# BLOKZİNCİR TABANLI UÇTAN UCA ENERJİ TİCARETİ PLATFORMLARI İÇİN DÜŞÜK ENERJİ TÜKETİMLİ BİR UZLAŞMA ALGORİTMASININ GELİŞTİRİLMESİ

# ADAPDATION OF CONSENSUS ALGORITHM ON A BLOCKCHAIN BASED PEER TO PEER ENERGY TRADING PLATFORM

**MERT BİLİCİ**

**DOÇ. DR. ADNAN ÖZSOY**

**Tez Danışmanı**

Hacettepe Üniversitesi

Lisansüstü Egitim-Öğretim ve Sınav Yönetmeliğinin

Temiz Tükenmez Enerjiler Anabilim Dalı için Öngördüğü

YÜKSEK LİSANS TEZİ olarak hazırlanmıştır.

2023

# ÖZET

## BLOKZİNCİR TABANLI UÇTAN UCA ENERJİ TİCARETİ PLATFORMLARI İÇİN DÜŞÜK ENERJİ TÜKETİMLİ BİR UZLAŞMA ALGORİTMASININ GELİŞTİRİLMESİ

**Mert BİLİCİ**

**Yüksek Lisans, Temiz Tükenmez Enerjiler**

**Tez Danışmanı: Doç. Dr. Adnan ÖZSOY**

**Nisan 2023, 83 Sayfa**

Mikro şebekelerin gelişmesi ve yerel ölçekte yenilenebilir enerji üretiminin hızla artması, enerji ve finans kaynaklarının verimli kullanıldığı hızlı bir ticaret mekanizması ihtiyacını doğurmaktadır. Blokzincir teknolojisi, eşler arası uçtan uca ticaret için güvenilir bir çözüm oluşturabilecek altyapıya sahiptir. Blokzincir kullanarak enerji ticaretine yönelik son teknoloji çözümler, merkezi sistemlerin bir takım sorunlarını çözmelerine rağmen enerji ve zaman verimliliği yetersiz kalmaktadır. Bu blokzincir tabanlı çözümlerin sorunlarından biri, doğrulama ve madencilik için çok fazla enerji harcayan hantal ve verimsiz uzlaşma algoritmalarıdır. Bu tezde önerilen model, bir ticaret döngüsünü tamamlamak için Ethereum akıllı sözleşmelerini kullanan yeni bir uzlaşma algoritması ile bu sorunu çözmeyi amaçlamaktadır. Sunulan model, akıllı sayaçları kullanarak üretim fazlası enerjiyi yerel mikro şebekeyle özerk bir şekilde takas etmeyi ve üreticilerin finansal gelirlerini artırmayı amaçlamaktadır. Aynı zamanda model, enerji ticaretinin eksiksiz olmasını ve çalışma kanıtına ihtiyaç duymadan birden fazla düğümde değişmez bir şekilde kaydedilmesini sağlamaktadır.

**Anahtar Kelimeler:** Blokzincir, Enerji Ticareti, Uzlaşma Algoritması, Uçtan Uca, Düşük Enerji Tüketimi, Ethereum, Akıllı Sözleşmeler

# ABSTRACT


**ADAPDATION OF CONSENSUS ALGORITHM ON A BLOCKCHAIN BASED PEER TO PEER ENERGY TRADING PLATFORM**

**Mert BİLİCİ**

**Master of Science, Department of Renewable Energy**

**Supervisor: Assoc. Prof. Dr. Adnan ÖZSOY**

**April 2023, 83 Pages**

The development of microgrids and the increase of renewable energy production on local scale requires a robust and fast trading mechanism to prevent any financial and energetic loss. Blockchain technology offers a trustless solution for peer-to-peer trading on a microgrid. The state-of-the-art solutions for energy trading with blockchain technology solves many problems of the centralized systems but lacks the energy and time efficiency. One of the substantial problems of these blockchain based solutions is the bulky and inefficient consensus algorithms that spend too much energy for validation and mining. The proposed model in this thesis aims to resolve this problem with a novel consensus algorithm that uses Ethereum smart contracts to complete a trade cycle. The model implies usage of smart meters and connection to the Internet to autonomously trade energy with the local microgrid and increase the financial revenue of prosumers. At the same time the model makes sure that the energy trade is complete and immutably recorded on multiple nodes without a need for proof-of-work.



**Keywords:** Blockchain, Energy Trade, Consensus Algorithm, Ethereum, Peer-to-peer, Low Energy Consumption, Smart Contract

# TEŞEKKÜR

Öncelikle tez danışmanım Sayın Doç. Dr. Adnan Özsoy'a tez yazım sürecindeki tüm destekleri için ve bana kattığı değerli bilgilerden dolayı teşekkür ederim. Hem kendisinden aldığım ders ile hem de tez çalışması süresince sağladığı bilgilerle benim için çok yeni olan bir alanda başarılı olmamı sağladığı için kendisine şükranlarımı sunarım.

Değerli hocam, Temiz Tükenmez Enerjiler Anabilim Dalı Başkanı Sayın Prof. Dr. Akın Bacıoğlu'na hem akademik hem de kişisel olarak sağladığı tüm destekler için teşekkür ederim. Bölüm dersleri ile birlikte beni temiz enerji ile tanıştıran ve geleceğe dair umut veren bilgileri ile yolumu aydınlatan Prof. Dr. Aynur Eray'a da ayrıca teşekkür ederim.

Tüm yüksek lisans ve tez sürecinde benden desteğini esirgemeyen, her zaman ve her şeyiyle benim yanımda olarak bu başarıya ortak olan çok değerli aileme ve Sayın Av.Aybüke Akdağ'a çok teşekkür ederim.

Mert Bilici

Nisan 2023, Ankara

# İÇİNDEKİLER

# ŞEKİLLER DİZİNİ

# ÇİZELGELER DİZİNİ

# SİMGELER VE KISALTMALAR

**Simgeler**

| | |
|---|---|
| CO2 | Karbondioksit |
| GWh | Giga Watt Saat |
| kVA | Kilo Volt Amper |
| kVARh | Kilo Volt Amper Reaktif Saat |
| kWh | Kilo Watt Saat |
| kWp | Kilo Watt Peak |
| MW | Mega Watt |
| TWh | Tera Watt Saat |

**Kısaltmalar**

| | |
|---|---|
| AES-NI | Advanced Encryption Standard – New Instructions |
| ASIC | Application Specific Integrated Circuit |
| AS | Akıllı Sözleşme |
| BİG | Bütünüyle İzin Gerektirmeyen |
| CPU | Central Processing Unit |
| EEYS | Ev Enerji Yönetim Sistemi |
| EKS | Eşit Katılım Sabiti |
| ET | Enerji Toplayıcıları |
| HK | Hisse Kanıtı |
| IIOT | Industrial Internet of Things – Endüstriyel Nesnelerin İnterneti |
| İK | İş Kanıtı |
| IoT | Internet of Things – Nesnelerin İnterneti |
| JSON | JavaScript Object Notation |
| KİG | Kısmen İzin Gerektirmeyen |

| | |
|---|---|
| LoRaWAN | Long Range Wide Area Network |
| M-Bus | Metering Bus |
| MQTT | Message Queuing Telemetry Transport |
| NIST | National Institute of Standards and Technology |
| P2P | Peer-to-peer |
| PLC | Power Line Communication |
| HK | Proof-of-Stake |
| RAM | Random Access Memory |
| RSA | Rivest, Shamir, Adleman |
| SHA-256 | Secure Özet Algorithm – 256 Bits |
| TPM | Trusted Platform Module |
| TÜF | Tüketim-Üretim Fonksiyonu |
| YEF | Yeşil Enerji Fonksiyonu |
| YEK | Yeşil Enerji Kanıtı |

# 1. GİRİŞ

Yenilenebilir enerji teknolojilerindeki gelişme ve iklim değişikliğine acil bir çözüm bulma ihtiyacı, enerji üretimindeki toplam yenilenebilir enerji payını hızla artırmaktadır. 2018 yılında Dünya'daki elektrik üretiminin %26,2'si yenilenebilir kaynaklardan sağlanmış olup, bu oran 2020 yılında %29'a yükselmiştir ve 2040 yılına kadar bu oranın %45'e kadar yükselmesi beklenmektedir [1]. Enerji üretim kaynaklarının dağıtık hale gelmesi elektrikli araçları, enerji depolama tesislerini, evleri ve işyerlerini içeren mikro şebekeler adı verilen ve sürdürülebilir bir şekilde elektrik üreten/tüketen yerel ve daha küçük elektrik şebekelerinin oluşumuna yol açmaktadır. Elektrik ticaretine yönelik mevcut çözümler oldukça merkezidir ve ticareti düzenlemek için bir hükümet kuruluşu veya özel kuruluş gerekmektedir. Günümüzde, tüm elektrik tüketicileri kendi enerjisini üretmeye ve depolamaya başladığından, (üreten tüketici haline geldikçe) merkezi elektrik ticareti sistemleri, daha küçük ölçekli şebekelerdeki artan aktörlerin sayısı ve ticaret miktarı ile başa çıkmakta zorlanmaktadır.

Geleneksel bir merkezi enerji ticareti organizasyonu ile ilgili temel sorunlardan biri, bu organizasyonların hatalara açık olması ve alternatif bir enerji ticareti aracının bulunmamasıdır. Bu durumda tek bir devlet kurumunda yaşanacak bir başarısızlık, enerji akışının yerel veya ulusal çapta bozulmasına neden olabilmektedir. Merkezi bir enerji ticareti organizasyonunun varlığı nedeniyle tek noktadan tüm sistemin çökmesine neden olacak bir arıza riski ve kötü niyetli saldırılara karşı zafiyet artmaktadır. Bu durum enerji güvenilirliği için ciddi bir tehlike oluşturmaktadır [2]. Geleneksel merkezi enerji ticaret sistemi ile ilgili diğer önemli bir sorun, tüketicilerin gizliliklerini sağlamak için merkezi bir kuruluşa güvenmek zorunda olmasından kaynaklanan gizlilik ve güvenlik endişeleridir. Merkezi piyasalar, merkezi olmayan alternatife kıyasla nispeten daha opak ve arızalara daha yatkındır, bu nedenle tüketiciler elektriklerinin güvenliği için tek bir kuruluşa koşulsuz güvenmek zorundadır. Merkezi elektrik piyasalarının, gün öncesi piyasa işlemlerinin taraflar arasında paylaşılmasının getirdiği zorluklar nedeniyle ölçeklendirilmesi de merkeziyetsiz sistemlere göre daha zordur [3]. Ayrıca, geleneksel merkezi piyasalar, küçük ölçekli yenilenebilir enerji üreticilerinin şebekeye dâhil olması ile riskin kaldırılması ve azaltılması adına daha büyük zorluklar ortaya koymaktadır. Merkezi olmayan piyasalar, enerji depolama ve talep yanıtı gibi yeni enerji kavramları

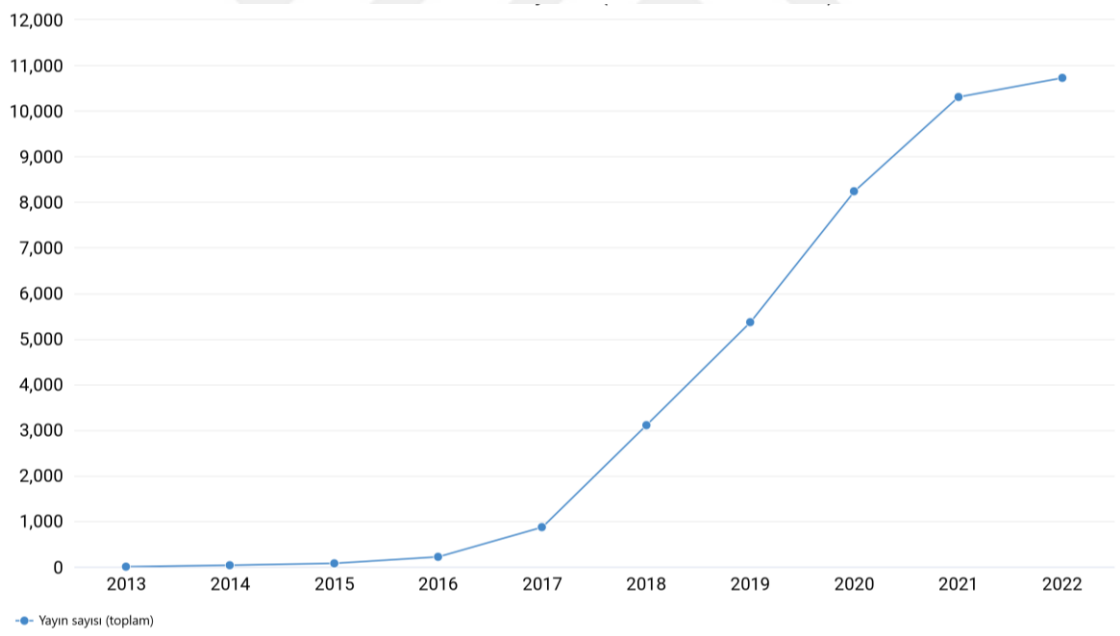
ve teknolojileriyle başa çıkabilecek daha esnek bir organizasyon sağlamaktadır [3]. Tüm Avrupa ülkeleri şu anda dağıtılmış enerji kaynaklarıyla daha iyi koordine olmak ve artan sayıda üreten tüketici ile başa çıkmak için merkezi piyasalar yerine merkeziyetsiz veya yarı merkeziyetsiz piyasalar kullanmaktadır.

Klasik şebeke ve piyasa türlerinden modern akıllı şebeke sistemlerine ve merkezi olmayan piyasalara geçişi, elektrik sayaç cihazlarının dönüşümü yakından takip etmektedir. Akıllı sayaçlar, tüketici tarafındaki elektrik yükü hakkında bilgi toplayabilen ve kullanıcının toplam enerji tüketimini hesaplayabilen enerji izleme ve faturalandırma cihazlarıdır [4]. Aynı zamanda, akıllı sayaçlar, sistem operatörleri veya kamu hizmeti firmaları ile iki yönlü bir iletişim yolu sağlamakta, böylece elektrik verileri hakkında daha fazla bilgi sağlayabilmekte ve operatörlerin şebekeden bir yükü ayırmasına izin verebilmektedirler. Akıllı sayaçların kullanımının artmasıyla birlikte, tüketici hakkındaki kişisel veriler, tüketici fark etmeden izlenebilmekte ve kullanılabilmektedir, bu da akıllı sayaçlar tarafından üretilen veriler için bir gizlilik ihtiyacı yaratmaktadır [5]. Elektrik tüketim verileri ve son kullanıcının cihazlarındaki voltaj ve frekans hakkındaki ayrıntılı bilgiler, yakın gelecekte risk altında olabilecek son derece değerli bir kişisel bilgi olarak kabul edilmektedir. Geleneksel elektrik şebekesinin modern akıllı şebekeye dönüştürülmesi, bazıları günümüzde bilinirlik kazanan blokzincir teknolojileri kullanılarak çözülebilecek birçok gizlilik ve verimlilik zorluğu ortaya çıkarmaktadır.

Enerji ticaretinin merkeziyetsiz hale getirilmesi, bir mikro veya ülke çapındaki şebekede blokzincir teknolojisi ile gerçekleştirilebilmektedir. Blokzincir algoritmasının kullanıldığı eşler arası bir ticaret sistemi, merkezi enerji ticaretinin sorunlarına bir çözüm getirmek ve yenilenebilir enerji tüketicilerinin gelirini en üst düzeye çıkarmak için bu tezin ilerleyen bölümlerinde değinilen çalışmalarca çözüm önerisi olarak sunulmaktadır. Blokzincir teknolojisine sahip merkezi olmayan enerji ticaret sistemleri için birçok farklı yaklaşım önerilmiş ve gerçek bir elektrik şebekesi üzerinde denemeler başlatılmıştır [6]. Santrallerden üreten tüketicilere doğru taşınan enerji ölçeğindeki azalma, yakın gelecekte bu tür teknolojilerin denenmesi için daha fazla fırsat yaratacaktır ve yakın gelecekte blokzincir tabanlı eşler arası enerji ticareti uygulamaları hakkındaki deneysel sonuçlar pratik kullanım senaryoları ile birlikte gözlemlenebilecektir. Dağıtık defter teknolojisi

tabanlı eşler arası enerji ticaretindeki en büyük zorluklardan biri, Bölüm 2'de ayrıntılı olarak açıklanan blokzincir teknolojisinin aşırı enerji tüketimidir. Referans olarak, bir Bitcoin işleminin 300 ila 1000kWh elektrik tüketimine neden olduğu tahmin edilirken, MasterCard tarafından yapılan tipik bir kredi kartı işlemi tahmini olarak yalnızca 0,0007kWh elektrik tüketimine neden olmaktadır [7]. Tek bir Bitcoin transfer işlemi için kullanılan bu muazzam enerji miktarı, ABD'deki bir evin ortalama aylık elektrik tüketiminin üzerindedir [8].

Şekil 1.1'de "Blokzincir enerji ticareti" arama terimi ile ilgili yapılan toplam yayın sayısı 2013-2022 yılları arasında gösterilmiştir. Şekil 1.1 incelendiğinde, 2017'den 2022'ye kadar bu alandaki araştırma makalelerinin sayısında 100 katlık bir artış görülmektedir ve bu durum enerji ticareti uygulamaları için enerji verimli bir blokzincir yönetimine olan acil ihtiyacı net olarak ortaya koymaktadır.




Şekil 1.1: 2013'ten 2022'ye kadar "Blokzincir enerji ticareti" arama terimi ile alakalı yapılan toplam yayın sayısı [9].

