir dışı ile sözleşme arasındaki köprü için web3 uygulama ara yüzü (web3-API) ‘nü kullandık. İlgili aktörün hesabı varsa açık anahtarı (public-key)(imzalı hash değeri) ve özel anahtarı (private-key) (imzalı hash değerinin hash değeri) kullanarak doğrulamayı gerçekleştirir. Hesabı yoksa, sistem tarafından istenen ilgili bilgilerle ilk kayıt yapılır. Ardından ilgili aktör talep edilen bilgileri sisteme aktarır ve işlemlerin kök hash değeri ECDSA tarafından diğer aktöre gönderilmek üzere imzalanır. Tüm bu işlemler sözleşmedeki gaz ücretini ve iş yükünü arttırdığı için zincir dışı entegre olay bazlı (event-based) sözleşmeler kullanarak gerçekleştirdik. Ayrıca, zincir dışı bir akıllı sözleşmeyi tanıtmak için EVM'de RPS arayüzü ile sözleşme-ABI kullandık (Şekil 4.1). Sistemi kolayca yönetmek için web tabanlı araçlar da kullandık. Olayların (events) kullanımında herhangi bir depolama olmasa bile blokzincir üzerinde kolaylıkla gözlemlenebilir ve doğrulanabilirdir.

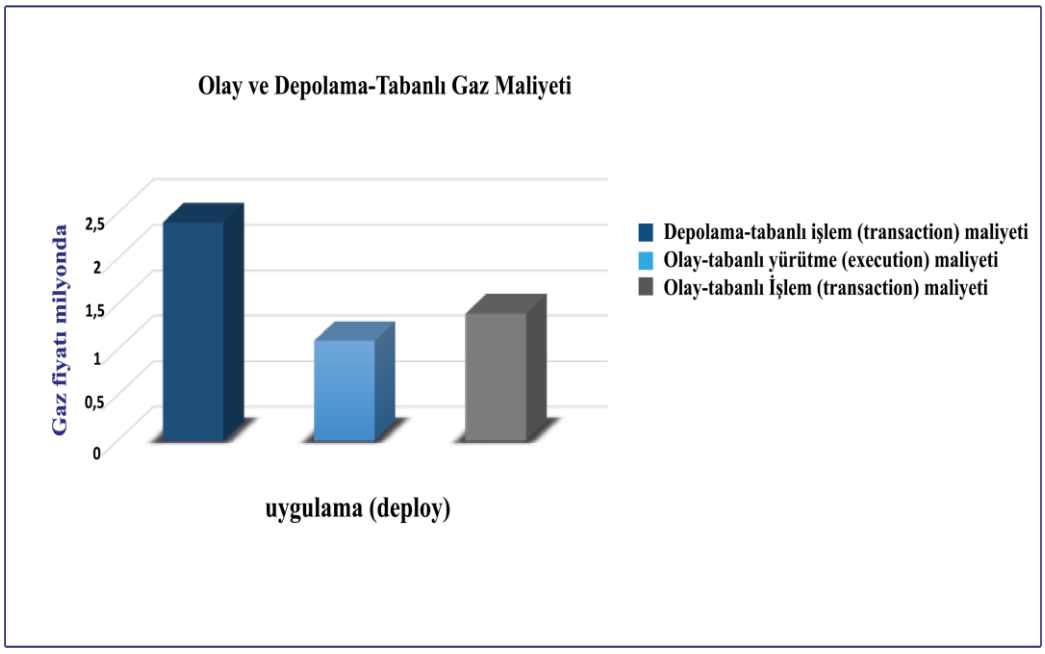


Şekil 4.1 Sistem Şeması, Zincir Dışı Ve Zincir Üzerinde Yürütülen Blok Zinciri Uygulamasının Test Ekranı.

Sözleşmemizde, uygulama (deploy) ve yürütme (execution) maliyetlerini birbirinden ayırıyoruz. Sözleşme üzerinde belirli ürün özelliklerinin uygulanması gerektiğinden dolayı, bunları sözleşmede sakladık. Ayrıca hem olayları kullanarak hem de sözleşmedeki tüm işlemleri kullanarak gaz ücretini karşılaştırdık. Şekil 4.2'da görüldüğü gibi, olay bazlı sözleşmeler (event-based-contract), depolama bazlı sözleşmelere (storage-based-contract) kıyasla önemli kod performansı sağlayarak işlem ücretini düşürürken gaz ücretini de önemli ölçüde düşürdü. Ayrıca bir işlemin oluşturulması ve onaylanması, ilgili aktörün girdi-çıktı işlem sayısı ile orantılıdır. Girdi-çıktı işlemlerinin miktarı arttıkça, işlemin hem

oluşturulması hem de doğrulanması için yürütme süresi doğrusal olarak artar. Ancak, doğrulamadaki çalışma zamanı artışı, oluşturmadan daha yavaştır (Şekil 4.3). Çünkü ilgili aktörün girdi işlemleri için sisteme girmesinden sonra, zincir dışı dijital imzalama işlemini gerçekleştirir ve çıktı işlemini oluşturur. Dolayısıyla olay bazlı ve depolama bazlı sözleşmede gaz ücretinin, girdi sayısındaki artış sonucu yürütme süresinde doğrusal (lineer) bir artış gözlendiğinden, aktörün işlem sayısı arttıkça ilgili aktörün girdi-çıktı işlemlerinin doğrusal olarak arttığını söyleyebiliriz (Sezer vd., 2022).