Bu makalede akıllı şebekeler, yerel enerji piyasaları, eşler arası enerji ticareti, blokzincir teknolojisi, uzlaşma algoritmaları ve mevcut uzlaşma yöntemlerinin enerji verimliliği sorunları hakkında ayrıntılı bir arka plan araştırması sunulmaktadır. Ayrıca bu makalede, blokzincir tabanlı merkeziyetsiz elektrik ticareti için en son teknolojiler ve önerilen

modeller, mevcut sınırlamaları ve olası sorunları açısından incelenmiştir. Son olarak, makalede Yeşil Enerji Kanıtı adı verilen yeni bir uzlaşma algoritması ile enerji verimliliği yüksek olası bir çözüm önerilmektedir.

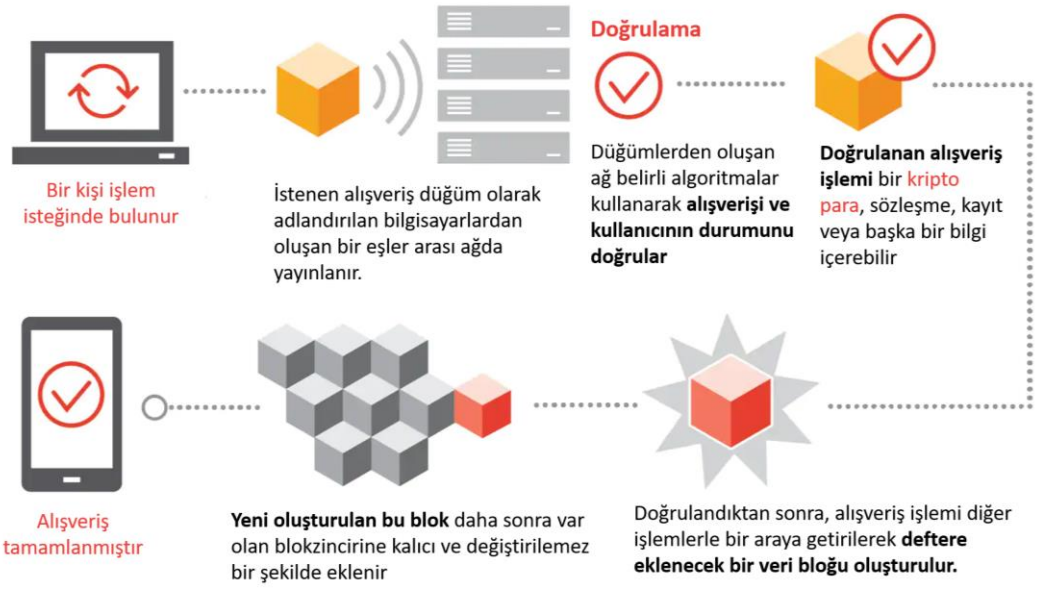
Bu makalenin oluşturduğu modele dair ilk varsayımı, merkeziyetsiz piyasa sistemlerinin uygulanabilmesi için çok sayıda üreten tüketici içeren, yeterince gelişmiş bir mikro şebekenin varlığıdır. The Climate Center organizasyonundan Ellie Cohen, bir mikro şebekenin gelecekteki uygulamasının büyük düzeydeki bakım uygulamalarına ve büyük ölçekli planlı güç kesintilerine olan ihtiyacı önleyebileceğini belirtmektedir [10]. Bu nedenle, enerji piyasasındaki yenilenebilir enerji kaynaklarının üstel büyümesi göz önüne alındığında, ihtiyaç duyulan akıllı sayaçlarla donatılmış mikro şebekelerin de yakın gelecekte geliştirileceği öngörülebilmektedir. Bu makalede önerilen modeli benimseyen blokzincir tabanlı bir enerji ticaret platformunun kullanılması, bu tür yerel mikro şebekelerin verimliliğini artırabilecektir. Sunulan model, akıllı sözleşmelerin kullanımıyla blokların doğrulanmasını basitleştiren yeni bir uzlaşma algoritması ile blokzincir enerji ticaret sistemlerine katkıda bulunmaktadır. Bu yeni uzlaşma algoritması olan Yeşil Enerji Kanıtı, üreten tüketicilerin yenilenebilir enerji üretimini karşılaştırmaya ve blokları doğrulamak için en iyi üreticilerin enerji yönetim cihazlarını kullanmaya dayanmaktadır. Bu yöntem, İş Kanıtı ile ilgili hesaplamalarla yanlış yönde harcanan enerjiyi önlemekte ve blokzinciri tabanlı bir sistemin enerji ve zaman verimliliğini artırmaktadır.

# 2. ARKAPLAN

## 2.1 Blokzincir Teknolojisi

Blokzincir, bir ağ içindeki farklı düğümler arasındaki işlemlerin değişmez kayıtlarına sahip dijital olarak dağıtılmış bir defterdir. Blokzincirindeki bir dijital varlığın her işlemi, diğer işlemlerle birlikte bir blok içinde saklanmakta ve her blok, kriptografik bir özet fonksiyonu kullanılarak bir sonrakine bağlanmaktadır. Her iki blok arasındaki bu bağlantı, çevrimiçi ve dağıtılmış bir defteri saklamak için kullanılabilecek, onaysız değişikliklere karşı korumalı bir yapı oluşturmaktadır. Blokzincir teknolojisinin ilk ortaya çıkışı, 2008 yılında gerçek kimliği bilinmeyen yazar(lar) Satoshi Nakamoto tarafından yayınlanan Bitcoin tanıtım raporudur [11]. Bitcoin, işlemleri kontrol etmek ve güvence altına almak için herhangi bir merkezi otoriteye ihtiyaç duymadan varlık ticareti

yapmak için alternatif bir yöntem olarak önerilmiştir. Gönderilen veya alınan her Bitcoin hakkındaki bilgiler, o blok tam olarak kabul edilene ve zincire yeni bir blok eklenene kadar bir blokta saklanmaktadır. Bu teknoloji, kriptografik özet fonksiyonunun getirdiği zorluk yardımıyla uç uca eklenen blok sayısı arttıkça daha yüksek bir tahrifat direnci sağlamaktadır. Yeni eklenen bloklar, ağ içindeki defterin tüm kopyaları arasında kopyalanmakta ve herhangi bir çakışma önceden belirlenmiş kurallar bütünü [12] tarafından çözülmektedir. Blokzincir teknolojisinin nasıl çalıştığına dair basit bir modelleme Şekil 2.1'de sunulmuştur.




Şekil 2.1: Blokzincir'in nasıl çalıştığına dair basit bir gösterim [13].

Blokzinciri teknolojisinin temel özellikleri şu şekilde özetlenebilir:

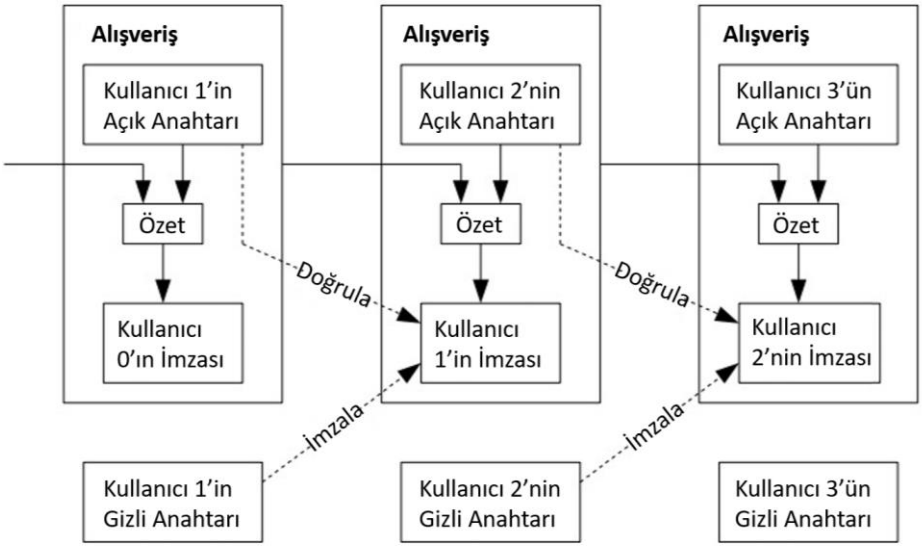
- Merkeziyetsiz: Blokzincir ağı ve ona atfedilen defter, sistemin yönetiminden sorumlu merkezi bir otoriteye sahip değildir. Ağın her bir düğümü tüm zincirin bir kopyasına sahiptir ve sistem otomatik olarak gerçekleştirilen hesaplamalarla yönetilmektedir. Bu, sistemin çalışması ve güvenliği için herhangi bir kuruluşa güvenmek zorunda kalmama avantajını getirmektedir, çünkü bu tür bir ağda üçüncü taraflar kötü niyetli veya güvenilmez olabilmektedir. Ayrıca, bu özellik, blokzincirini her üye için şeffaf hale getirmekte ve güvenlik açıklarının fark

edilmeden varlığını sürdürmesi çok daha zor olduğu için bilgisayar korsanlığı faaliyetleri riskini azaltmaktadır.

- Güvenli: Blokzincirinde devam eden her işlem/bilgi, kriptografik fonksiyonlar kullanılarak şifrelenmektedir. Blokzincirinde kullanılan cüzdan adreslerinin oluşturulması ve halka açık olarak paylaşılması için asimetrik kriptografi kullanılmaktadır. Böylece güvenli bir cüzdan adresi sistemi oluşturulmaktadır. Her bloğun içeriğinin özetini oluşturmak için bir kriptografik özet fonksiyonu kullanılmakta ve bu özet, zincirdeki her blok arasında kriptografik olarak güvenli bir bağlantı oluşturarak bir sonraki bloğa eklenmektedir.
- Dağıtık: Blokzincir ağları, sisteme katılan tüm düğümlere dağıtılmakta ve her üye tüm zincirin kendine ait bir kopyasını tutmaktadır. Bu, her düğümün eşit haklara sahip olduğu, saldırması zor ve saydam bir ağ oluşturmaktadır. Bir işlemin geçerli ve tamamlanmış olarak kabul edilmesi için ağdaki üyelerin çoğunluğunun bu işlemi doğrulaması gerekmektedir. Bu özellikler, blokzincirinin takip edilmesini kolaylaştırmakta, düzenleyici bir otoriteye sahip çözümlerden daha hızlı olmasını sağlamakta ve kötü amaçlı düğümlerin verilerin bütünlüğüne zarar vermesini önlemektedir.
- Değiştirilemez: Özet fonksiyonunun sonucunu bir sonraki bloğa ekleyerek blokların önceki ve sonraki bloklara bağlanması, zincirdeki önceki verilere yönelik güçlü bir bağ oluşturmaktadır. Bir bloktaki herhangi bir veri değiştirildiğinde, özet fonksiyonunun ilgili çıktısı büyük ölçüde değişmekte ve bu bir sonraki bloğun özet fonksiyonunun da değişmesine ve yepyeni bir özet fonksiyonu çıktısı elde edilmesine neden olacaktır. Bu, değiştirilmiş bloktan sonraki tüm bloklarda zincirleme bir reaksiyon oluşturmakta ve bu bloktan sonraki tüm zincirin başarısız olmasına neden olmaktadır. Kullanılan kriptografik özet fonksiyonunun ters yönde çalıştırılmaya direnci çok yüksektir, bu nedenle sahte bir işlem girişi ancak bir sonraki bloklar için tüm özetlerin kaba kuvvetle tekrar hesaplanmasıyla doğrulanabilmektedir. Bu durum var olan kayıtları değiştirmeye yönelik saldırıların pratikte imkânsız hale gelmesini sağlamaktadır.

Blokzincir teknolojisi, tanımlama, kimlik doğrulama ve şifreleme için açık ve gizli anahtarlardan oluşan açık anahtarlı şifreleme tekniğini kullanmaktadır. Her düğüm veya cüzdan, diğer düğümlerle paylaştıkları bir açık anahtara sahiptir, böylece diğer

kullanıcılar kolaylıkla bu cüzdana kripto para birimi veya benzeri bir varlık gönderebilmektedir. Bu yapıda açık anahtarın tamamlayıcısı, herkesten saklanan bir gizli anahtardır. Tüm işlemler alıcının açık anahtarı kullanılarak dijital olarak imzalanmakta, böylece alıcı düğüm gizli anahtarını kullanarak ilgili varlığın sahipliğini onaylayabilmektedir. Şekil 2.2, Bitcoin teknik makalesinde gösterildiği şekliyle blokzincir işlemlerinde açık-gizli anahtar çiftinin rolünü göstermektedir. Bu yöntemde, açık anahtar anonim tutulmakta, böylece hiçbir cüzdan adresi gerçek bir kişiye bağlanamamakta ve bir gizlilik oluşturulmaktadır. Ayrıca Sathoshi Nakamoto, gizliliği korumak için ek bir önlem olarak her işlem için yeni bir anahtar çifti kullanılmasını önermektedir [11]. Bununla birlikte, Bitcoin gibi blokzincirlerindeki adresler gerçek manada anonim olarak kabul edilmemekte, ancak bir takma isim olarak kabul edilir, çünkü bu teknoloji önceki tüm işlemlerin ilgili tek bir adrese bağlanmasını önleyememektedir. Kullanılan cüzdanın gizli adresi yalnızca gerçek kullanıcının kimliği için seçilmiş bir takma addır [14].




Şekil 2.2: Açık-gizli anahtar çiftinin blokzincir işlemlerindeki rolü [11].

Bitcoin ağı, herhangi bir bilgisayarın görüntülemesi veya katkıda bulunması için halka açıktır, fakat diğer bazı blokzinciri uygulamaları izinli bir özel ağ üzerinde kurulabilmektedir. Kısmen İzin Gerektirmeyen blokzincirleri, verilerin gözlemlenmesi, dağıtılması veya eklenmesi için sisteme katılmak isteyen herhangi bir bilgisayar ile ilgili erişim izni verilen, merkeziyetsiz platformlar olarak sınıflandırılmaktadır. Hem Kısmen

İzin Gerektirmeyen hem de Bütünüyle İzin Gerektirmeyen blokzinciri ağlarında, kötü niyetli düğümlerin, çeşitli yöntemlerle gerçek ve geçerli olan zincirden ayrıştırıldığından emin olmak için bir uzlaşma algoritması kullanılmaktadır. Kısmen İzin Gerektirmeyen blokzincirleri, kullanıcıya zincire okuma veya yazma erişimi vermek için merkezi veya merkezi olmayan bir otoriteye ihtiyaç duymaktadır. Bu ağlarda yetkili, bazı düğümlerin bloklara ulaşmasını veya bunlara yeni veriler eklemesini engelleyebilmektedir. Bu durum, blokzincirini yöneten otoriteye güven mecburiyeti getirmekte, ancak aynı zamanda blokzincirinin yararlı özelliklerini daha fazla güvenlik önlemi altında kullanmak için kontrollü bir ortam sağlamaktadır. Şekil 2.3, doğrulayıcıların anonimlik durumuna ve doğrulayıcılara duyulan güvene göre farklı blokzinciri uygulama kategorilerini göstermektedir.


Şekil 2.3: Doğrulayıcıların anonimlik durumuna ve güvene göre blokzincir uygulamalarının sınıflandırılması [15].

Blokzincir teknolojisinin en popüler uygulamaları arasında Bitcoin, Ethereum, Hyperledger, Solana ve Ripple bulunmaktadır. Blokzincir teknolojisi, burada belirtilen kullanım durumlarıyla sınırlı değildir ve enerji ticareti de dâhil olmak üzere birçok farklı amaç için birçok farklı şekilde uygulanabilmektedir.

## 2.2 Uzlaşma Algoritmaları

Blokzincir teknolojisinin önemli bir kısmı, düğümlerin çoğunluğunun blokzincirinin aynı durumu üzerinde hemfikir olmasını sağlayan bir uzlaşma algoritmasının kullanılmasıdır. Uzlaşma algoritmalarının genel olarak 3 önemli özelliği vardır: güvenlik, hata toleransı ve canlılık. Uzlaşma algoritmasının güvenliği, blokzincirinin her bir üyesi için algoritmanın çıktı sonuçlarının tutarlılığı ile belirlenmektedir. Tüm düğümler, verilen kurallar altında her zaman aynı çıktıyı üretebilmelidir. İkinci önemli özellik, ağa sağlıklı bir şekilde bağlanabilen düğümlerin zamandan bağımsız olarak kesinlikle bir sonuç çıkaracağı anlamına gelen canlılıktır. Son özellik ise algoritmanın hata toleransıdır; uzlaşma sürecine dâhil edilen başarısız bir ağ düğümü, diğer düğümler için uzlaşmaya varılmasını engellemeyecektir [16].

Bu uzlaşma algoritması genellikle bir sonraki bloğu yayınlayacak düğüme karar vermektedir. Bütünüyle İzin Gerektirmeyen halka açık blokzincirlerinde, genellikle seçilen uzlaşma algoritması, ağ düğümlerinin rekabet etmesi için bir teşvik yaratırken, aynı zamanda bir sonraki blok için bir sonraki doğrulayıcıyı seçmektedir. Örneğin, Bitcoin, ağ düğümlerinin bir sonraki Bitcoin ödülü için rekabet ettiği, matematiksel olarak karmaşık ve zaman alıcı bir bulmaca yaratan ve bu blok için tüm işlem ücretlerini bir adet Bitcoin'le birlikte ödül olarak doğrulayıcıya veren İş Kanıtı uzlaşma algoritmasını kullanmaktadır [11]. Bu tür bir uzlaşma algoritmasının kullanılması, bir bloğun doğrulanmasını sağlayarak kripto para birimi ve/veya işlem ücretlerini kazanmak isteyen pek çok kullanıcıyı ağa çekmektedir. Aynı zamanda, bu algoritma doğrulanacak ve blokzincirine kalıcı olarak eklenecek bloğa karar vermektedir. Bu süreç, finansal bir değerin takası veya diğer birçok amaç için kendi kendine yeten ve güvene ihtiyaç duymayan bir ağ oluşturan Bitcoin yazılımı tarafından otomatikleştirilmiştir. Blokzincire bir genel bakış sunan NIST raporu bu teknoloji ile ilgili şu dört ana özelliği belirtir:

- Blokzincir'in ilk durumu hakkında tüm üyeler ortak bir fikre sahiptir.
- Bir sonraki bloğa karar veren uzlaşma algoritması üzerinde önceden anlaşmaya varılmıştır.

- Her blok, önceki bloğun kriptografik özet fonksiyonundan çıktısının bir sonraki bloğa giriş olarak eklenmesiyle önceki bloğa bağlanmaktadır.
- Tüm üyeler sistemdeki herhangi bir bloğu kendi başlarına doğrulayabilmektedir [12].

Burada, zincirin ilk bloğunun (Genesis bloğu) önceki bloğu olmadığı için önceki blok özeti kısmının sıfırlardan oluştuğu gibi dikkate alınması gereken bazı önemli noktalar vardır. Uzlaşma algoritması tüm kullanıcılar için geçerlidir ve herkes ilgili özet değerini bulmak için aynı anda rekabet edebilmektedir. Bir blok ödülü kazanmak için doğru özet değerinin bulunmaya çalışıldığı bu sürece madencilik adı verilmektedir. Rakip düğümler, kendi uçlarında bulunan işlemlerle oluşturdukları geçerli blokları diğer düğümler ile yaklaşık olarak aynı anda bulabilmekte ve yayınlayabilmektedir. Bu durum blokzincirinde bir çatışma yaratır fakat bu çatışma durumuna izin verilmektedir ve uzun vadede sistemde herhangi bir soruna neden olmamaktadır. Bir süre sonra çatışan bu zincirlerden biri terk edilecek ve daha fazla doğrulanmış bloğa sahip en uzun zincir gerçek blokzinciri olarak kabul edilecektir. Blokzincirinin bu belirsiz doğası nedeniyle, belirli bir işlemi içeren blok üzerine birkaç blok daha inşa edilmeden önce ağdaki işlemler tamamlanmış olarak kabul edilmemektedir. Bitcoin teknik makalesi, dürüst bir zincirden daha hızlı şekilde kötü niyetli bir zincir oluşturmaya çalışan bir saldırganın, dürüst bir bloktan sonra bağlanan blok sayısını arttıkça nasıl başarısız olduğunu açıklamaktadır [11]. Burada, ilgili işlemi içeren bloktan sonra eklenen blok sayısı $z$ ile ifade edilir ve bir saldırganın olası ilerleyişi bir Poisson dağılımı olarak ifade edilmiştir:

$$\lambda = z\frac{q}{p}$$

Poisson dağılımı daha sonra, saldırganın daha uzun bir blokzincirini daha hızlı oluşturabilmesi olasılığı ile saldırganın yapmış olabileceği her ilerleme miktarı için çarpılmıştır. Bu olasılık sonlu bir çözüm için yeniden düzenlendiğinde bir saldırganın dürüst zinciri yakalama olasılığı şu şekilde verilmiştir:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}\left(1 - (q/p)^{(z-k)}\right)$$

Aşağıda gösterildiği gibi bir saldırının başarılı olma olasılığı $z$ arttıkça üstel olarak azalmaktadır [11].

$$q = 0.1$$

$$z = 0 \qquad P = 1.0000000$$

$$z = 1 \qquad P = 0.2045873$$

$$z = 2 \qquad P = 0.0509779$$

$$z = 3 \qquad P = 0.0131722$$

$$z = 4 \qquad P = 0.0034552$$

$$z = 5 \qquad P = 0.0009137$$

$$z = 6 \qquad P = 0.0002428$$

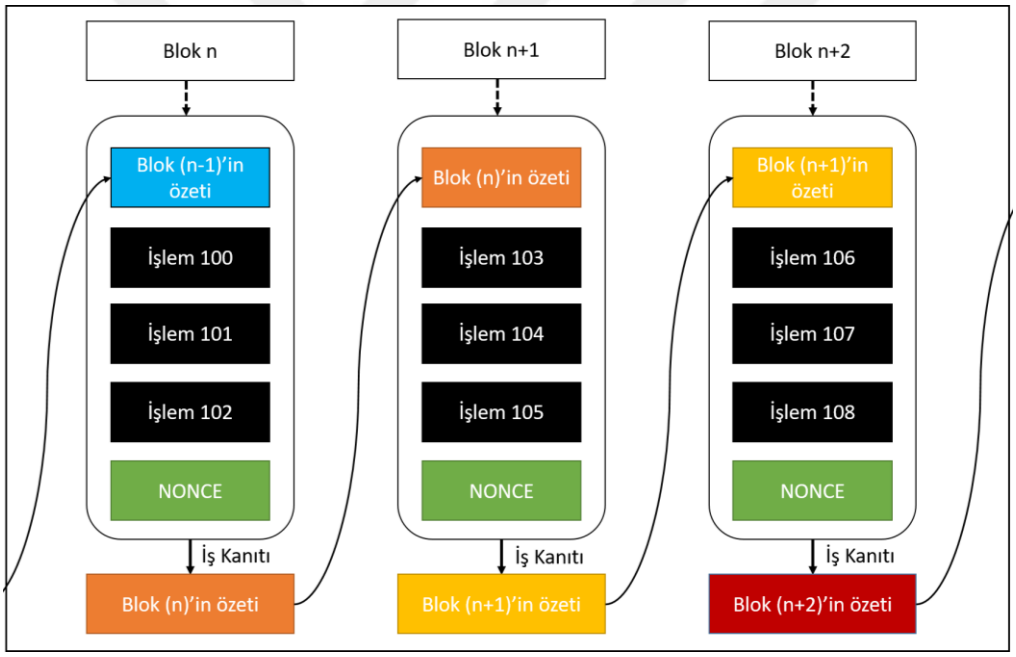
Bu sonuçlar, belirli bir işlemi içeren bloktan sonra yeterli sayıda doğrulanmış blok olduğunda, bu işlemin geçersiz kılınma olasılığının büyük ölçüde düştüğünü göstermektedir. Genellikle 6 blok, Bitcoin işlemleri için büyük miktarlardaki para transferleri için yeterince güvenli kabul edilmektedir, çünkü dürüst bloğun işlemi içermeyen bir blok zincirine geçme olasılığı % 0.1'in altındadır.

Uzlaşma algoritması, söz konusu zincirin amacına ve ihtiyaçlarına göre hem Kısmen İzin Gerektirmeyen (KİG) hem de Bütünüyle İzin Gerektirmeyen (BİG) blokzincirleri için Bitcoin'de kullanılan İş Kanıtı'ndan (İK) farklı olabilmektedir. Çoğu zaman, KİG blokzincirleri, sistemin güvenliği yönetim otoritesi tarafından da yönetilebildiğinden, hız elde etmek amacıyla çok daha kolay ve hesaplamaya daha az bağımlı algoritmalar kullanmaktadır. Ethereum, 2015 yılında piyasaya sürülmesinde İş Kanıtı ile çalışmaktaydı fakat yakın zamanda daha hızlı ve enerji verimliliği daha yüksek işlemler sağlayabilmek için Hisse Kanıtı yöntemine geçiş yapmıştır [17]. Günümüzde büyük blokzinciri ağları havuzunda farklı amaçlar için birçok farklı uzlaşma algoritması vardır ve en popüler olanlardan önerilecek benzer bir model için kullanışlı olabilecek bazıları bu bölümde ayrıntılı olarak açıklanmaktadır.

Bitcoin için kullanılan uzlaşma algoritması olan İş Kanıtı, doğrulama için birçok hesaplama gerektirdiğinden, enerji açısından çok verimsiz olarak görülmektedir. Ayrıca, matematiksel bulmacanın karmaşıklığı, bir bloğun yaklaşık her 10 dakikada bir çıkarıldığından emin olmak için kendini ayarlamaktadır, bu da bir sonraki bloğu doğrulamak ve bir ödül almak için farklı taraflar arasında bir yarış yaratmaktadır.

### 2.2.1 İş Kanıtı

İş Kanıtı (İş Kanıtı), herkese açık erişime sahip bir ağda yüksek Bizans Hata Toleransı sağlayan ve Bitcoin ağında kullanılan uzlaşma algoritmasıdır [18]. İş Kanıtı, herhangi bir kötü amaçlı bloğun gerçek sistemi ele geçirmesini önleyen matematiksel bir karmaşıklık için ana algoritma olarak SHA-256 kriptografik özet fonksiyonunu kullanmaktadır [11]. Adından da anlaşılacağı gibi, bu uzlaşma yöntemi ağır bir hesaplama çalışmasına dayanmakta ve ortaya çıkan özet, doğrulayıcının tamamladığı işin bir kanıt oluşturmaktadır. Blokzincirin blokları birbirine nasıl bağladığına ve İş Kanıtı'nın görevine dair bir diyagram Şekil 2.4'te sunulmuştur. Bu şekilde "nonce" olarak gösterilen kısım İngilizce "number only used once" ifadesinden üretilmiş rastgele bir sayıyı ifade eden bir blokzincir terimidir.




Şekil 2.4: Blokların birbirine nasıl bağlandığının ve İK'nın bu süreçteki rolünün bir temsili.

Burada İK zinciri, Bizans Generalleri Problemi'ne bir çözüm olarak kullanılmıştır, çünkü tüm düğümler en sondaki geçerli blok üzerinde hemfikirdir ve önceki bloklardaki herhangi bir bozulma, sonraki tüm bağlantılı bloklarda bir hataya neden olmaktadır. Bu yöntem, kötü amaçlı bir kişiyi, kötü amaçlı oluşturulan blok ve takip eden her blok için zorluk kurallarıyla (geçerli bir özet değerinin ilk 5 karakterinin sıfır olması gibi) eşleşen geçerli bir özet değeri bulmaya mecbur kılmaktadır. Kötü niyetli aktörlerin sayısı tüm

düğümlerin 1/3'ünden az ise kötü niyetli bir aktörün daha uzun bir zincir oluşturması her zaman daha fazla zaman almaktadır [18]. İK'nın dinamik zorluğu, ağdaki kötü niyetli aktörlerin varlığında bile en uzun zincirin her zaman belirli bir süre içinde kararlaştırılmasını sağlamaktadır.

İK uzlaşma algoritması, yöntemde kullanılan hesaplama açısından yoğun yazılımla ilgili ölçeklenebilirlik sorunları nedeniyle çeşitli eleştiriler almaktadır. Bu uzlaşma yöntemiyle ilgili temel sorunlardan biri, kriptografik özet fonksiyonunun kaba kuvvet hesaplamasına güvenmesidir. Bu, ödül kazanma teşvikiyle sisteme dâhil olan birçok insanın madencilik faaliyetlerine büyük miktarda hesaplama gücü harcamasına neden olmaktadır [19]. Bu tür madencilik gücüne duyulan ihtiyaç üç ana soruna neden olmaktadır:

- Blokzincir madenciliği için kullanılan donanımlar nedeniyle üretilen elektronik atıklar
- Bulmaca çözme işlemi için aşırı miktardaki enerji tüketimi
- Ucuz donanım ve enerji fiyatlarına sahip ülkelerde coğrafi yoğunlaşma

İK ile ilgili hesaplamanın aşırı güç tüketimi bölüm 2.3'te ayrıntılı olarak tartışılmıştır. İK yöntemine yönelik bir başka eleştiri, bir saldırganın düğümlerin zincire erişiminin çoğunluğunu kontrol edebildiği durumda oluşan güvenlik sorunudur. Çoğunluğu sağlamayı başaran saldırgan, kötü amaçlı veri içeren bir zincir oluşturmak için bloklarda hile yapabilmekte veya iki zinciri tamamen ayırabilmektedir [20]. Ayrıca İK ile ilgili başka bir sorun, düğümlerin yeterince büyük bir kısmının ortak bir kararla belirli bir düğümün işlem mesajlarını sansürlemeye ve bu düğümün blokzincirine katılmasını engellemeye karar vermesi ile oluşabilecek ağın adaletsiz hale gelmesidir. Güvenlik ve adalet için İK'ya yönelik bu iki eleştiri, Bitcoin ağı içindeki madencilik havuzlarının merkezileşmeye neden olan payının artmasıyla daha belirgin hale gelmiştir. Madencilerin madencilik havuzlarında toplanması, ağın bu büyük madencilik havuzlarına bağımlı olmasına neden olmakta ve İK'nın savunmasız olduğu bilinen bir saldırı türü olan %51 saldırısı için risk oluşturmaktadır [21].

### 2.2.2 Hisse Kanıtı

Hisse Kanıtı (Proof-of-Stake), İş Kanıtı ile ilgili bazı problemleri, özellikle de enerji verimliliği problemini çözen bir uzlaşma algoritması oluşturmak için geliştirilmiştir. İş Kanıtı sistemleri için madenciler, kripto paraları çıkarmak için bilgisayarlara veya özel donanımlara yatırım yapmalı, bu sermayelerini ödül kazanmak için riske atmalı ve büyük miktarda enerji harcayarak isteklerini kanıtlamak zorundadır. Hisse Kanıtı'nda (HK), doğrulayıcılar (veya madenciler), sözde rastgele bir seçim sürecinde doğrulayıcı adayı olarak değerlendirilmek üzere belirli miktarda kripto para birimi satın almalı ve bir hesaba yatırmalıdır. Doğrulayıcı olarak seçilme olasılığı, doğrusal olarak söz konusu paranın miktarına bağlıdır. HK yöntemi, bir doğrulayıcı olarak para kazanma umuduyla donanım satın alan kişilerin, blok ödülleri kazanmak için doğrudan kripto para birimine aynı miktarda nakit harcamalarını sağlamaktadır. Örneğin, 2000$'a pahalı bir madencilik teçhizatı satın alarak ve 7/24 çalıştırarak kripto para birimi kazanmaya istekli bir kişi, aynı miktarda para kazanma şansını yaratan bir kripto para birimi satın alarak aynı 2000 $'ı buraya yatırabilmektedir. Bu süreç, sadece uzlaşma yönteminin odağını değiştirerek büyük miktarda elektronik atık, elektrik tüketimi ve karbondioksit emisyonundan tasarruf sağlamaktadır. HK, İK'ya göre daha yüksek bir enerji verimliliği, daha az merkezileşme riski ve %51 gibi saldırılara karşı daha güçlü bir güvenlik gibi çeşitli avantajlar sağlamaktadır.

Hisse Kanıtı protokolü, adaylar arasında bir sonraki doğrulayıcıyı sözde rastgele bir algoritma ile seçmekte ve seçilen doğrulayıcı seçim sırasında çevrimiçi değilse, bu blok kazılana kadar yeni bir doğrulayıcı seçilmektedir. Bu algoritma aynı zamanda Nothing-at-Stake adı verilen ve aday doğrulayıcının hiçbir şeyi riske atmadan aynı anda birçok olası sonraki bloğa oy verebileceği bir problem yaratmaktadır [16]. Bunun nedeni, sonunda doğrulayıcı tarafından oylanan bir bloğun seçilecek olması ve doğrulayıcı olma şansının, madencinin oy verdiği olası blok miktarı kadar artmasıdır. Doğrulayıcı, bu protokoldeki bir bloğu onaylarken değerli bir şey harcamamakta, bu nedenle İK'nın aksine, olası doğru bloklar için bir kaynak ayırmaya gerek duymamaktadır. Bu davranış, çok sayıda doğrulayıcının birçok olası blok için oy kullandığı koşullar altında blokzinciri üzerinde uzlaşmanın başarısız olmasına neden olmaktadır. Bu sorunun çözümü, doğrulayıcının kötü niyetli davranması durumunda doğrulayıcının yatırdığı para için bir risk faktörü oluşturularak elde edilmektedir. Ethereum'un Casper adlı HK uygulaması,

kişisel çıkarları için dürüst olmayan bir şekilde hareket eden doğrulayıcıları cezalandırma yolları oluşturarak Nothing-at-Stake sorununu çözmeyi hedeflemektedir. Bu amaçla kullanılan ilk yöntem, bir doğrulayıcının kötü niyetli davranması durumunda ceza olarak yatırılan miktarın bir kısmını yok etmektir. Kötü niyetli veya dürüst olmayan eylemler, aynı anda birden fazla blok için oy kullanmak veya çelişkili doğrulamalar yapmak olarak kabul edilmiştir [22]. Bir miktar Ethereum'un doğrulayıcının yatırdığı tutardan eksiltilmesine kesme (sharding) adı verilmektedir ve kesilecek miktar kötü niyetli eylemin süresine göre değişebilmektedir. Ayrıca, bir doğrulayıcının doğrulama için seçildiğinde çevrimiçi ve cevap vermeye hazır olması beklenmektedir; doğrulayıcı çevrimiçi değilse veya yanıt vermiyorsa, doğrulayıcı seçilen herhangi bir ödül kazanmamaktadır. Bu, doğrulayıcıların blokzincirinin canlılığını sağlamak için bir donanımı çalışır vaziyette tutmasını sağlamaktadır ve bunda başarısız olurlarsa onları cezalandırmaktadır.