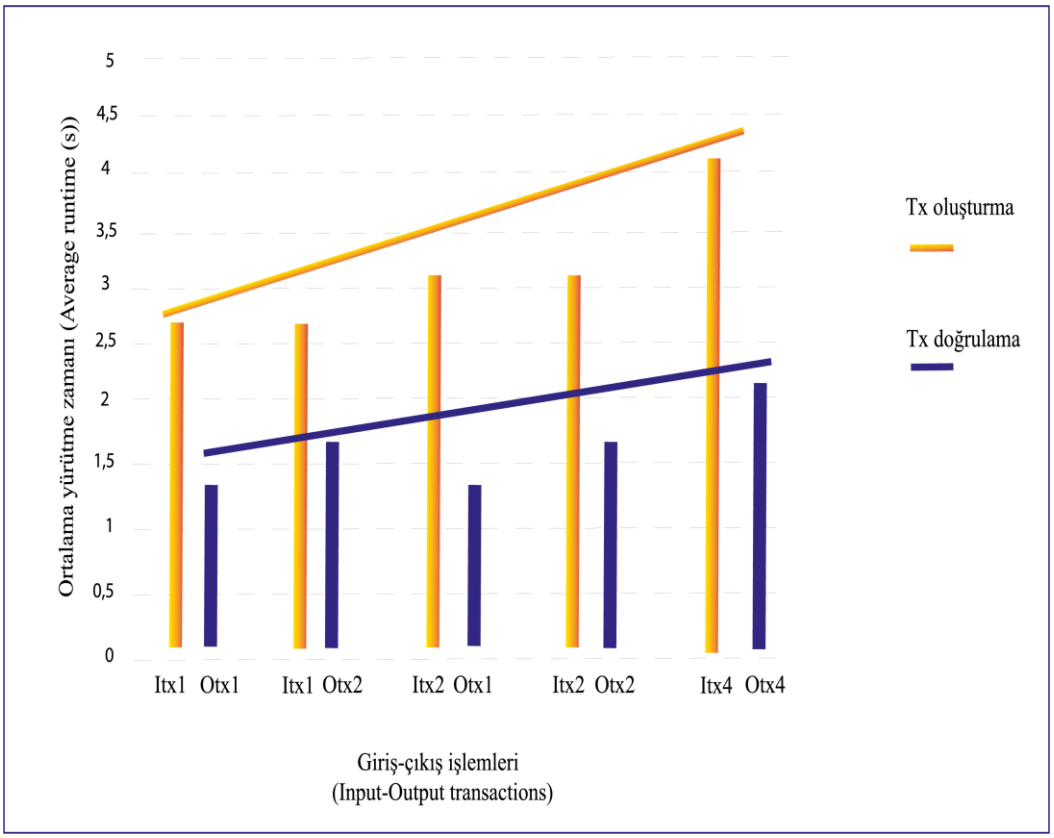
İletişim maliyetinin (communication cost) ilgili hesabın, blok başlığının ve iletişim protokolü başlığının veri yapısının boyutundan kaynaklanmaktadır. Dolayısıyla olay bazlı ve depolama bazlı sözleşmenin gaz ücretindeki performans sonucunda, olay bazlı sözleşmede iletişim maliyetinin daha az olduğu açıktır (Şekil 4.4).



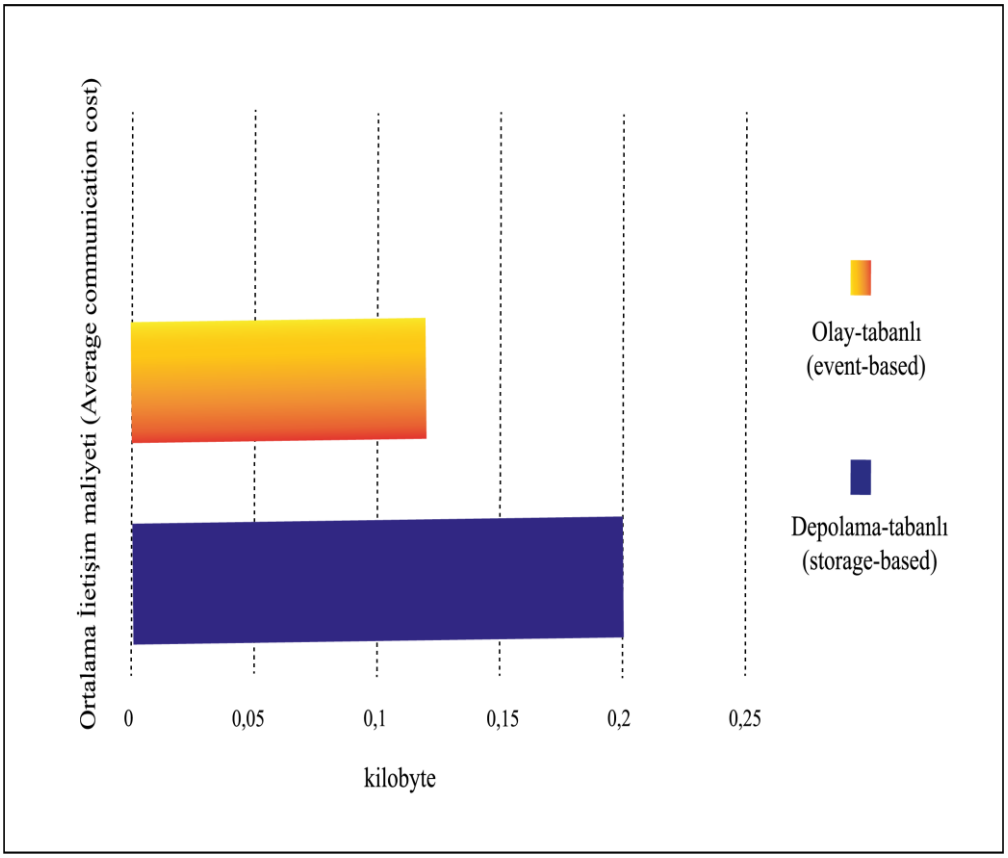
Şekil 4.2 Olay ve Depolamaya Tabanlı (Event-Storage-Based) Sözleşmelerin Ortalama Gaz Maliyeti