HK, İK'nın enerji verimliliği problemini çok büyük bir oranda çözmekte ve İK uygulamasından daha az elektronik atığa neden olabilmektedir. Bununla birlikte, HK oldukça yenidir, İK gibi gerçek uzun süreli kullanım koşullarına tabi tutulmamıştır ve bu durum HK'nın daha büyük ölçekte uygulandığı gelecekteki uygulamalarda sorunlara neden olabilecektir. HK uygulanan sistemleriyle ilgili bir başka sorun, zenginliğin doğrulayıcılara yoğunlaşmasıdır; bu zenginin daha da zengin olması (rich-gets-richer) [23] olarak da ifade edilmektedir. Bu etkinin arkasındaki ana neden, bir blok ödülü için seçilen bir doğrulayıcının, bu doğrulayıcının tekrar seçilme şansını artıracak kripto para birimleri alması ile oluşan bileştirme sorundur. Bu bir kartopu etkisi yaratabilmekte ve sistemin ilk doğrulayıcılarının yeterince servet biriktirmesine ve baskın bir şekilde dağıtılan ödüllerin kendilerinde yoğunlaşmasına neden olabilmektedir. Bu etkiyi önlemek için olası çözümler vardır, ancak bu yöntemler HK'nın zaten karmaşık olan uygulamasını pratikte daha da karmaşık ve kullanımını daha da zor hale getirmektedir. Olası bir çözüm [23]'te verilmiştir. Burada yeni bir geometrik ödül fonksiyonu kullanılarak HK protokolü sunulmaktadır. Ayrıca, HK'nın önemli bir servet yoğunlaşmasına değil, uzun vadede eşit bir dağılıma neden olduğunu öne süren daha yeni araştırmalar da vardır [24]. HK protokolüne yönelik bir diğer olası eleştiri, HK sürecine katılmak için kullanıcı tarafında çalışan bir yazılıma duyulan ihtiyaçtır. Bu, bir kripto para birimi uygulaması için sıradan görünebilse de aslında çok az bilgi işlem gücüne sahip veya hiç bilgi işlem gücü olmayan

eski cihazların ağa dahil edilmesi gereken uygulamalar için ciddi şekilde sorun olabilecektir.

HK, Ethereum ağında 1 Aralık 2020'den 15 Eylül 2022'de birleşme olarak adlandırılan ve 2. en büyük kripto para biriminin (piyasa değerine göre Bitcoin'den sonra) ana uzlaşma algoritmasının İK'dan HK'ya dönüştürüldüğü zamana kadar ayrı bir blokzinciri olarak uygulanmıştır [17]. Yan zincirin ve ana zincirin birleşmesinden sonra, başlangıçta merkeziyetsizlik vaat eden bir sistem için merkezileşme riski ortaya çıkmıştır, çünkü hisse mevduatı sahiplerinin büyük bir kısmı hisse havuzlarına yoğunlaşmıştır. "Hildobby" kullanıcısı tarafından oluşturulan bir Dune web sitesi, en büyük bahis havuzu Lido'nun yatırılan tüm tutarın %29'una sahip olduğunu, Coinbase'in %12.9 ve Kraken'in %7.5 payla hisse barındırdığını göstermektedir. Bu web sitesi Ethereum ağındaki hisseler hakkında ayrıntılı istatistikler göstermektedir ve %49,4'luk bir hisse payının hisse havuzlarında olduğu izlenebilmektedir [25]. Bu, Ethereum ağının merkeziyetsizlikten uzaklaştığını ve kripto para biriminin, blokzincirinin adaleti ve güvenliği için risk oluşturabilecek belirli havuzlara odaklandığını göstermektedir.

### 2.2.3 Yetki Kanıtı

Yetki kanıtı veya bazen kimlik kanıtı olarak adlandırılan bu yöntem, yalnızca özel blokzinciri uygulamalarında kullanılan bir uzlaşma protokolüdür ve gerçek hayattaki kimlikleri bilinen doğrulayıcılar için uygulanan bir itibar sistemine dayanmaktadır. Bu yöntemde, bir doğrulama düğümü olarak görev alabilmek için, doğrulayıcı adayları gerçek kimlikleriyle ilgili doğrulanmış ve noter onaylı belgeler sağlamalıdır [12]. Doğrulayıcı adresi gerçek bir kimliğe bağlı olduğundan, kötü niyetli bir kişinin blokları doğrulamasına izin verilmeyeceğinden emin olunan bir güvenlik düzeyi oluşturulmuştur. Yetki kanıtı, ilk olarak KİG blokzincirleri için Ethereum kripto para birimi ortamının bir unsuru olarak önerilmiştir ve Aura ile Clique [26] adlı istemcilerde gerçekleştirilmiştir. Bu uzlaşma algoritması genellikle doğrulayıcılar için bir itibar sisteminin kullanılmasıyla desteklenmektedir. En yüksek itibara sahip doğrulayıcı, bir sonraki bloğu doğrulamak için en yüksek olasılığa sahiptir ve en az itibarlı doğrulayıcı, ödül almak için en küçük şansa sahip olacaktır. Doğrulayıcılar, blokzincir düğümleri tarafından kararlaştırılan izlek adına hareket ederek itibar kazanmakta ve çelişkili davranışlarla itibar kaybetmektedir.

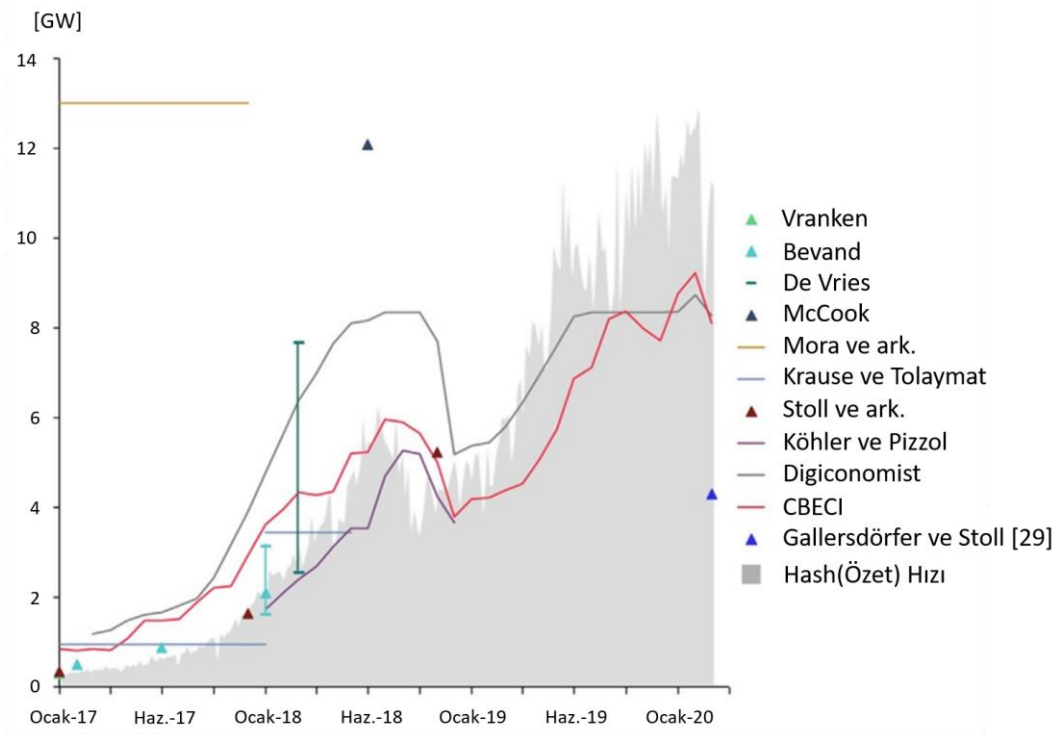
Bu mekanizma, doğrulayıcıların kötü niyetli davranmamalarını sağlamaktadır, çünkü yanlış davranışlar sonucunda bir ödül kazanmak için blokları yayınlama konusundaki değerli haklarını kaybetmektedirler. Ayrıca, doğrulayıcıların donanımlarını çalışır durumda tutmaları beklenmektedir, böylece ağda herhangi bir anda yeterli sayıda doğrulayıcı bulunmaktadır. Doğrulayıcı düğümün donanımının güvenliği de doğrulayıcıların yükümlülüğüdür. Bu nedenle, doğrulayıcılar sık sık bilgisayarlarının güvenliğinin ihlal edilmediğinden veya yanlış davranmadığından emin olmalıdır.

Yetki Kanıtı uzlaşma algoritması, hızlı ve enerji tasarruflu bir blok doğrulaması sağlamaktadır, ancak yöntem yalnızca KİG blokzincirleriyle sınırlıdır. Doğrulayıcıya yönelik güven gerçek hayattaki belgelerle kurulduğundan, dünyanın her yerinden düğümlere sahip halka açık bir blokzincirinde bir uygulama çok zor olacaktır. Yetki Kanıtı'na yönelik bir başka eleştiri, kötü niyetli olarak hareket eden düğümlere karşı düşük direnç göstermesi ve bunun sonucunda blokzincirinin tutarlılığındaki kayıptır. De Angelis ve ark., Yetki Kanıtı protokolünün, Bizans hatası üreten düğümlerinin varlığında kullanılabilirlik uğruna tutarlılıktan fedakarlık edebileceğini iddia etmektedir [26]. Bu problem, bu uzlaşma algoritmasının, blokların içindeki verilerin kritik bütünlüğünü gerektiren kullanım durumları için uygun olmadığı anlamına gelmektedir.

## 2.3 Yaygın Olarak Kullanılan Uzlaşma Algoritmalarının Enerji Tüketimi

Blokzincir teknolojilerinin kullanımından kaynaklanan enerji tüketimi, teknolojinin ölçeklenebilirliği için büyük bir endişe kaynağıdır. Blokzincir teknolojisinin öncüsü olan Bitcoin, şu anda tüm kripto para birimleri arasında en büyük elektrik gücü tüketicisidir. Aşırı elektrik tüketiminin temel nedeni, yoğun hesaplama gücü gerektiren bir uzlaşma algoritması olan İş Kanıtı algoritmasıdır. Bitcoin madenciliğine veya işletmesine harcanan gücün kesin miktarını hesaplamanın bilinen bir yöntemi yoktur, ancak dünyanın dört bir yanındaki araştırmacılar tarafından akademik çalışlar ile tahminler yapılmaktadır. Alex De Vries tarafından yürütülen çalışmalar, Bitcoin'in yıllık enerji tüketiminin, 71.60TWh ile Columbia'nın yıllık toplam güç tüketimiyle karşılaştırılabilir ve Çek Cumhuriyeti'nin yıllık güç tüketiminden daha fazla olduğu belirtmektedir. Bitcoin'in ilgili karbon ayak izi yıllık 39.93Mt $CO^{2}$'dir ve Digiconomist web sitesinde [27] sunulan istatistiklere göre İsviçre'nin karbon emisyonlarına yakındır. Kullanılan

enerji miktarı ve İK blokzincirini kullanmanın genel olumsuz etkisi, dijital bir ödeme sistemi için oldukça büyük bir problemdir. Bitcoin ağının güç tüketimi üzerine yapılan bir başka araştırma Christian Stoll ve ark. tarafından Bitcoin'in tahmini güç tüketiminin Kasım 2018'de 5.501 MW olacağını belirtmektedir [28]. Aynı araştırma, Bitcoin'in ve ardından gelen üç kripto para biriminin birleşik enerji tüketiminin 30 TWh'ye kadar çıkacağını tahmin etmektedir. Şekil 2.5, farklı araştırma makalelerinden toplanan Bitcoin ağının tahmini güç tüketimi verileri göstermektedir.



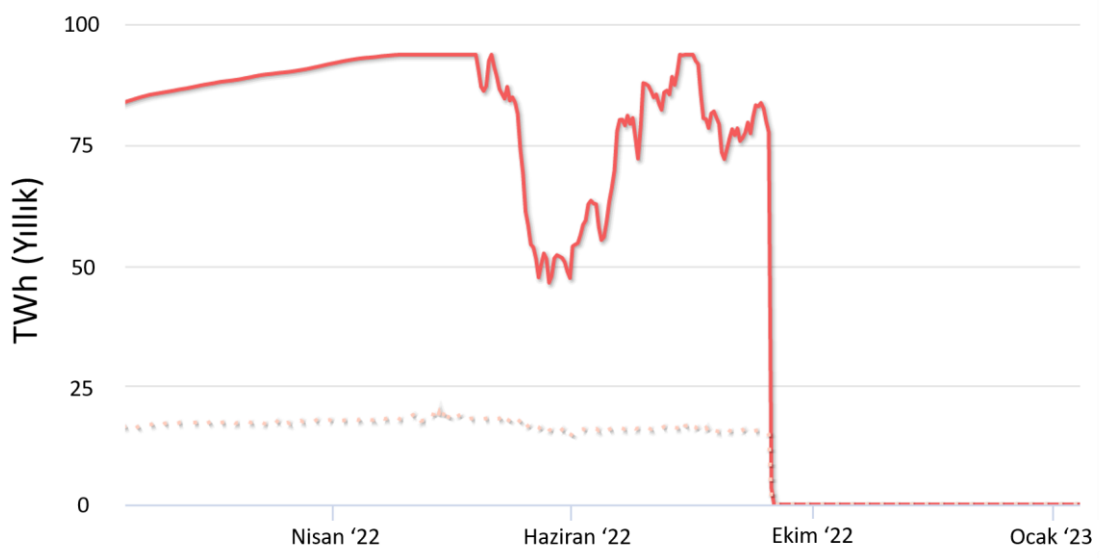

Şekil 2.5: Bitcoin'in 2017'den 2020'ye kadar olan güç tüketimi tahminleri [29].

İş Kanıtının enerji yoğun yapısı, birçok akademisyen ve blokzincir topluluğu tarafından ciddi eleştirilere maruz kalmaktadır, ancak kripto para sektörü Bitcoin'e ve Bitcoin'in değerine fazlasıyla odaklanmıştır ve bu durum Bitcoin'e karşı alınacak tedbirleri önlemektedir. Ağın en büyük katılımcıları olan ve Bitcoin madenciliği için ASIC'ler gibi pahalı donanımlara yatırım yapan madenciler, kripto para biriminin uzlaşma algoritmasını değiştirmeye istekli olmayacaktır, çünkü bu halihazırda yapılmış yatırımları için ekonomik bir kayıp anlamına gelecektir.

Bitcoin kullanımı tek başına değerlendirildiğin de dahi çok miktarda sera gazı üretmekte ve küresel ısınmaya aktif olarak katkıda bulunmaktadır. Camilo Moro ve ark. analizinde, kripto para biriminin yaygın olarak kullanılan diğer teknolojiler gibi benimsenmesi durumunda Bitcoin'in tek başına $2^{o}$C'lik bir küresel ısınma için yeterli karbon emisyonu yaratacak bir elektrik talebine neden olabileceğini öne sürmüştür [30]. Bu, karbon emisyonlarını azaltmak ve küresel ısınmayla mücadele etmek için Paris İklim Değişikliği Anlaşması'nda belirtilen çabanın, Bitcoin'in yaygın olarak benimsenmesi durumunda asla başarılamayacağı anlamına gelmektedir. De Vries'in bir başka makalesi, elektrikli araçların adaptasyonu sağlanacak ile 2020'deki toplam karbon emisyonu tasarrufunun, yalnızca Bitcoin'in tahmini toplam karbon ayak izi ile aşılabileceğini belirtmiştir [31]. Bu araştırmalar, Bitcoin gibi İş Kanıtı tabanlı blokzincir teknolojilerinin, iklim değişikliğiyle mücadele etmek için net sıfır emisyona giden yolda yaygın olarak kullanılamayacağını göstermektedir. Politikacılar bu gerçeğin farkında olduklarını göstermek istemektedirler ve ABD, AB ve Çin'de Bitcoin madenciliği gibi İş Kanıtı kullanan blokzincir teknolojilerini yasaklamak için artan bir çaba sarf edilmektedir [31]. Avrupa Parlamentosu, Mart 2022'de enerji yoğun uzlaşma algoritmalarını kullanan blokzincir teknolojilerine yasak getirmeye çalışmıştır, ancak kripto para birimi destekçilerinin karşıt eylemleriyle bu istek başarısız olmuştur [32]. İş Kanıtına karşı gerçekleşen bu siyasi hareketler, Bitcoin'i uzlaşma algoritmasını değiştirmeye veya talepte büyük bir düşüşle karşı karşıya kalmasına neden olacak şekilde Dünya'nın farklı yerlerinde bu uzlaşma algoritmasının yasaklanmasıyla sonuçlanabilecektir.