Çalışmamızı ölçeklenebilirlik konusunda analiz ettiğimizde yukarıda elde ettiğimiz ölçümleri kullanabiliriz. Bir işlemin oluşturulmasına ve doğrulanmasına bağlı olarak, işlem sayısı arttıkça ilgili aktörün girdi ve çıktı işlem sayısının lineer olarak arttığını belirtmiştik. PoW konsensüsünü kullanan Ethereum'un yaklaşık

15s blok süresine ve saniyede ortalama 15-30 işleme sahip olduğunu varsayıyoruz. Bu, Ethereum için gerçekçi bir hipotezdir. Daha sonra bu fikir birliği süresini mevcut kriptografik protokollerin (yani Dijital imza (ECDSA), Doğrulama) zamanı ile birleştirdik. Aynı mimaride yazdığımız olay tabanlı ve depolama tabanlı iki farklı koddan da anlaşılacağı üzere çalışmamamızın hesaplama ve iletişim maliyeti, kriptografik primitifler kullanımına rağmen olay tabanlı sözleşme Ethereum'da depolama tabanlı sözleşmenin performansından daha yüksektir (Şekil 4.2). Ayrıca, tedarik zincir'de gizliliği koruyan bir sistem sağlayan başka bir başarılı mimariyle (Lin et al., 2020) karşılaştırdığımızda, ilgili heterojen mimarinin Ethereum tabanlı sistemde Zaman ve iletişim maliyeti açısından bakacak olursak, zaman maliyetinin daha düşük ve iletişim maliyetinin daha yüksek olduğu belirtilmektedir. Ayrıca iletişim maliyetinin yüksek olmasının sebebinin mimaride kullanılan kriptografik ilkellerden kaynaklandığı ifade edilmiştir. Test sonucunda yukarıda bahsettiğimiz gibi mimarimizde kriptografik protokoller kullanılsa da iletişim maliyeti Ethereum'un depolama tabanlı sözleşmesine göre daha düşüktür. Dolayısıyla mimarimizde kullandığımız olay tabanlı sözleşmenin zincir dışı entegrasyonu ile iletişim maliyetinin diğer mimariye göre daha düşük olduğunu söyleyebiliriz (Şekil 4.3, 4.4). Ayrıca hem olay tabanlı akıllı sözleşme kullanımı hem de zincir dışı kullanım, akıllı sözleşmedeki iş yükünü azaltmak için gaz ücretini önemli ölçüde azaltmıştır. Olay tabanlı akıllı sözleşmelerin zincir dışı ile entegrasyonu sonucunda elde edilen veriler, ölçeklenebilirlik konusunda bize olumlu sonuçlar vermiştir. Ayrıca, önceki bölümlerde tartıştığımız gibi, aktörler arasında göz ardı edilen gizlilik hassasiyeti, zincir dışı dijital imzalama ve zincir üstü doğrulama kullanılarak sağlanmıştır. Aynı zamanda mimari sayesinde aktörler tüm ürün bilgilerini şeffaf bir şekilde izleyebilmektedir.



Şekil 4.3 İşlemin Oluşturulması ve Doğrulanmasının Hesaplama Süresi.



Şekil 4.4 Olay ve Depolama Tabanlı Sözleşmenin İletişim Maliyeti.

Son zamanlarda, Ethereum 2.0 olarak adlandırılan hisse kanıtı (PoS) fikirbirliği protokolüne geçtiği belirtilmektedir. Ayrıca, Algorand (Gilad et al., 2017) ve Avalanche (Rocket et al., 2019) gibi geliştirilen yeni fikirbirliği protokollerinin saniyede 100 kata kadar işlem (tps) ile sonuçlandığına dair öneriler bulunmaktadır. Ayrıca, zincir dışı entegre sistemi kullanılarak olay bazlı sözleşme ve iş yükünün azalması nedeniyle aynı platformda yazılan akıllı sözleşmeye kriptografik protokollerin eklenmesiyle iletişim ve zaman maliyetlerinin Ethereum ve diğer mimarilere göre daha düşük olduğu gözlemlenmiştir. Bu nedenle çerçevemiz bu fikirbirliği protokolleri ile güvenle kullanılabilir ve kullanım kolaylığı ve performansı, özellikle anonimlik ve şeffaflık dengesi nedeniyle tercih edildiği düşünülmektedir. Ayrıca çerçevemiz gerçek zamanlı (real-time) izlenebilirlikte sağlamıştır.

4.1 Detaylar

Mevcut blok zinciri tabanlı tedarik zincir modelinde, RFID teknolojisi genellikle üretim, işleme, depolama ve dağıtım aşamalarında veri toplamak ve paylaşmak için kullanılmaktadır. Ancak orijinal verilerin doğrudan zincir üzerinde saklanması veri gizliliği hassasiyetine neden olmaktadır. Bu nedenle herhangi bir işletmenin ticari çıkarları olumsuz etkilenebilmektedir. Bu durumda, güvenli ve gizliliği koruyan bir tedarik zincir modeli önerilmektedir. Ancak tedarik sürecinde kullanıcı hassasiyeti ve veri gizliliği düşünüldüğünde, bu mimarilerde anonimlik ve şeffaflığı dengelemek en önemli faktördür. Bu noktada mimarimiz, belirtilen dengeye sahip olduğu ve gizliliği koruyan bir tedarik zincir modeli sunduğu için önerilmektedir. Bu mimarinin altında yatan anonimlik, gizlilik ve şeffaflık özellikleri ile anonimlik ve şeffaflık parametreleri arasında bir dengeye sahip olması nedeniyle gizlilik ve güvenilirlik gerektiren uygulamalarda kullanılabildiğini söyleyebiliriz. Mimaride, akıllı sözleşme işlevi EVM'nin işlevini devralır, ancak zincir dışı kullanarak zincir üzerindeki iş yükünü azaltır. Bu durum, mimari içinde uygulama dağıtmanın güvenliğini sağlamaktadir. Mimari örneği tedarik üzerinde verilmiştir, ancak önceki bölümlerde de belirtildiği üzere mimarimizin kullanımı bu uygulamalarla sınırlı değildir.

Geçmiş 10 yılda gerçekleştirilen çalışmalar incelendiğinde, tedarik zincir izlenebilirliği (Kang and Lee, 2013; Van Der Vorst et al., 2009) ve mahremiyeti koruma teknikleri (Han et al.,2015; Efthymiou and Kalogridis,2010) ile ilgili farklı yöntemlerle karşılaşılmaktadır. Bu yöntemler daha sonra blok zincir (Min, 2019; Ahmad et al., 2021; Schmidt and Wagner, 2019; Dwivedi et al., 2020; Dietrich et al., 2021; Sunmola, 2021) ile entegre edilerek sunulmuştur. Ayrıca diğer çalışmaların çoğunun aktörlerin verilerini açık olarak paylaştığı veya gizliliği içeren merkezi olmayan bir SC uygulamasına geçildiği ve kısmi mahremiyetin hayata geçirildiği görülmektedir (Lin et al., 2020). Bu durum rekabetçi piyasalarda çelişkileri de beraberinde getirebilmektedir. Başka bir deyişle, çalışmaların çoğu doğrulanabilirlik ve denetlenebilirlik ile ilgili hassas endişeleri ele alamamaktadır. Çalışmamızda, tedarik zincirde gizliliğe duyarlı merkezi olmayan izlenebilirlik sağlayan bir sistem sunduk. Yetkili kurumun anahtar paylaşım talebine bağlı olarak, aktörlerin verilerini şeffaf bir şekilde izleyebilen, gizliliğe duyarlı doğrulanabilirlik ve denetlenebilirliği içeren bir çerçeve tasarladık. Yapılan pilot testler ile sistemin çalışır durumda olduğunu göstermiş olduk. Ölçeklenebilirlikte daha iyi performans göstermek için olay tabanlı akıllı sözleşmeyi ve web3 tabanlı zincir dışı çerçeveyi kullandık. Böylece, deneysel sonuçlarda tartışıldığı gibi, sözleşme üzerindeki işlem yükü azaltılarak ve olay tabanlı bir akıllı sözleşme kullanılarak gaz ücreti optimize edilmiştir. Ayrıca ilgili aktörler, sistemdeki ürüne özel tüm işlemleri izleyebilir ve kontrol edebilmektedir.

Deneysel çalışmalarımıza dayanarak, tedarik zincirde imzalama ve doğrulama başarıyla tamamlanmıştır. Ancak, doğrulama ve imzalamada yan zincirlerin kullanılmasıyla alan karmaşıklığının (space complexity) daha da en aza indirilebileceği tahmin edilmektedir. Çünkü yan zincirler, şifrelenmiş verilerin ayrı bir yerde saklanmasına izin vermektedir (Back et al., 2014). Bu durum bize istenilen sonucu verebilir.

5. SONUÇ

Bu tez çalışmasında, zincir içi ve zincir dışı akıllı sözleşmeler kullanarak anonimlik ve şeffaflığı dengeleyen ve izlenebilirlik ve gizliliği sağlayan izinli blok zinciri mimarisine dayalı yeni bir çerçeve hazırladık. Verimliliği artırmak için sözleşmede doğrulama ve zincir dışında ECDSA protokolünü kullanarak dijital imzalama gerçekleştirdik. Böylece sistemin bütünlüğü ve inkar edilemezliği sağlanmaktadır. Deneysel sonuçlar, yetkili kurumun anahtar paylaşım talebine bağlı olarak hem anonimlik hem de izlenebilirlik sağlayan, kolay uygulanabilir, denetlenebilir bir tedarik zincir modeli olabileceğini göstermiştir. Ayrıca mimari, gıda tedariğinden ilaç tedariğine kadar her alanla kolayca entegre olma potansiyeline sahiptir ve aynı zamanda mahremiyeti koruyan birçok uygulama alanında kullanılabilirdir. Gelecekteki araştırmalar, gerçek bir bağlamda kimlik doğrulama ve imzalama ve uygulama için yan zincirler kullanılarak alan karmaşıklığının daha da azaltılabileceğini içermektedir. Ayrıca tedarik bileşeninde kullanılacak IoT cihazlarının sınırlı alanı ve düşük gücü nedeniyle, mevcut bir protokolün hesaplama maliyetini azaltmak için *keccak-256* gibi mevcut hash fonksiyonları yerine hafif hash fonksiyonları bir seçenek olarak sunularak gizliliği içeren hafif blokzincir mimarisinin oluşturulması planlanmaktadır.