Uzlaşma algoritmasının güç tüketimi sadece bir İş Kanıtı veya Bitcoin sorunu değil, aynı zamanda kripto varlıklarının mevcut durumu hakkında daha genel bir sorun olarak kabul edilmektedir. Jingming Li ve ark. tarafından yapılan araştırmaya göre, Nisan-Aralık 2018 tarihleri arasında, Çin'de popüler olan bir kripto para Monero'nun madenciliği nedeniyle 19,12 ila 19,42 bin ton arasında tahmini karbon emisyonu ve 30,34 GWh elektrik tüketimi meydana gelmiştir [33]. Benzer bir durum BitcoinCash için de geçerli olup, Tim Swanson'ın çalışmasıyla BitcoinCash için kripto para işlemlerinin yıllık 4,3 milyar kWh elektrik tüketimine neden olduğu tahmin edilmektedir [34]. Aynı çalışma, Litecoin için yılda ortalama 4,2 milyar kWh elektrik tüketimi tahmin etmektedir. BitcoinCash, Litecoin ve Monero da büyük miktarda güç harcamasına yol açan bir uzlaşma algoritması olan İş Kanıtı kullanmaktadır. En popüler kripto para birimlerinden bazılarının güç tüketiminin

ve ilgili özet algoritmalarının kapsamlı bir karşılaştırması [29]'da verilmiştir. Bu karşılaştırmada Bitcoin, en büyük 20 kripto ağı arasında enerji tüketiminin %68,39'u ile en çok tüketici olurken, onu %11,46 ile Ethereum, %4,32 ile RavenCoin, %3,35 ile Monero, %2,63 ile Litecoin, %2,51 ile DogeCoin, %2,44 ile BitcoinCash takip etmektedir. Ethereum'un söz konusu makalenin yayınlanması sırasında hala HK yerine İK kullandığını ve Ethereum'un enerji tüketiminin birleşmeden sonra büyük ölçüde düştüğünü dikkate almak gereklidir. Hisse Kanıtı mekanizması, yoğun bilgi işlem gücüne bağlı olmadığından, katılımcı düğümler arasında uzlaşmaya varmak için elektrik kullanımını verimli bir şekilde azaltmaktadır. Bugün, Ethereum ağının yıllık yalnızca 0.01TWh güç tüketimine neden olduğu tahmin edilmektedir [35]. Şekil 2.6, HK uzlaşma protokolünün uyarlanmasından sonra Ethereum ağı için elektrik tüketiminde ciddi bir düşüş olduğunu göstermektedir.




Şekil 2.6: HK'nın uygulanmasından önce ve sonra Ethereum ağının enerji tüketimi [35].

## 2.4 Akıllı Şebekeler ve Akıllı Sayaçlar

Bir elektrik şebekesi, üretim, iletim, dağıtım ve elektrik tüketimini içeren güç sistemi olarak tanımlanmaktadır [4]. Geleneksel bir elektrik şebekesinde, elektrik az sayıda merkezi enerji üreticisinden çok sayıda dağıtılmış elektrik müşterisine aktarılmaktadır. Akıllı şebeke, gelişmiş bir otomatik ve dağınık enerji dağıtım ağı oluşturmak için geleneksel olmayan güç akışı ve çift yönlü bilgi akışı yetenekleri sağlayan bir elektrik

şebekesi olarak tanımlanan, halen geliştirilmekte olan yeni bir kavramdır [36]. Geleneksel şebeke yapısı ile akıllı şebekenin karşılaştırması Tablo 2.1'de sunulmaktadır.

Tablo 2.1: Geleneksel şebeke ve akıllı şebeke yapılarının karşılaştırılması [36].

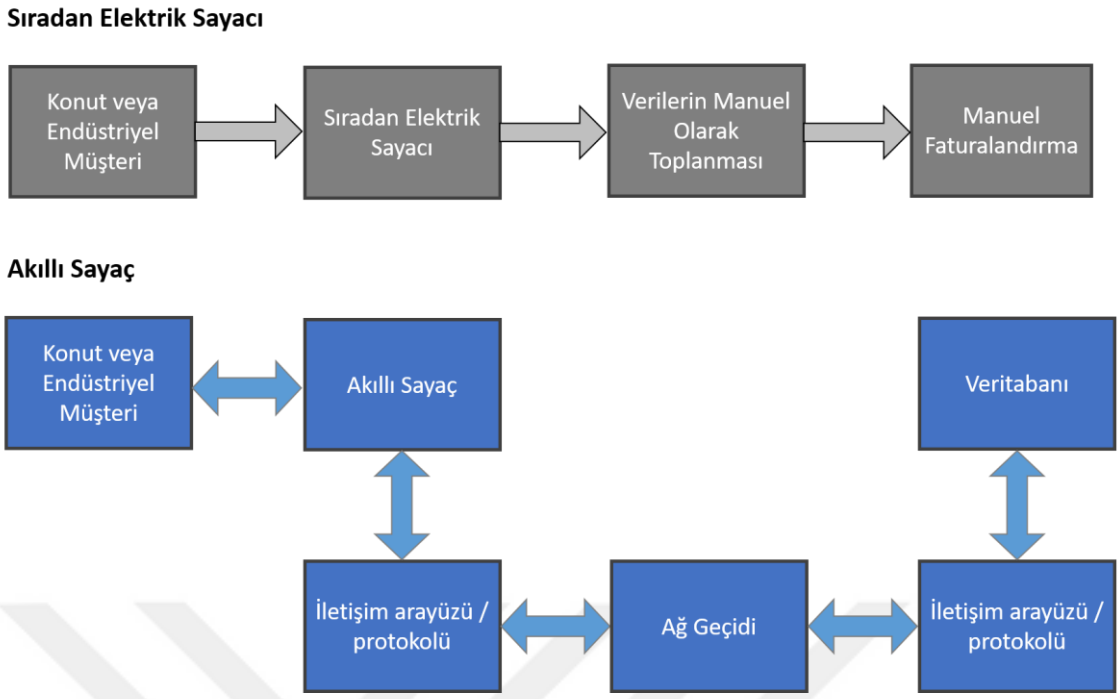
| Geleneksel Şebeke | Akıllı Şebeke |
|---|---|
| Sınırlı kontrol | Kapsamlı kontrol |
| Tek yönlü iletişim | İki yönlü iletişim |
| Manuel izleme | Kendi kendini izleme |
| Arızalar ve elektrik kesintileri | Uyarlanabilirlik ve bağımsızlaştırma |
| Manuel geri yükleme | Kendi kendini iyileştirme |
| Merkezi üretim | Dağıtılmış üretim |
| Az sayıda müşteri seçeneği | Pek çok müşteri seçeneği |
| Elektromekanik | Dijital |
| Birkaç sensör | Sensör yoğun |

Akıllı bir şebeke, modern teknolojinin kullanılmasıyla genel elektrik üretimi, dağıtımı, iletimi ve tüketimine çeşitli şekillerde fayda sağlayabilmektedir. Örneğin, bir akıllı şebekenin kullanılması, otomatik cihazların elektrik akışını yeniden yönlendirdiği ve arızalı bileşenleri son kullanıcıdan izole ettiği bir dağıtım yapısıyla birlikte, bir arıza olması durumunda elektrik kesintisini önleyebilecektir. ABD Enerji Bakanlığı Ulusal Enerji Teknolojisi Laboratuvarı, 2007 yılında elektrik şebekelerinin geleceği hakkında bir araştırma yaparak bir eylem çağrısı yayınlamıştır ve gelecekteki bir şebekenin aşağıda listelenen 7 temel özelliğe sahip olması gerektiğini belirtmiştir [37]:

- Kendi kendini iyileştirmek
- Müşteriyi motive etmek ve dâhil etmek
- Saldırılara direnmek
- 21. yüzyılın ihtiyaçları için güç kalitesi sağlamak
- Tüm üretim ve depolama seçeneklerine uyum sağlamak
- Piyasaları etkinleştirmek
- Varlıkları optimize etmek ve verimli bir şekilde çalışmak

Akıllı şebekeye duyulan ihtiyaç, yerel ölçekte yenilenebilir enerji üretimine yönelik mevcut eğilimle birlikte artmaktadır. Dünyanın dört bir yanındaki birçok elektrik müşterisi yenilenebilir enerji kaynaklarıyla kendi elektriğini üretmeye yatırım yapmaya başladıkça, elektrik şebekesinin geleneksel yapısı, üreten tüketici talebini ve katkısını ele almada yetersiz kalmaya başlamaktadır. Dağıtılmış yenilenebilir enerji kaynakları ve enerji depolama ekipmanı, depolanan fazla elektriği ve üretimlerini diğer tüketicilere satma seçeneği mevcut olduğunda müşteriler için daha davetkâr hale gelmektedir [38]. Dağıtılmış yenilenebilir enerji kaynaklarından kaynaklı çift yönlü elektrik aktarımı için oluşan bu gereklilik, akıllı şebekelerin adaptasyonunu daha acil hale getirmektedir. Aynı zamanda günümüzde sera gazı emisyonlarını azaltma çabaları ve küresel ısınmaya karşı önleyici tedbirler sürekli olarak artmaktadır. Gelişmiş ülkelerin sürdürülebilirlik çabaları ve yenilenebilir enerji tesislerinin daha küçük ölçekte kurulmasıyla elektrik üretimini daha yerel hale getirmektedir. Bu etken, yenilenebilir enerji kaynaklarının elektrik şebekesine verimli bir şekilde katkıda bulunduğundan emin olmak için akıllı şebekelerin geliştirilmesini ve uygulanmasını hızlandırmaktadır.

Akıllı şebeke kavramı, akıllı sayaçlar, talep yanıtı, talep tarafı yönetimi, doğrudan yük kontrolü ve toplayıcılık gibi çeşitli yeni teknolojilerin ve kavramların kullanımı ile bir arada anılmaktadır. Bu makale boyunca da atıfta bulunulan önemli bir akıllı şebeke teknolojisi akıllı sayaçlardır. Akıllı sayaç, tüketici tarafından kullanılan her elektrik yükünden enerji kullanım verilerini toplayan ve faturalama ve izleme için faydalı bilgileri ilgili hizmet şirketine aktaran son teknoloji bir güç ölçerdir [4]. Akıllı sayaçların önemli bir özelliği de tüketim verilerini gerçek zamanlı olarak raporlayabilmesidir. Bu, yüklerin düzenli zamanlaması, güç hattındaki frekans-gerilim ihtiyaçları ve gelecekte ortaya çıkabilecek olası yükler hakkında şebeke yöneticisine değerli bir veri akışı sağlar. Akıllı sayaçlar ayrıca tüketiciler ve şebeke hizmeti yöneticisi için birçok farklı enerji yönetimi amacı için kullanılabilen iki yönlü bir iletişim yapısı sağlamaktadır. Akıllı sayaçların belirli bir yükün bağlantısını kesme yeteneği, toplayıcı veya şebeke hizmeti şirketi tarafından talep tarafı yönetimi ve talep yanıtı için kullanılabilmektedir [4]. Bir akıllı sayaç ile sıradan sayacın basitleştirilmiş mimarileri Şekil 2.7'de gösterilmektedir.

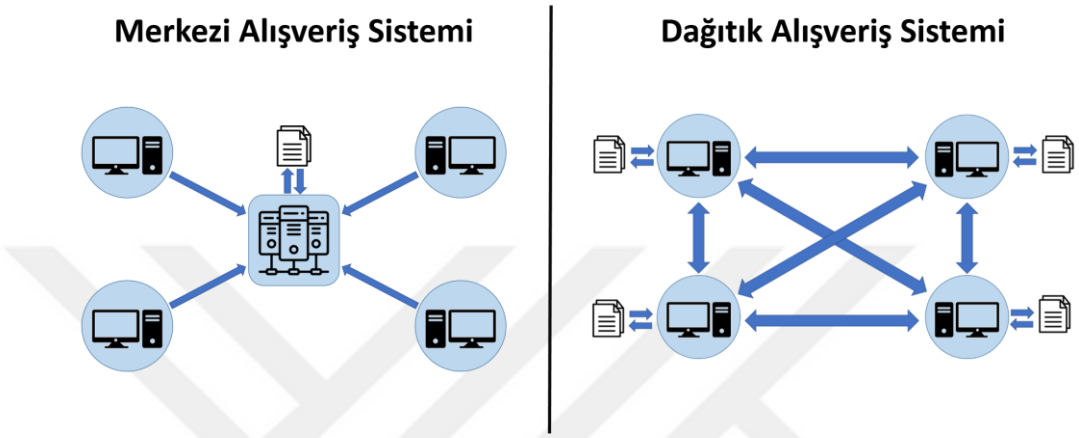



Şekil 2.7: Klasik ve akıllı sayaç arasındaki mimari farklılıklar [39].

## 2.5 Eşler Arası Enerji Ticareti ve Yerel Enerji Piyasaları

Klasik enerji piyasası yapısı, dengeli ve güvenilir bir enerji ticareti elde etmek için birlikte çalışan merkezi bir ticaret otoritesine ve ilgili sistem operatörlerine dayanmaktadır. Elektriğin depolanması çok sınırlı ve pahalı olduğundan, üretilen enerjinin şebekede üretilmesi ile aynı anda tüketilmesi gerekmektedir. Elektrik tüketimi ve üretimi arasındaki dengeyi kolaylaştırmak için santrallerin bir sonraki günkü üretim oranlarının belirlenmesinde gün öncesi piyasası kullanılmaktadır. Spot piyasa olarak da adlandırılan gün öncesi piyasasında bir şebeke işletmecisinin bağlantılı santrallerin üretim oranını belirlediği piyasalarda elektrik piyasası merkezileşmiş olarak kabul edilmektedir [3]. Öte yandan, merkeziyetsiz elektrik piyasalarının elektrik üretimine ilişkin günlük bir planlaması yoktur veya spot piyasada sadece taahhütle çalışmaktadır. Her iki piyasa tipinin de günlük enerji dengesi ve günlük elektrik yönetimi üzerinde kendi olumlu ve olumsuz etkileri vardır, ancak geleneksel merkezi piyasa yapıları, artan sayıda dağıtılmış enerji kaynaklarının sisteme dâhil edilmesi için kıyasla daha az uygundur. Enerji sektörü hızla dijitalleşmektedir, bu nedenle günümüz elektrik piyasalarında bilgi alışverişi, çift yönlü iletişim ve yerelleştirme ihtiyacı daha fazla önem kazanmaktadır. Çok fazla iletişim talebi olan birçok aktörün merkezi yönetimi, merkezi olmayan bir çözüme kıyasla daha zordur [40]. Merkezileştirilmiş enerji piyasası, çok sayıda üreten tüketiciye sahip bir

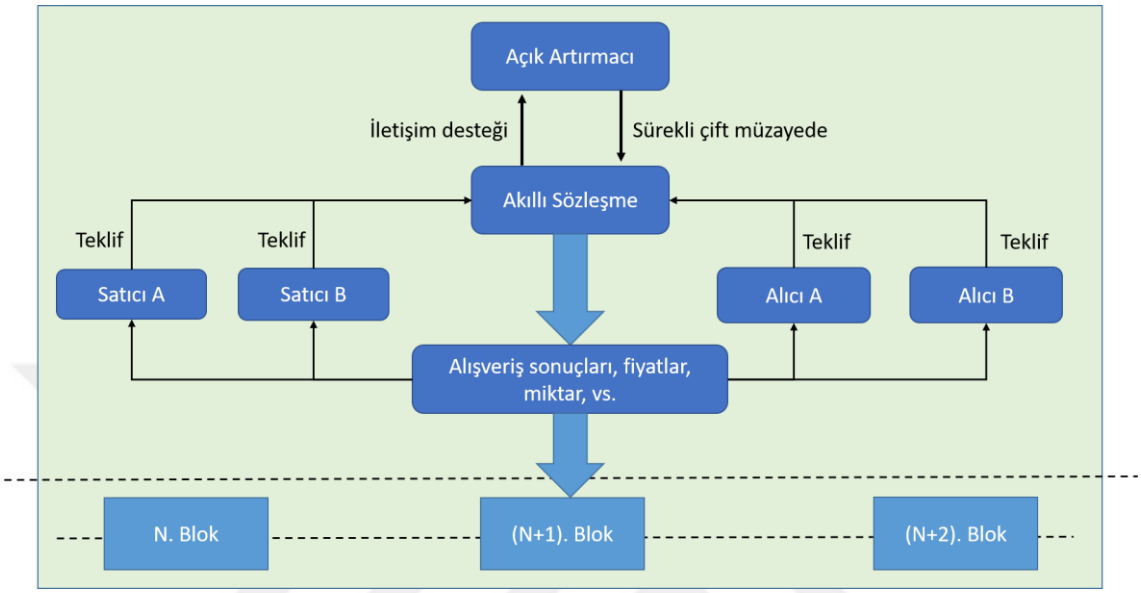
topluluk için merkeziyetsiz bir piyasaya kıyasla daha az ölçeklenebilirdir. Akıllı şebeke üyeleri arasındaki elektrik ticaretini merkeziyetten uzaklaştırmak için sunulabilecek iyi bir çözüm, eşler arası ticaret ve dağıtık defter teknolojilerinin kullanılmasıdır. Merkezi alışveriş hizmetleri ile dağıtılmış alışveriş hizmetleri arasındaki genel yapısal fark, Şekil 2.8'de gösterilmektedir.




Şekil 2.8: Merkezi ve dağıtılmış alışveriş sistemleri arasındaki temel yapısal farklılıkları gösteren bir şema [40].

Eşler arası (Peer-to-peer, P2P), tüm aracıların bir mal veya hizmeti üretmek, değiş tokuş etmek veya dağıtmak için erişilebilir yetenekleriyle işbirliği yaptığı merkezi olmayan bir sistemi tanımlamaktadır [41]. Bu durumda eşler tüketiciler, üreticiler, üreten tüketiciler, enerji depolama işletmecileri ve şebeke işletmecileri gibi elektrik piyasasındaki aktörler olarak tanımlanmaktadır. Enerji ticareti için P2P mimarisini kullanma önerisi ilk olarak Hakem Beitollahi ve Geert Deconinck tarafından "Peer-to-Peer Networks Applied to Power Grid" [42] adlı makalede yapılmıştır. P2P enerji ticareti, aynı zamanda, eşler arasında enerji alışverişi için çoklu ikili anlaşmalar olarak da açıklanabilmektedir. İkili anlaşma, elektrik piyasasındaki iki farklı aktör arasında kararlaştırılan bir fiyat üzerinden belirli bir süre için elektrik ticareti yapmak için bağlayıcı bir garanti anlamına gelmektedir. Bir P2P bağlamında gerçekleştirilen bu sözleşmeler, bir mikro şebekenin üyeleri arasındaki elektrik ticareti için bir temel anlamına gelmektedir. P2P pazar tasarımı ve uygulamaları üzerine yapılan araştırmalar, blokzincir teknolojisinin kullanımının, birçok aktif kullanıcıya sahip merkeziyetsiz bir enerji piyasası için umut verici bir çözüm olabileceğini göstermektedir [43]. Blokzincir tabanlı P2P enerji ticareti ile ilgili diğer çalışmalar, bu makalenin 3. Bölümünde daha ayrıntılı olarak ele alınmış ve 4. Bölümde

yüksek enerji verimliliğine sahip yeni bir örnek model önerilmiştir. P2P enerji ticareti için akıllı sözleşmeler kullanan olası bir blokzincir uygulamasının örnek şeması Şekil 2.9'da gösterilmektedir.