KAYNAKLAR DİZİNİ

Abbas, K., Tawalbeh, L. A. A., Rafiq, A., Muthanna, A., Elgendy, I. A., El-Latif, A., & Ahmed, A. (2021). Convergence of blokzincir and IoT for secure transportation systems in smart cities. *Security and Communication Networks*, *2021*.

Abeyratne, S. A., & Monfared, R. P. (2016). Blokzincir ready manufacturing supply chain using distributed ledger. *International journal of research in engineering and technology*, *5*(9), 1-10.

Abd El-Latif, A. A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., & Peng, J. (2021). Quantum-inspired blokzincir-based cybersecurity: securing smart edge utilities in IoT-based smart cities. *Information Processing & Management*, *58*(4), 102549.

Ahmad, R. W., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2021). Blokzincir for aerospace and defense: Opportunities and open research challenges. *Computers & Industrial Engineering*, *151*, 106982.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., & Yellick, J. (2018). Hyperledger fabric: a distributed operating system for permissioned blokzincirs. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).

Akkerman, R., Farahani, P., & Grunow, M. (2010). Quality, safety and sustainability in food distribution: a review of quantitative operations management approaches and challenges. *OR spectrum*, *32*(4), 863-904.

Amrioui, S., Malhéné, N., & Deschamps, J. C. (2012). Traceability in collaborative logistics: How to use EPCglobal solution in transport reconfiguration. In 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST) (pp. 1-7). IEEE.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust* (pp. 164-186). Springer, Berlin, Heidelberg.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019). SoK: Consensus in the age of blokzincirs. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (pp. 183-198).

KAYNAKLAR DİZİNİ (DEVAM)

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blokzincir innovations with pegged sidechains. *URL: http://www. opensciencereview. com/papers/123/enablingblokzincir-innovations-with-pegged-sidechains*, *72*.

Badra, M., & Zeadally, S. (2014). Design and performance analysis of a virtual ring architecture for smart grid privacy. *IEEE transactions on information forensics and security*, *9*(2), 321-329.

Baliga, A. (2017). Understanding blokzincir consensus models. *Persistent*, *4*(1), 14.

Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2011). The keccak sha-3 submission. *Submission to NIST (Round 3)*, *6*(7), 16.

Bitcoin Mining Centralization, https://www.bitcoinmining.com/bitcoin-mining-centralization, (Erişim tarihi 21. Mayıs 2022).

Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: an introduction. R3 CEV, August, 1(15), 14.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

Boneh, D. (1998). The decision Diffie-hellman problem. In *International algorithmic number theory symposium* (pp. 48-63). Springer, Berlin, Heidelberg.

Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance. In *OsDI* (Vol. 99, No. 1999, pp. 173-186).

Cao, X., Zhang, J., Wu, X., & Liu, B. (2022). A survey on security in consensus and smart contracts. *Peer-to-Peer Networking and Applications*, 1-21.

Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018). Blokzincir-based traceability in Agri-Food supply chain management: A practical implementation. In 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany) (pp. 1-4). IEEE.

Chan, F. T., Chan, H. K., Lau, H. C., & Ip, R. W. (2006). An AHP approach in benchmarking logistics performance of the postal industry. Benchmarking: An International Journal.

KAYNAKLAR DİZİNİ (DEVAM)

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017). Blockbench: A framework for analyzing private blokzincirs. In *Proceedings of the 2017 ACM international conference on management of data* (pp. 1085-1100).

Dietrich, F., Ge, Y., Turgut, A., Louw, L., & Palm, D. (2021). Review and analysis of blokzincir projects in supply chain management. *Procedia computer science*, *180*, 724-733.

Dhumwad, S., Sukhadeve, M., Naik, C., Manjunath, K. N., & Prabhu, S. (2017). A peer-to-peer money transfer using SHA256 and Merkle tree. In 2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM) (pp. 40-43). IEEE.

Douceur, J. R. (2002). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.

Duffield, E., & Diaz, D. (2018). Dash: A payments-focused cryptocurrency. *Whitepaper, https://github. com/dashpay/dash/wiki/Whitepaper*.

Dwivedi, S. K., Amin, R., & Vollala, S. (2020). Blokzincir based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications*, *54*, 102554.

Dwivedi, S. K., Amin, R., & Vollala, S. (2020). Blokzincir based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications*, *54*, 102554.

Eberhardt, J., & Tai, S. (2017). On or off the blokzincir? Insights on off-chaining computation and data. In *European Conference on Service-Oriented and Cloud Computing* (pp. 3-15). Springer, Cham.

Efthymiou, C., & Kalogridis, G. (2010). Smart grid privacy via anonymization of smart metering data. In *2010 first IEEE international conference on smart grid communications* (pp. 238-243). IEEE.

Ekparinya, P., Gramoli, V., & Jourjon, G. (2018). Impact of man-in-the-middle attacks on ethereum. In *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)* (pp. 11-20). IEEE.

KAYNAKLAR DİZİNİ (DEVAM)

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436-454). Springer, Berlin, Heidelberg.

Expósito, I., Gay-Fernández, J. A., & Cuiñas, I. (2013). A complete traceability system for a wine supply chain using radio-frequency identification and wireless sensor networks [wireless corner]. *IEEE Antennas and Propagation Magazine*, *55*(2), 255-267.

Eyal, I. (2015). The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy* (pp. 89-103). IEEE.

Garay, J., Kiayias, A., & Leonardos, N. (2015). The bitcoin backbone protocol: Analysis and applications. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 281-310). Springer, Berlin, Heidelberg.

Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *Acm Sigact News*, *33*(2), 51-59.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles* (pp. 51-68).

Grunert, K. G., Hieke, S., & Wills, J. (2014). Sustainability labels on food products: Consumer motivation, understanding and use. *Food policy*, *44*, 177-189.

Guegan, D. (2017). Public blokzincir versus private blockhain.

Han, S., Zhao, S., Li, Q., Ju, C. H., & Zhou, W. (2015). PPM-HDA: privacy-preserving and multifunctional health data aggregation with fault tolerance. *IEEE Transactions on Information Forensics and Security*, *11*(9), 1940-1955.

Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.

Helo, P., & Shamsuzzoha, A. H. M. (2020). Real-time supply chain—A blokzincir architecture for project deliveries. *Robotics and Computer-Integrated Manufacturing*, *63*, 101909.

Jansma, N., & Arrendondo, B. (2004). Performance comparison of elliptic curve and rsa digital signatures. *nicj. net/files*.

KAYNAKLAR DİZİNİ (DEVAM)

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*, *1*(1), 36-63.

J Michael Martinez de Andino, 2014 ‘’Counterfeits in the Supply Chain: A Big Problem and it’s Getting Worse’’, url:htpp//www.industryweek.com/inventory-management/counterfeits-supply chain-big-problem-and-its-getting-worse (Erişim tarihi:20 Nisan 2022).

Kang, Y. S., & Lee, Y. H. (2013). Development of generic RFID traceability services. *Computers in industry*, *64*(5), 609-623.

Karlsen, K. M., Sørensen, C. F., Forås, F., & Olsen, P. (2011). Critical criteria when implementing electronic chain traceability in a fish supply chain. Food Control, 22(8), 1339-1347.

Khan, S., Haleem, A., Khan, M. I., Abidi, M. H., & Al-Ahmari, A. (2018). Implementing traceability systems in specific supply chain management (SCM) through critical success factors (CSFs). Sustainability, 10(1), 204.

Kerry, C. F., & Director, C. R. (2013). FIPS PUB 186-4 federal information processing standards publication digital signature standard (DSS).

Kim, M., & Chai, S. (2017). The impact of supplier innovativeness, information sharing and strategic sourcing on improving supply chain agility: Global supply chain perspective. *International Journal of Production Economics*, *187*, 42-52.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blokzincir model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

Kolb, J., AbdelBaky, M., Katz, R. H., & Culler, D. E. (2020). Core concepts, challenges, and future directions in blokzincir: A centralized tutorial. *ACM Computing Surveys (CSUR)*, *53*(1), 1-39.

Lewis., A 2016, ‘’A gentle introduction to smart contracts’’. url: https://bitsonblocks.net/2016/02/01/gentle-introduction-smart-contracts/ (Erişim Tarihi: 20 Haziran 2022).

KAYNAKLAR DİZİNİ (DEVAM)

Li, D., Kehoe, D., & Drake, P. (2006). Dynamic planning with a wireless product identification technology in food supply chains. *The International Journal of Advanced Manufacturing Technology*, *30*(9), 938-944

Lin, C., He, D., Huang, X., Xie, X., & Choo, K. K. R. (2020). PPChain: A privacy-preserving permissioned blokzincir architecture for cryptocurrency and other regulated applications. *IEEE Systems Journal*, *15*(3), 4367-4378.

Lin, C., He, D., Zhang, H., Shao, L., & Huang, X. (2021). Privacy-enhancing decentralized anonymous credential in smart grids. *Computer Standards & Interfaces*, *75*, 103505.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (n.d.). Making Smart Contracts Smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 254–269). ACM.

Ma, S., Deng, Y., He, D., Zhang, J., & Xie, X. (2020). An efficient NIZK scheme for privacy-preserving transactions over account-model blokzincir. *IEEE Transactions on Dependable and Secure Computing*, *18*(2), 641-651.

Mai, N., Bogason, S. G., Arason, S., Árnason, S. V., & Matthíasson, T. G. (2010). Benefits of traceability in fish supply chains–case studies. British Food Journal.

Memon, M. S., Lee, Y. H., & Mari, S. I. (2015). Analysis of traceability optimization and shareholder's profit for efficient supply chain operation under product recall crisis. *Mathematical Problems in Engineering*, *2015*.

Miller, V. S. (1985). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Springer, Berlin, Heidelberg.

Min, H. (2019). Blokzincir technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45.

Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4, 2.

Naor, M. (2003). On cryptographic assumptions and challenges. In *Annual International Cryptology Conference* (pp. 96-109). Springer, Berlin, Heidelberg.

Nicolas Van Saberhagen and Nicolas van Saberhagen, 2013 "Cryptonote v 2.0." In: Self-published, pp. 1–20. url: https://cryptonote.org/whitepaper.pdf. (Erişim tarihi Şubat 2022)

KAYNAKLAR DİZİNİ (DEVAM)

Nguyen, G. N., Le Viet, N. H., Elhoseny, M., Shankar, K., Gupta, B. B., & Abd El-Latif, A. A. (2021). Secure blokzincir enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *Journal of parallel and distributed computing*, *153*, 150-160.

Óskarsdóttir, K., & Oddsson, G. V. (2019). Towards a decision support framework for technologies used in cold supply chain traceability. *Journal of Food Engineering*, *240*, 153-159.

Pan, S., Trentesaux, D., McFarlane, D., Montreuil, B., Ballot, E., & Huang, G. Q. (2021). Digital interoperability and transformation in logistics and supply chain management. *Computers in Industry*, *129*, 103462.