Şekil 2.9: Blokzincir akıllı sözleşmeleri ile P2P enerji ticaretine bir örnek [43].

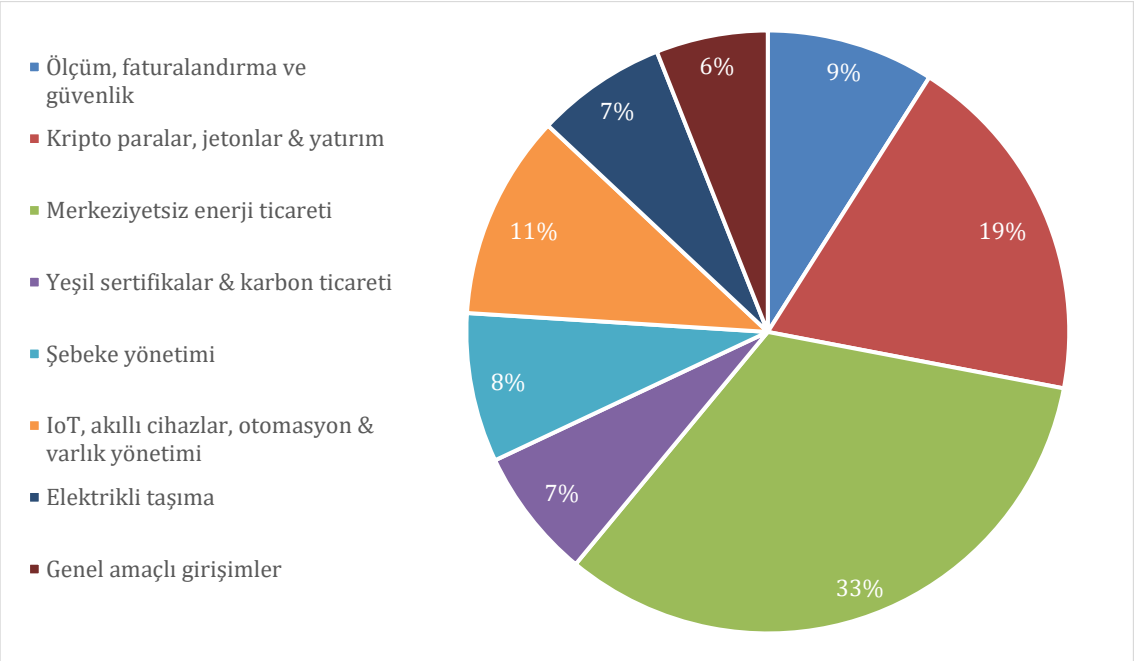
# 3. İLGİLİ ÇALIŞMALAR

## 3.1 Literatür Taraması

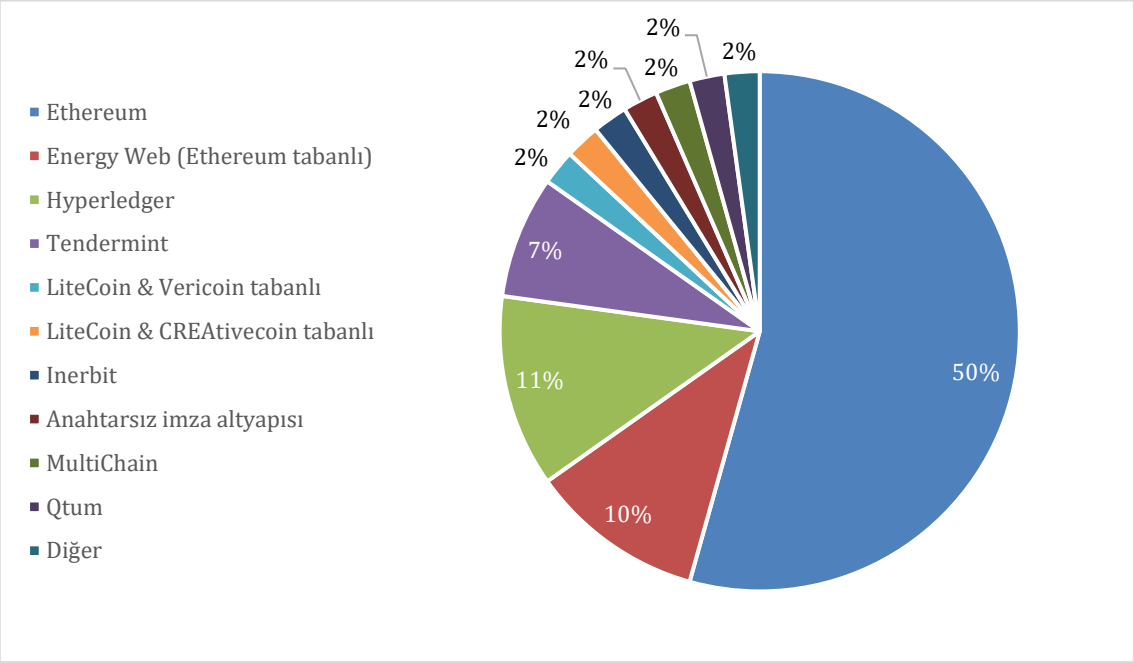
Blokzincir teknolojisinin kullanılmaya başlanmasının ardından dünyanın birçok farklı yerinden akademisyenler, soruna farklı yaklaşımlarla merkeziyetsiz elektrik ticareti çözümleri önermişlerdir. Blokzincir tabanlı bir çözüm üzerinde çalışmak, birçok düğümün ve dağıtık bir sistemin katılımını içermektedir, bu nedenle alanda çalışan akademisyenler genellikle daha küçük bir ölçekle başlamakta ve gelecekte gerçekten ihtiyaç duyulabilecek daha büyük uygulamalara ölçeklenebilirlik önerilerinde bulunmaktadır. Bu nedenle, bu alandaki çalışmalar, doğrudan bir ulusal enerji ticareti çözümünden ziyade çoğunlukla küçük ölçekli mikro şebekelere dayanmaktadır. Bu bölümdeki gözden geçirilen araştırmalar, dağıtık defter çözümünün farklı yönlerine odaklanmaktadır ve bu yönler şu şekildedir: önerilen blokzincir çözümünün yönetimi, piyasa mimarisi, şebeke yapısı ve güvenlik. Blokzincir teknolojisini kullanan P2P enerji

ticaretiyle ilgili bir dizi makale, uzlaşma algoritmasına odaklanarak bu bölümde daha ayrıntılı olarak incelenmiş ve analiz edilmiştir. İncelenen her bir makale bu çalışmanın bir sonraki bölümünde önerilen modellerin enerji verimliliği, güvenlik, mahremiyet ve büyük ölçekli gerçek yaşam kullanımına uygunluğu açısından analiz edilmiştir.

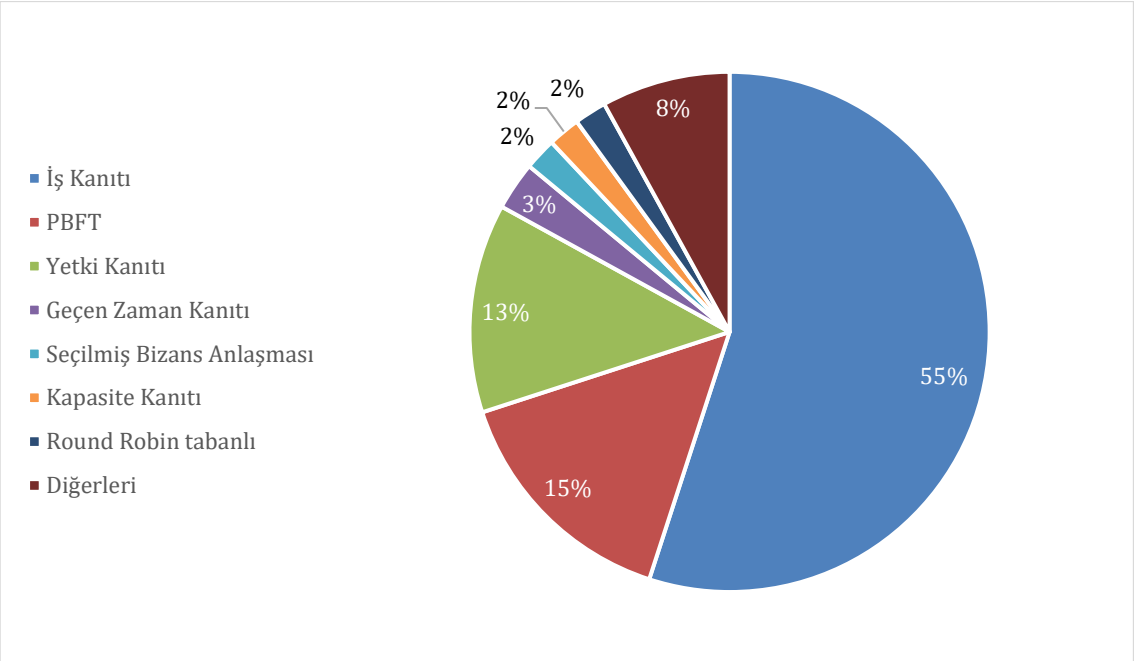
Enerji endüstrisindeki blokzincir teknolojisinin kullanımının kapsamlı bir incelemesi, M. Andoni ve ark. Tarafından mevcut kısıtlamalar ve gelecekteki fırsatların açısından araştırılmıştır [40]. Söz konusu makale, enerji sektöründeki farklı uzmanlık alanları için blokzincir teknolojisinin kullanımına ilişkin verileri sunmaktadır. Şekil 3.1, blokzincir teknolojisi için enerji sektöründeki farklı kullanım alanlarının dağılımını göstermektedir. Bu şekilde görüldüğü gibi, merkezi olmayan enerji ticareti, blokzincir teknolojisi için en popüler kullanım işlevidir ve bunu kripto para birimleri, jetonlar ve yatırım takip etmektedir. Şekil 3.2, enerji ile ilgili bu uygulamalarda kullanılan blokzincir platformunun yüzde olarak dağılımını göstermektedir. Ethereum, akıllı sözleşmelerin kolay devreye alınmasını ve sektör için birçok avantajı beraberinde getirmesi nedeniyle, enerji projeleri ve araştırmaları için en yaygın kullanılan platformdur. Şekil 3.3, incelenen makale ve projelerde kullanılan uzlaşma algoritmalarının dağılımını göstermektedir. Şekil 3.3'te, İK en sık kullanılan uzlaşma algoritmasıdır ve onu Pratik Bizans Hata Toleransı ve Yetki Kanıtı takip etmektedir. İK en yaygın yöntem olarak görünmektedir çünkü bu uzlaşma algoritması söz konusu makale yayınlandığında Ethereum ekosisteminde hala kullanılmaktaydı, ancak bugün bu yüzde muhtemelen Ethereum'un birleştirilmesinden sonra çok daha düşük olacaktır [17]. Bu makalede Andoni ve ark. alandaki mevcut ve potansiyel zorlukları gözden geçirmekte ve İK'nın düşük enerji verimliliğinin üstesinden gelinmesi gereken kritik bir zorluk olacağını önermektedir. Çalışmamızın 4. Bölümü, bu incelemede belirtilen zorlukların merkezi olmayan enerji ticareti için nasıl çözülebileceğini açıklayacaktır. Mikro şebekeler için P2P enerji ticareti projelerinin genel bir karşılaştırması Zhang ve ark tarafından verilmiştir. [44]. Bu literatür taraması, blokzincir teknolojisinin müşterilerin faturalandırmasını kolaylaştırırken P2P elektrik ticareti için çok başarılı bir çözüm olabileceğini göstermektedir. Zhang ve ark. P2P enerji ticareti için pratik ulusal şebeke uygulamalarından örnekleri sunmuş ve bunları proje kapsamlarına ve kazanımlarına göre karşılaştırmıştır.




Şekil 3.1: Blokzincir teknolojisi kullanımının farklı alanlarına ve bunların dağıtımına genel bakış [40].




Şekil 3.2: Enerji sektörü uygulamalarında kullanılan blokzincir platformlarına genel bakış [40].




Şekil 3.3: Her bir uygulama için kullanılan uzlaşma algoritması türünün dağılımı [40].

Güney Kore'den Kang, Song ve ark. tarafından mikro şebeke ölçeğinde orijinal bir Ethereum dağıtılmış uygulaması kullanan blokzincir temelli bir enerji ticareti uygulaması önerilmiştir [45]. Kang, Song ve ark. mikro şebekenin enerji akışını ve elektrik ticaretini kontrol etmenin bir yolu olarak Ethereum tabanlı bir blokzinciri tanımlamıştır. Her bir düğüm, bir madenciye sahip bir tüketici evi olarak tanımlanmıştır ve her düğüm, bir Ethereum akıllı sözleşmesi kullanılarak otonom olarak elektrik ticareti yapmaktadır. Önerilen model, Ethereum'un eşit kurallara sahip bir yan zinciri olan özel bir blokzinciridir. Bu nedenle model, akıllı sözleşmeleri çalıştırma ücreti olarak İş Kanıtı ve Ethereum'un gaz yapısını kullanmaktadır. Yazarlar tarafından mikro şebekedeki talebi ve üretimi dengeleyen bir dizi al/sat komutuyla enerji ticareti yapmak için akıllı sözleşmeler kodlanmıştır. Bu makale, piyasa yapısına oldukça geniş bir bakış sunmakta ve bir enerji piyasasının akıllı sözleşme yapısıyla uygulamasına odaklanmaktadır.

Li, Kang ve ark. tarafından yapılan başka bir çalışma eşler arası enerji ticareti için IIOT'de bir konsorsiyum blokzinciri önermektedir [46]. Konsorsiyum terimi, sisteme yalnızca seçilen düğümlerin katılabileceği için blokzincirinin KİG yapısında olduğunu açıklamak için kullanılmaktadır. Bu model ayrıca, enerji toplama ağlarını ve araçtan şebekeye uyarlamalarını dikkate almanın yanı sıra bir mikro şebeke yaklaşımı kullanmaktadır.

Modelde kullanılan blokzinciri, Endüstriyel Nesnelerin İnterneti kullanım maliyetini en aza indirecek şekilde tasarlanmıştır. Yazarlar ayrıca, uzun doğrulama süresini telafi eden ve ticareti sürekli kılan ödemeler için bir kredi sistemi önermişlerdir. Bu yöntemde kullanıcılar, cüzdanlarında istedikleri enerji ticaretini tamamlamak için yeterli para yoksa sanal bir bankadan kredi alabilmektedir. Krediler, blokzincirindeki önceki davranışlarına göre her bir düğüme atanan bir kredi puanına göre verilmektedir. Şebekeye bağlı IIOT cihazlarının sürekli olarak enerji ticareti yapması ve bakiyeleri yeterli olmadığında kripto para biriminde otonom olarak gerekli krediyi alması önerilmiştir. Bu makale ayrıca mikro şebeke ekonomisini dengede tutmak için bir sanal banka sistemi ve optimal fiyatlandırma önermektedir.

Mengelkamp ve ark. Almanya'da bir akıllı şebekede bulunan blokzincir ile yerel bir enerji piyasası modeli önermiştir [47]. Bu model aynı zamanda akıllı sözleşmelerden yararlanmak için Ethereum tabanlı blokzincir teknolojisini kullanmaktadır. Ücretler üzerindeki kontrolü kolaylaştırmak ve güvenlik konularını bir otoritenin yardımıyla savuşturmak için özel ağa sahip bir blokzincir modeli kullanılmıştır. Yazarlar bir simülasyon yöntemi sağlamakta ve önerilen modeli Alman elektrik şebekesinden gerçek girdilerle simüle etmektedir. Yazarlar, mikro şebekede bir yıllık ticaretin ve gerektiğinde ulusal şebekeyle yapılan ticaretin simülasyonunun ardından, ortaya çıkan avantajlar ve dezavantajlar için sonuçları analiz etmiştir. Sistem, alternatiflerinden daha düşük bir elektrik fiyatı ile güvenli, özel, şeffaf ve uygun maliyetli bir ticaret sistemini başarıyla gerçekleştirmiştir. Ancak bu yeni teknolojinin ölçeklenebilirlik sorunları ve yüksek enerji tüketimi gibi endişeler olduğundan, sistemin sürdürülebilirliğinin kısa ömürlü olacağı öngörülmektedir.

Aitzhan ve Svetinovic, blokzincir tabanlı çoklu-imza enerji ticaret platformları ile güvenlik-gizlilik konularını gözden geçirmiş ve ticaret / mesajlaşma sistemleri için çözümler önermişlerdir [48]. Makale, merkezi olmayan bir platformda ticareti güvenli hale getirmenin bir yolu olarak çoklu imza işlem teknolojisine odaklanmaktadır. Farklı özet algoritmaları ve bunların sistem güvenliği üzerindeki etkileri, ilgili İş Kanıtı süresi sayımlarıyla karşılaştırılmaktadır. Anlık imza kripto mesajlaşmasına sahip token tabanlı bir sistem önerilmiş ve simüle edilmiştir. Sonuçlar, "Priwatt" adlı modele yönelik 43 olası

saldırıyı ve bunlara karşılık gelen çözümleri sunmaktadır. Sistem, yalnızca özel ağa sahip blokzincirlerinde uygulanmadığı için önceki çalışmalardan farklı olarak halka açık erişime sahip güvenli bir blokzinciri sağlamaktadır. Söz konusu makale, blokzincir iletişimini güvence altına almak için dağıtık defter sistemlerinin en son teknoloji kriptografi yöntemleriyle nasıl birleştirilebileceğini göstermektedir.