Peck, M. E. (2017). Blokzincir world-Do you need a blokzincir? This chart will tell you if the technology can solve your problem. IEEE Spectrum, 54(10), 38-60.

Pizzuti, T., Mirabelli, G., Grasso, G., & Paldino, G. (2017). MESCO (MEat Supply Chain Ontology): An ontology for supporting traceability in the meat supply chain. Food Control, 72, 123-133.

Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blokzincir technology in supply chain management. *Future Internet*, *11*(7), 161.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

Rocket, T., Yin, M., Sekniqi, K., van Renesse, R., & Sirer, E. G. (2019). Scalable and probabilistic leaderless BFT consensus through metastability. *arXiv preprint arXiv:1906.08936*.

Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, *7*, 50759-50779.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE symposium on security and privacy* (pp. 459-474). IEEE.

Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blokzincir-based soybean traceability in agricultural supply chain. *Ieee Access*, *7*, 73295-73305.

KAYNAKLAR DİZİNİ (DEVAM)

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the attack surface of blokzincir: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 1977-2008.

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 515-532). Springer, Berlin, Heidelberg.

Schmidt, C. G., & Wagner, S. M. (2019). Blokzincir and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management*, *25*(4), 100552.

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Proceedings First International Conference on Peer-to-Peer Computing* (pp. 101-102). IEEE.

Sezer, B. B., Topal, S., & Nuriyev, U. (2022). TPPSUPPLY: A traceable and privacy-preserving blokzincir system architecture for the supply chain. *Journal of Information Security and Applications*, *66*, 103116.

Sezer, B. B., and Nuriyev, U. (2020). Blockchaın Scalabılıty and Dıstrıbuted Ledger Technologıes, Materials International Scientific II Conference for the "*Informatıon systems and technologıes achıevements and perspec*tıves"**,** Sumgait State University, Sumgait, Azerbaijan, July 09-10, 2020, pp. 8-11.

Silverman, J. H., & Suzuki, J. (1998). Elliptic curve discrete logarithms and the index calculus. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 110-125). Springer, Berlin, Heidelberg.

Simmons, G. J. (1979). Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR), 11(4), 305-330.

Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blokzincir-based traceability: An overview with demonstration. *Computers & Industrial Engineering*, *150*, 106895.

Steffen, S., Bichsel, B., Gersbach, M., Melchior, N., Tsankov, P., & Vechev, M. (2019, November). zkay: Specifying and enforcing data privacy in smart contracts. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 1759-1776).

KAYNAKLAR DİZİNİ (DEVAM)

Sunmola, F. T. (2021). Context-aware blokzincir-based sustainable supply chain visibility management. *Procedia Computer Science*, *180*, 887-892.

Szabo N., (1994). ‘’Smart Contracts’’.url: http://szabo.best.vwh.net/smart.contracts.html, (Erişim Tarihi 12 Ocak 2022)

Trienekens, J., & Zuurbier, P. (2008). Quality and safety standards in the food industry, developments, and challenges. *International journal of production economics*, *113*(1), 107-122.

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, Blokzincir & Internet of things. In 2017 International conference on service systems and service management (pp. 1-6). IEEE.

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blokzincir technology. In 2016 13th international conference on service systems and service management (ICSSSM) (pp. 1-6). IEEE.

Tsanos, C. S., & Zografos, K. G. (2016). The effects of behavioural supply chain relationship antecedents on integration and performance. *Supply Chain Management: An International Journal*.

Tse, D., Zhang, B., Yang, Y., Cheng, C., & Mu, H. (2017, December). Blokzincir application in food supply information security. In 2017 IEEE international conference on industrial engineering and engineering management (IEEM) (pp. 1357-1361). IEEE

Van Der Vorst, J. G., Tromp, S. O., & Zee, D. J. V. D. (2009). Simulation modelling for food supply chain redesign; integrated decision making on product quality, sustainability and logistics. *International Journal of Production Research*, *47*(23), 6611-6631.

Van Wingerde, M. (2017). Blokzincir-enabled self-sovereign identity. *Master's thesis*.

Vo, V. D., Mainetti, N., & Fenies, P. (2016). Traceability and transaction governance: a transaction cost analysis in seafood supply chain. In Supply Chain Forum: An International Journal (Vol. 17, No. 3, pp. 125-135). Taylor & Francis

Vukolić, M. (2015). The quest for scalable blokzincir fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Springer, Cham.

KAYNAKLAR DİZİNİ (DEVAM)

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

Wang, L., Kwok, S. K., & Ip, W. H. (2010). A radio frequency identification and sensor-based system for the transportation of food. *Journal of Food Engineering*, *101*(1), 120-129.

Yan, C., Huanhuan, F., Ablikim, B., Zheng, G., Xiaoshuan, Z., & Jun, L. (2018). Traceability information modeling and system implementation in Chinese domestic sheep meat supply chains. *Journal of Food Process Engineering*, *41*(7), e12864.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). Modeling the impact of network connectivity on consensus security of proof-of-work blokzincir. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications* (pp. 1648-1657). IEEE.

Xiong, Z., Feng, S., Niyato, D., Wang, P., & Han, Z. (2018, May). Optimal pricing-based edge computing resource management in mobile blokzincir. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

Xu, P., Lee, J., Barth, J. R., & Richey, R. G. (2021). Blokzincir as supply chain technology: considering transparency and security. *International Journal of Physical Distribution & Logistics Management*.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blokzincir as a software connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182-191). IEEE.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., & Rimba, P. (2017). A taxonomy of blokzincir-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA)* (pp. 243-252). IEEE

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blokzincir. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34.