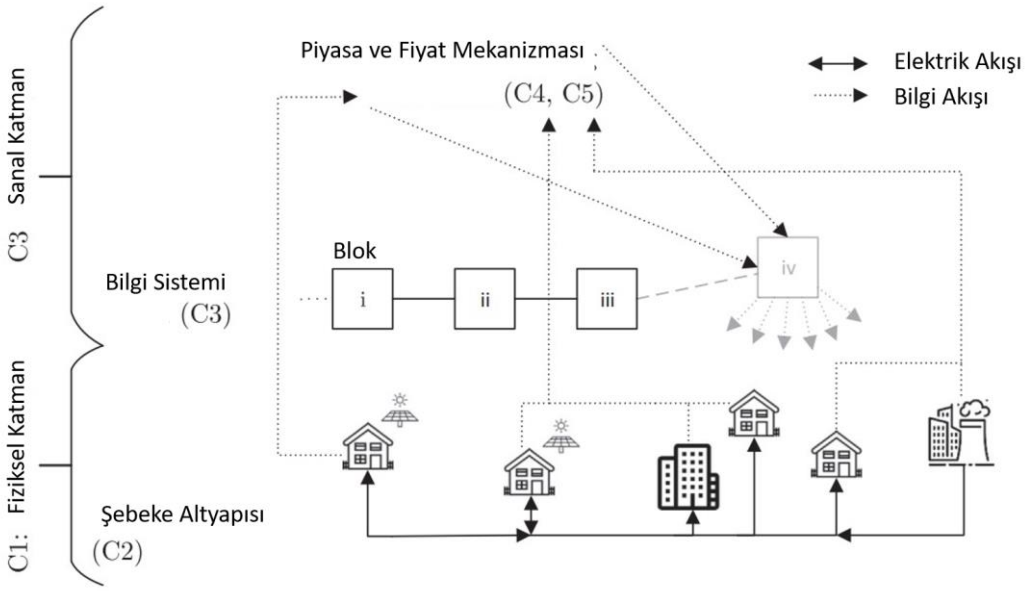
İrlanda Ulusal Üniversitesi'nden Subhasis Thakur ve John G. Breslin, blokzincir tabanlı koalisyon oluşumunu dağıtılmış bir şekilde kullanan bir enerji ticareti platformu tasarlamıştır [49]. Çalışma diğer mikro şebekeler ile modelin arasındaki işlemleri de kapsadığı için bu araştırmadaki model daha büyük bir ölçeğe sahiptir. Koalisyon oluşturma algoritmaları, kavramsal olarak eşler arası yerel enerji piyasaları için mevcuttur, ancak Thakur ve Breslin, benzer yöntemlerdeki bazı kritik sorunları çözen dağıtılmış bir koalisyon oluşturma yöntemi geliştirmiştir. Yöntemin önemli sonuçları arasında eşzamansız ticaret, güvenli ve ölçeklenebilir kurallara sahip merkezi olmayan ticaret yapısı yer almaktadır. Yazarlar, mikro şebekeler arasındaki bir ticareti simüle etmiş ve yakınsama ve ölçeklenebilirlik kriterleri ile merkezi ve merkezi olmayan ticaret seçeneklerini karşılaştırmışlardır. Önerilen model, çok sayıda düğüm üzerinde daha hızlı yakınsama sağlamaktadır ve yakın gelecekte gerçeğe dönüşebilecek birçok bağlantılı mikro şebeke için merkezi modelden daha ölçeklenebilirdir.

Thakur ve Breslin, Barry Heyes ile birlikte çalışarak, fiyata karar vermek için çift müzayede kullanımını içeren, bir mikro şebeke içindeki ticareti kapsayan daha küçük ölçekli bir model önermişlerdir [50]. Modelde kullanılan uzlaşma algoritması, simülasyonların daha hızlı gerçekleştirilebilmesi için özet fonksiyonunun getirdiği bulmacanın zorluğunu azaltmak için değiştirilmiş bir İş Kanıtı varyantıdır. Simülasyon sonuçları, eşler arası bir enerji ticaret sisteminin bilgisayar yatırımı, yakınsama, verimlilik ve sağlamlık açısından merkezi sistemden daha iyi bir çözüm sunduğunu göstermektedir. Çifte açık artırma ilkesi, işlemleri daha hızlı hale getirmekte ve ticareti daha az değişken tutarak talebi ve üretimi sabit tutmaktadır. Genel olarak, blokzincir kullanımı birçok saldırı tarafından kesintiye uğrayabilmektedir, bu nedenle makalede yazarlar güvenlik nedenleriyle kullanıcıların kimliklerini ortaya çıkarmak için hükümet liderliğindeki özel bir blokzinciri önermektedir.

Piyush Verma ve ark. tarafından İrlanda'da gerçekleştirilen bir deneysel blokzincir tabanlı enerji ticaret sistemi olan EnerPort için bir proje raporu hazırlanmıştır [6]. Bu proje, bir yıl boyunca test edilecek olan bir mikro şebekede, eşler arası enerji ticaretine dayanmaktadır. Proje, piyasa modellerinin performansını keşfetmeyi, ihtiyaç duyulan konut yazılımı ve donanımını tasarlamayı ve aynı zamanda blokzincir ve enerji transferinin simülasyonunu hedeflemektedir. Üç ticaret modelinin kullanılması planlanmıştır: koalisyon oluşumu, çift müzayede ve Stackelberg Oyunu. Alanla ilgili literatür taramasına ilişkin bir başka kaynak da, Energy Web Chain'in blokzincir teknolojisi uygulaması hakkındaki teknik incelemesidir [51]. Makale, geliştiricilerin Ethereum sistemindeki, enerji alanındaki kullanımla eşleşmeyen sorunlu noktaları nasıl değiştirdiklerini açıklamaktadır. Burada Yetki Kanıtı, sistemi orijinal Ethereum ağından 30 kata kadar daha fazla ölçeklenebilir ve enerji açısından daha verimli hale getirmek için uzlaşma algoritması olarak seçilmiştir. Blokzincir, ağa katılım için katı bir izin sistemi ile özel ağa sahip bir zincir olarak planlanmış ve IoT cihaz entegrasyonunu küçük bir maliyetle sağlamak için hafif bir istemciye sahip olacak şekilde tasarlanmıştır. Sistemde kullanılan Yetki Kanıtı, kullanıcıların gerçek hayattaki kimlikleri ilgili açık anahtarlara bağlı olduğundan, kullanıcıların mahremiyetinden ödün vererek çok düşük bir doğrulama süresi sağlamaktadır. Ayrıca, uzlaşma algoritması olarak Yetki Kanıtı'nın kullanılması, zincire katılmadan önce her bir düğümün onaylanmasını gerektirdiğinden, birçok elemana sahip büyük ölçekli bir mikro şebekeye uygulandığında bu durum başka ölçeklenebilirlik sorunlarına yol açacaktır.

Blokzincirine dayalı bir P2P enerji ticaret sisteminin test edilmesi için gerçek bir elektrik şebekesinin kullanıldığı bir vaka çalışmasına odaklanan bir proje ABD'de gerçekleştirilmiştir [52]. Brooklyn Microgrid projesi, yeni yenilenebilir enerji kaynaklarının ve modası geçmiş şebeke ekipmanlarının uygulanmasının genellikle ağda tıkanıklıklara neden olduğu ABD, New York'ta 3 farklı dağıtım şebekesinde test edilmiştir. Proje, yerel olarak üretilen elektriğin mikro şebekede yerel enerji piyasasıyla ticareti için iki uygulama katmanı içermektedir: sanal enerji piyasası ve fiziksel mikro şebeke. Projenin bir topolojisi Şekil 3.4'te verilmiştir. Kullanılan blokzinciri teknolojisi, TransActive Grid platformunun blokzinciri uygulamasıdır, dolayısıyla dağıtık defterin yönetim özellikleri buradan devralınmıştır. Vaka çalışmasının sonuçları, blokzincirinin

gerçek hayattaki mikro şebekelerde enerji ticaretinde etkili bir şekilde kullanılabileceğini göstermektedir; ancak yazarlar kullanılan İK uzlaşma algoritmasının büyük enerji tüketiminden bahsetmemiştir.




Şekil 3.4: Brooklyn Microgrid projesinin üst düzey topolojisi [52].

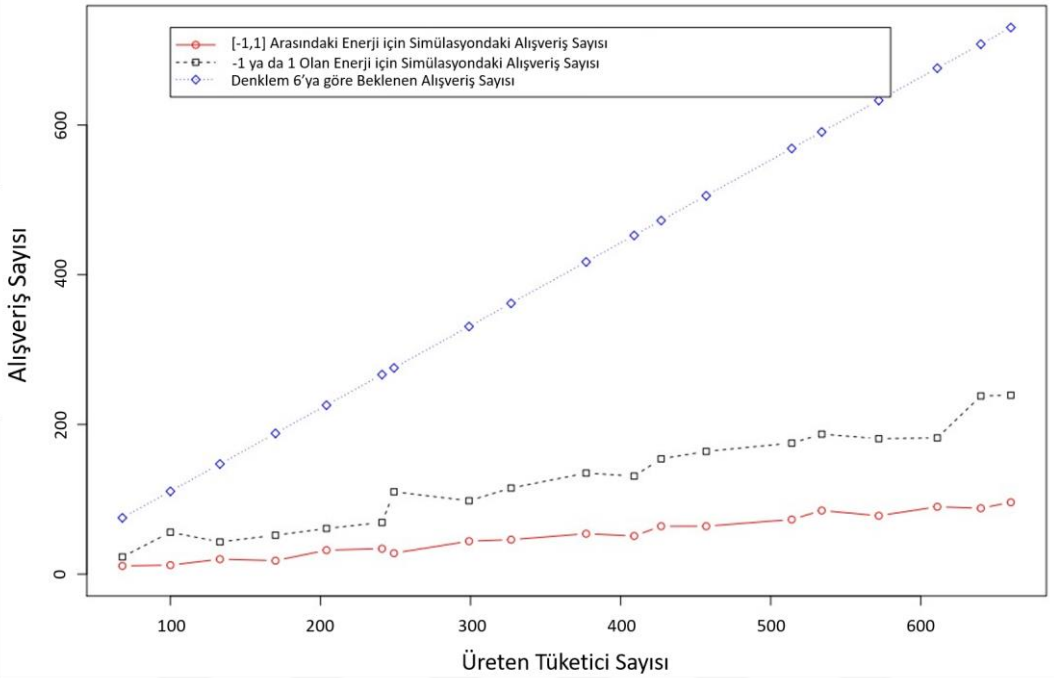
Enerji ticareti ve yönetim sistemleri için bir akıllı sözleşme mimarisi [53]'te sunulmuştur. Söz konusu araştırma, bir mikro şebeke içinde otonom olarak elektrik ticareti yapan Ethereum akıllı sözleşmelerine dayalı bir P2P enerji ticaret ağı kurmaktadır. Kang, Song ve ark. tarafından yapılan çalışmaya benzer bir yaklaşım mevcuttur. Dokuz aktörden oluşan sanal bir şebeke için simülasyon sonuçları da araştırma kapsamında sunulmaktadır. 2 adet şebekeye bağlı elektrikli araç, evleri temsil eden 2 adet yük, 1 adet fotovoltaik enerji kaynağı, 1 adet rüzgar enerjisi tesisi ve 2 büyük çaplı enerji santrali ile gerçekleştirilen simülasyonda 4 adet tüketici ve 4 adet üreten tüketici bulunmaktadır. Simülasyonun sonuçları, topluluk içinde P2P enerji ticaretinin yapıldığı bir günde, elektriğin %83,72'sinin aktörlerin teklif ettiği teklif aralığında karlı bir şekilde alınıp satıldığını göstermektedir. Önerilen akıllı sözleşme mimarisi, aynı anda 25 oyuncuyu destekleyebilirken, altı madenci düğümlü bir konfigürasyon için çalışma süresi 13 ile 19,25 saniye arasındadır. İncelenen bu makale, bir mikro şebekede yerel bir enerji piyasasında enerji ticaretini başarıyla gerçekleştiren çift müzayede piyasası mekanizmasına sahip bir akıllı sözleşme çözümü sunmaktadır.

Petri, Barati ve ark. tarafından yürütülen bir başka çalışma dağıtılmış enerji toplulukları için blokzincir tabanlı bir enerji ticareti ve paylaşımı incelemektedir [54]. Bir şebeke içinde P2P enerji ticareti için Ethereum tabanlı akıllı sözleşmeler kullanıldığından, daha önce incelenen makalelere benzer yaklaşımlar bu çalışmada da gözlemlenmiştir. Önerilen model, akıllı bir şebekede taraflar arasındaki enerji ticaretini tamamlamak ve kaydetmek için 3 orijinal akıllı sözleşme kullanmaktadır. Bu sözleşmeler "Enerji ticareti sözleşmesi", "Doğrulama sözleşmesi" ve "Okuma sözleşmesi" olarak adlandırılmıştır. Önerilen model, Solidity akıllı sözleşmeleri ile geliştirilmiş ve dağıtık modelleri test etmek için geliştirilmiş bir araç olan Remix üzerinde test edilmiştir. Bu çalışmanın sonuçları, blokzinciri teknolojisinin akıllı bir şebekedeki üretici tüketicilerin gelirlerini artırmak için etkin bir şekilde kullanılabileceğini ve değişmez bir işlem kaydı sağlayabileceğini göstermektedir. Makale ayrıca, önerilen modelin daha büyük ölçekli bir uygulaması için bir gaz ücreti deneyi sunar. Deneyin sonuçları, işlem başına akıllı sözleşmeleri çalıştırma maliyetinin şu etkenlere bağlı olarak arttığını göstermiştir:

- Artan ödeme seviyeleri
- Artan düğüm sayısı
- Mevcut enerji türlerinin azalması
- Artan işlem sayısı.

Blokzincir teknolojisine dayalı bir P2P enerji ticareti, madencilik maliyeti için bir simülasyon ile [55]'te değerlendirilmektedir. Makale, 50 ila 1000 üreten tüketici ile bir mikro şebekede gerçek zamanlı P2P enerji ticaretini destekleyebilen, İK tabanlı bir blokzincir çözümü için bir maliyet analizi sunmaktadır. Simülasyon sonuçları, hesaplama gücüne yatırım yapan bir madenciye verilen blok ödülünün madencilik maliyetinden daha yüksek olabileceğini göstermektedir ki bu da sistemin madenciler için pozitif bir gelirle işletilebileceği anlamına gelmektedir. Maliyet analizi, yüksek sistem verimine sahip akıllı bir sözleşme yapısı kullanarak, üreten tüketicilerin eşler arası enerji ticareti yaptıkları bir simülasyona dayanmaktadır. Artan sayıda tüketici için, elektrik ticaretinin kayıt altına alınması için gerekli işlem sayısı Şekil 3.5'te verilmektedir. Bu sonuçlar, İK tabanlı bir sistem için mikro şebekeye katkıda bulunan 600 üreten tüketici için işlem sayısının 200'ü geçebileceğini göstermektedir. Blok madenciliği için bir teşvik oluştururken yüksek

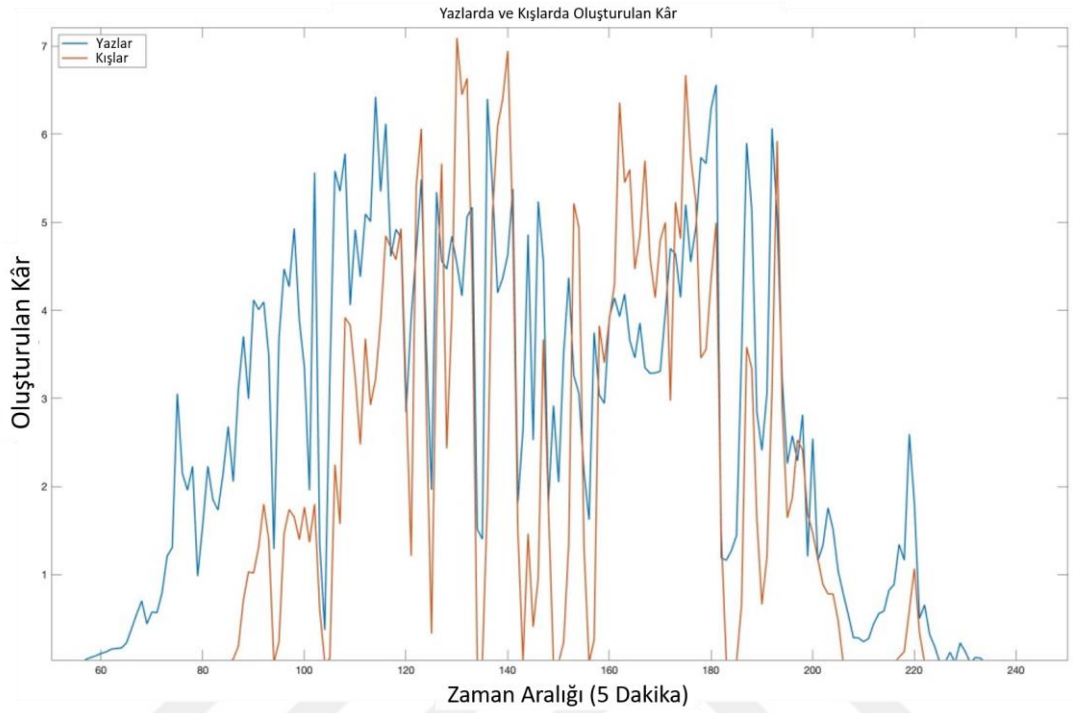
sayıda işlem gerçekleştirmenin İK kullanımı ile mümkün olduğu bu çalışma ile kanıtlanmıştır.