Zhang, C., Xu, C., Sharif, K., & Zhu, L. (2021). Privacy-preserving contact tracing in 5G-integrated and blokzincir-based medical applications. *Computer Standards & Interfaces*, *77*, 103520.

KAYNAKLAR DİZİNİ (DEVAM)

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blokzincir challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.

Zhou, Z., Gong, J., He, Y., & Zhang, Y. (2017). Software defined machine-to-machine communication for smart energy management. *IEEE Communications Magazine*, *55*(10), 52-60.

TEŞEKKÜR

Öncelikle tez çalışmam boyunca bana rehberlik eden ve danışmanlığımı üstlenen Prof. Dr. Urfat NURİYEV'e ve fikirleriyle yoluma ışık olan ikinci danışmanım Doç. Dr. Selçuk TOPAL'a teşekkürlerimi sunarım.

Başta üniversitemiz olmak üzere ülkemize bilimsel alanda katkı sağlamak ve akademik çalışmalar yapmak için desteklerini esirgemeyen Fen Bilimleri Enstitü Müdürü Prof. Dr. Bahri BAŞARAN'a, müdür yardımcılarımız Prof. Dr. Ali MERT ile Dr. Öğr. Üyesi Aysun BALTACI'ya ve yaptığım işi hakkıyla bitireceğime inanan desteklerini esirgemeyen Enstitü Sekreteri Osman TORUN'a teşekkürlerimi sunuyorum.

Doktora çalışmam boyunca bana gösterdiği sonsuz desteği için Dr. Hasret TÜRKMEN'e teşekkür ederim.

Son olarak tüm yaşamım boyunca beni destekleyen anne ve babama teşekkürü bir borç bilirim.

31/ 08 / 2022

Bora Buğra SEZER

ÖZGEÇMİŞ

BORA BUĞRA SEZER , Araş.Gör.

İLETİŞİM BİLGİLERİ	Fen Bilimleri Enstitüsü, Ege Üniversitesi, İZMİR
AKADEMIK	**Araştırma Görevlisi** **2012 -- devam** Fen Bilimleri Enstitüsü Matamatik (Bilgisayar Bilimleri Bilim dalı) Ege Üniversitesi **Bilgi Teknolojileri** **2012 -- devam** Fen Bilimleri Enstitüsü Ege Üniversitesi
EĞITIM	**Doktora,** Fen Bilimleri Enstitüsü**,** Matematik (Bilgisayar bilimleri bilim dalı), Ege Üniversitesi, 2016-- **Yüksek Lisans,** Fen Bilimleri Enstitüsü, Matematik (Bilgisayar bilimleri bilim dalı), Ege Üniversitesi 2012- 2015 **Lisans**, Fen Fakültesi, Matematik (Bilgisayar bilimleri bilim dalı), Ege Üniversitesi 2008- 2012
ARAŞTIRMA ALANLARI	Blokzincir Teknolojileri, Akıllı Sözleşme, Bilgi Teknolojisi, Tedarik Zinciri Yönetim sistemleri, Yerinden Yönetim Sistemleri, Nesnelerin İnterneti (IoT), Kriptografi, Bilgi Güvenliği

YAYINLAR

SCI, SSCI and AHCI Indexes

I. **Sezer, B. B., Topal, S., & Nuriyev, U.** (2022). TPPSUPPLY: A traceable and privacy-preserving blokzincir system architecture for the supply chain. *Journal of Information Security and Applications*, *66*, 103116.

Diger Dergiler

I. Sezer B.B., HYPERLINK https://arxiv.org/search/cs?searchtype=author&query=Topal%2C+S **Topal S., Nuriyev U.,** "An Auditability, Transparent, and Privacy-Preserving for Supply Chain Traceability Based on Blokzincir", https://arxiv.org/abs/2103.10519, 10 p., March 2021.

Hakemli Kongre/ Sempozyum Bildiri Kitabındaki Yayınlar

I. Sezer, B. B., and Nuriyev, U. (2020). Blokzincir Scalabılıty and Dıstrıbuted Ledger Technologıes, Materials International Scientific II Conference for the "*Informatıon systems and technologıes achıevements and perspec*tıves"**,** Sumgait State University, Sumgait, Azerbaijan, July 09-10, 2020, pp. 8-11.

II. Sezer B.B., Nuriyev U.G., PICprince –8 bit Microişlemciler için Prince'ın Verimli Bir Uygulaması*, II. Ulusal Kripto Günleri Çalıştayı,* TÜBİTAK, BİLGEM, UEKAE, Gebze/Kocaeli, Türkiye, 09-11 Nisan, 2015. http://mcs.bilgem.tubitak.gov.tr/cryptodays/files/posters/Bora%20Bugra%20SEZER.pdf

SERTİFİKALAR, KURSLAR VE EĞİTİM SEMPOZYUMU ETKİNLİKLER	• II, National Blokzincir Workshop, TUBITAK, Turkey, 2019 • International Eurasia Blokzincir Summit, Turkey,2019 • International Autumn School on Computational Number Theory (IYTE), Turkey, October 2017 • International Conference on Information Security and Cryptology, Turkey, October 2014 • Nopcon International Hacker Conference, Turkey, September 2014 • TUBITAK cryptology summer school education / Gebze Institute of Technology, Turkey, September 2011
BİLİMSEL HAKEM	Journal of Modern Technology and Engineering, Other Indexed Journal, September 2020 Dergipark, Other Journals, September 2020