Şekil 3.5: P2P ticaretinde gereken işlem sayısını artırmak için ihtiyaç duyulan üreten tüketici sayısı [55].

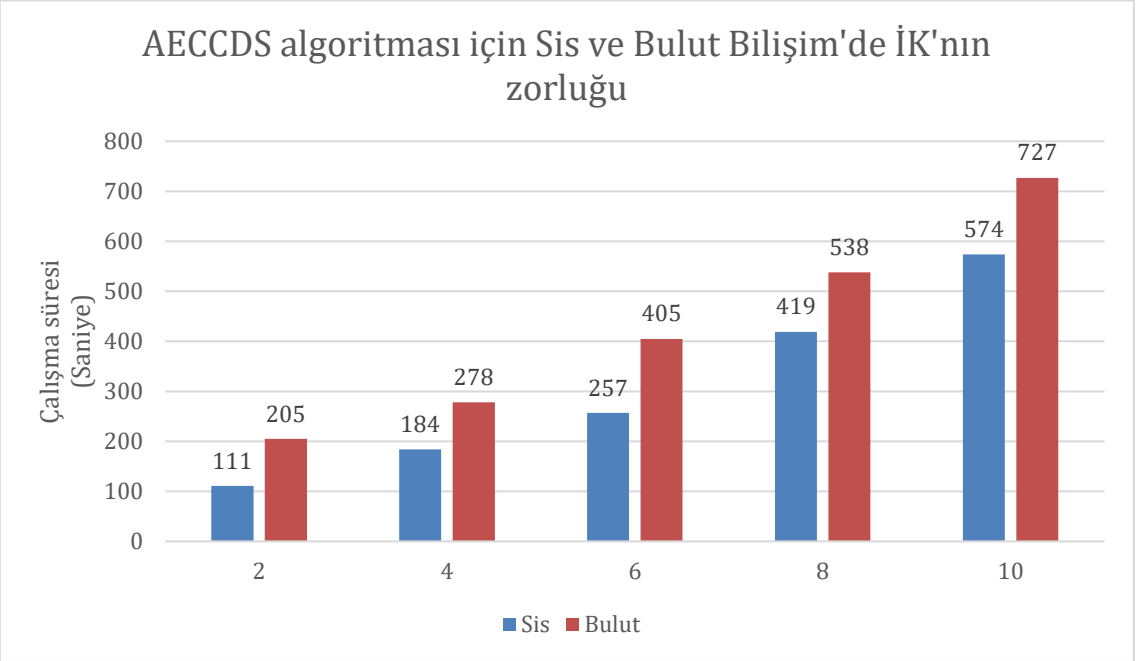
Malik, Duffy ve ark. tarafından yapılan daha güncel bir çalışma, bir mikro şebeke içinde elektrik ticareti yapmak için Ev Enerji Yönetim Sistemlerini (EEYS) kullanan bir P2P blokzinciri enerji ticaret sistemi sunmaktadır [56]. Önerilen sistem, blokzincir ve dağıtılmış veri depolama teknikleri ile birlikte enerji ticareti için çift müzayede yöntemini kullanmaktadır. EEYS sisteminin mikro şebeke aktörlerinin akıllı telefonlarına yüklenmesi planlanmış ve elektrik ticareti yapmak için toplayıcılar aracılığıyla blokzincir sistemi ile iletişim kurması öngörülmüştür. Önerilen modelin simülasyonu, 25 evde 100 kullanıcı ile kış ve yaz mevsimleri için ayrı ayrı ve 3kWp çatı fotovoltaik gücü ile gerçekleştirilmiştir. Makale, blokzincir teknolojisinin kişisel enerji kullanımını teşvik etmek için EEYS ile etkili bir şekilde kullanılabileceğini iddia etmektedir. Şekil 3.6, simülasyonda önerilen modelin yarattığı toplam geliri göstermektedir. Burada 24 saat boyunca ortalama 1175 Avro teşvik dağıtılmıştır. Bu sonuçlar, enerji ticareti yapmak için blokzinciri kullanmanın, bir mikro şebekedeki üreticiler veya tüketiciler için geliri etkili

bir şekilde artırabileceğini ve yenilenebilir enerji kaynakları için yatırım geri dönüş süresinin azaltılabileceğini göstermektedir.

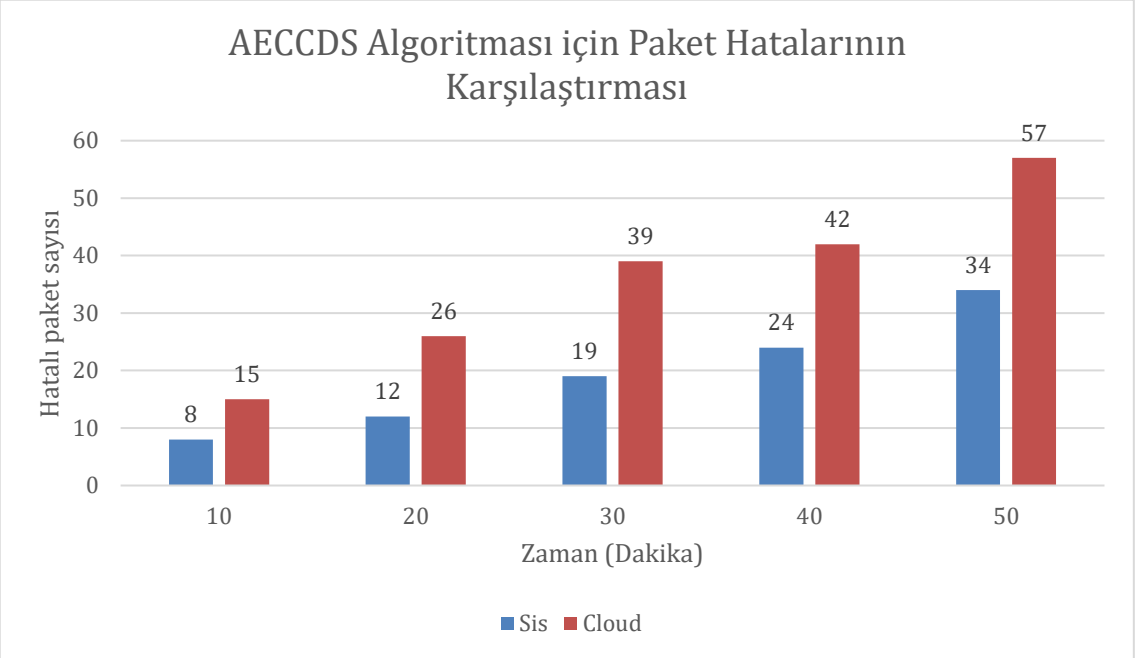



Şekil 3.6: MATLAB simülasyonunda yaz ve kış mevsimleri için blokzincir tabanlı ticaretin kullanılmasıyla elde edilen toplam kâr [56].

Aktarılan enerji verileri kötü niyetli aktörler için kıymetli olabileceğinden, akıllı bir şebekede akıllı sayaç iletişimleri için blokzinciri uygulamalarının güvenliği kritik öneme sahiptir. Shukla ve ark. enerji ticareti için bir blokzincir ağı üzerindeki akıllı sayaç iletişimleri için bir kriptografik şifreleme çözümü sunmaktadır [57]. Makale, akıllı sayaçlar ve bir blokzincirindeki ilgili taraflar arasındaki iletişimi güvence altına alan Sis Bilişim ortamında yeni bir Gelişmiş Eliptik Eğri Kriptografi Dijital İmza (AECCDS) algoritması sunmaktadır. Önerilen modelin, akıllı bir şebekeyle elektrik veri iletişimini güvenli hale getirdiği kanıtlanmıştır ve düğümlerin mahremiyetini korumak için etkili bir yöntem ortaya konulmuştur. Uzlaşma algoritması olarak İK kullanıldığında, güvenlik amaçlı Sis Bilişim ve Bulut Bilişim uygulamaları arasındaki bir karşılaştırma makalede verilmiş ve Şekil 3.7 ve Şekil 3.8'de gösterilmektedir. Sonuçlar, Sis Bilişiminin paket hataları ve çalışma süresi açısından Bulut Bilişimden daha etkili olduğunu göstermektedir.




Şekil 3.7: İK için değişen zorluklarla Sis ve Bulut Bilişim için çalışma süresinin karşılaştırılması [57].




Şekil 3.8: AECCDS algoritmasının Sis ve Bulut Bilişim uygulamaları için paket hata oranının karşılaştırılması [57].

P2P enerji ticareti için blokzincir teknolojisinin büyük ölçekli uygulamasının şebeke işletim performansı üzerindeki etkilerinin bir analizi [58]'de sunulmuştur. Yazarlar, blokzincir tabanlı ticaret sistemlerinin kullanımının etkilerini gözlemlemek için Avrupa'daki operasyonel bir şebekenin gerçek verilerini kullanmıştır. Makalede sunulan sonuçlar, bu tür bir sistemin kullanılmasının şebeke operasyonel performansı üzerinde çok az etkiye sahip olduğunu ve blokzincir teknolojisinin büyük ölçekli uygulamalarda kullanılabileceğini göstermektedir. Bir dağıtım ağı simülasyonu yapılmış ve sonuçlar Tablo 3.1'deki gibi oluşmuştur. Bu tablodaki sonuçlar, aktif güç kaybı, maksimum kompleks güç ve faz gerilimi dengesizlik oranında önemli bir değişiklik olmadan, net ihraç edilen enerjinin arttığını, reaktif gücün ise azaldığını göstermektedir. Bu nedenle, blokzinciri ile P2P enerji ticaretinin kullanılması, şebekenin operasyonel performansı üzerinde fazla bir etki olmaksızın Avrupa'daki mevcut Alçak Gerilim şebekelerinde uygulanabilir haldedir.

Tablo 3.1: Dağıtılmış şebeke simülasyon sonuçlarının özeti [58].

| Simülasyon Sonuçları [Birimler] | Temel Kılıf | P2P Kılıf | Fark |
|---|---|---|---|
| İhraç edilen net enerji [kWh] | 40.06 | 59.12 | +19.06 |
| İthal edilen reaktif güç [kVARh] | 41.07 | 34.85 | -6.22 |
| Maksimum karmaşık güç [kVA] | 148.73 | 149.32 | +0.59 |
| Aktif güç kayıpları [%] | 3.33 | 3.40 | +0.07 |
| Faz Voltajı Dengesizlik Oranı [%] | 8.866 | 8.865 | -0.001 |

Bu bölümde gözden geçirilen son makale Siano, Rolan ve Loia tarafından yazılmıştır ve yerel enerji piyasaları için geçişken enerji alışverişlerinin bir incelemesini ve değerlendirmesini sunmaktadır [59]. Makale, Enerji Kanıtı adlı yeni bir uzlaşma algoritması önermekte ve önerilen algoritmanın bir Sanal Güç Santrali ile uygulanmasına ilişkin bir tartışma sunmaktadır. İlgili makale, GridWise Architecture Council tarafından "Değeri temel bir operasyonel parametre olarak kullanarak tüm elektrik altyapısında dinamik arz ve talep dengesine izin veren bir ekonomik ve kontrol mekanizmaları sistemi" olarak tanımlanan geçişken enerji kavramını temel almaktadır. [60]. Bu makale, tüketici ile akıllı şebeke arasında bir iletişim arabirimi görevi gören bir Ev Enerji

Yöneticisi sunmakta ve bir akıllı sayaç, Ev Cihazı Ağ Geçidi, Geçişken kontrolör ve bir Enerji Yönetim Sisteminden oluşan Ev Enerji Yönetim Sistemi'ni (EEYS) ortaya koymaktadır. Bu EEYS sistemi, her eve kurulması gereken ek bir donanımdır ve geçişken enerji alışverişinin belkemiğidir. Makale, çift müzayede mekanizmasıyla enerji ticaretini otomatikleştiren akıllı sözleşme tabanlı bir dağıtık defter çözümü sunmaktadır. Önerilen model, aşağıdaki görevleri gerçekleştirmek için EEYS içindeki bir yazılımı kullanmaktadır:

1. Ortak MQTT kanalında ilan edildiğinde, alış ve satış tekliflerinin gönderilmesi ve alınması.
2. Düğümün gizliliğini korumak için Tüketim-Üretim Fonksiyonu (TÜF) değerini anonim olarak iletmek.
3. Uzlaşma protokolü, TÜF değerlerine dayalı olarak payların verildiği hisse değeri üzerine kuruludur.
4. Enerji işlemlerini saklamak için blokzinciri işlevlerini gerçekleştirilmesi
5. Dijital cüzdanların her an sorgulanabilir olması

Bahsedilen makale, HK'ya dayalı Enerji Kanıtı adı verilen ve bu makalenin bir sonraki bölümünde ve 4. Başlıkta detaylı olarak incelenen bir uzlaşma algoritması sunmaktadır.

### 3.2 Analiz

Alanla ilgili literatür taraması, blokzincir teknolojisinin yerel pazarlardaki enerji ticaretinde başvurulacak güvenilir bir çözüm olma potansiyeline sahip olduğunu göstermektedir. Bununla birlikte, literatür taraması, blokzincir teknolojisinin sağlamlık, güvenlik, mahremiyet, bilgisayar yatırımı, zamanlama, enerji verimliliği ve sürdürülebilirlik gibi birçok sorunla karşı karşıya olduğunu göstermektedir. Bu makale, teknolojinin ölçeklenebilirliğini geliştirmeye ve doğrulama sürecini aşırı miktarda enerji harcamadan çözmeye odaklanmaktadır. Sunulan literatür taraması, merkezi bir otorite içermeden blokların doğrulanmasını kolaylaştırabilecek uygun bir uzlaşma algoritması sağlamamaktadır. Önerilen model, İş Kanıtı ile ilgili enerji kayıplarını ve sistemin merkezi kontrol ihtiyacını önleyen bir uzlaşma algoritmasına odaklanmaktadır. Literatür taramasının analizinin sonuçları Tablo 3.2'de özetlenmiştir.

Enerji ticaretindeki ana sınırlamalar, merkezi bir sisteme kıyasla operasyonun maliyeti ve verimliliğidir. Blokzincir ticaret platformunun maliyeti ve verimliliği, çoğunlukla

uygulanacak piyasa mekanizmasının türü, uzlaşma algoritması, depolama ve gizlilik önlemlerinden etkilenmektedir. Doğrulama süresinin en aza indirilmesi, özel veya genel ağ arasında karar verilmesi, optimal piyasa sistemi seçimi ve saldırılara karşı önlem alınması, uygulamada iyileştirmenin anahtarıdır. Bir akıllı sayaca, İnternet bağlantısına, şebeke bağlantısına veya bir enerji depolama sistemine duyulan ihtiyaç, önerilen modellerden bazılarını çok özel mikro şebeke uygulamalarıyla sınırlandırmaktadır. Blokzincir tabanlı enerji ticareti kavramının bir sınırlaması olan İnternet erişimi ihtiyacı, enerji endüstrisinde kritik öneme sahip kırsal alanlara ulaşma zorunluluğu ile çelişmekte ve kapsam konusunda bu uygulamaları sınırlandırmaktadır. Ayrıca, blokzincir sisteminin donanım gereksinimleri, gerektiğinde blokları geri yüklemek için büyük bir depolama alanı gerektirmekte fakat birçok akıllı sayaç, yeterince büyük veri depolama kapasiteleri ile tasarlanmamaktadır. Bir P2P enerji ticareti blokzincirinin kullanımını sınırlayan fiziksel faktörlerin yanı sıra, blokzincirinin yönetimi, sistemin optimizasyonu için çok önemli olabilmekte ve değiştirilmesi fiziksel sınırlamalardan daha kolay olabilmektedir. Yönetim özellikleri için optimizasyon sorunu, güvenli ancak hızlı bir işlem ve doğrulama sağlamak için uzlaşma algoritmasının optimizasyonunu temel almalıdır. İncelenen makaleler zaman ve güvenlik açısından fark yaratan farklı uzlaşma yöntemlerine sahip modelleri içerdiğinden, bu yazıda güvenlik ve zaman sorunu ana odak noktalarından olacaktır. Bir uzlaşma algoritmasının seçimi, aynı zamanda özel veya genel bir blokzincir seçimi anlamına gelebilmektedir, bu nedenle büyük ölçekli uygulamalar için bu dikkate alınmalıdır.

Literatür incelemesinde önerilen modeller, miras aldıkları blokzincirinin uzlaşma algoritmalarını modifikasyonlarla veya klasik formlarında kullanmaktadır. Tablo 3.2, önceki bölümde incelenen makalelerde kullanılan uzlaşma algoritmalarını göstermektedir. Bu makaleler, bu noktadan itibaren tez çalışmasının devamında Tablo 3.2'de verilen makale numaralarıyla anılacaktır.

Tablo 3.2: İncelenen Makalelerde Kullanılan Uzlaşma Algoritmaları

| Makale No | Yazar | Uzlaşma Algoritması |
|---|---|---|
| 1 | Kang, Song, Pee, Jang | İş Kanıtı (→ Hisse Kanıtı) |

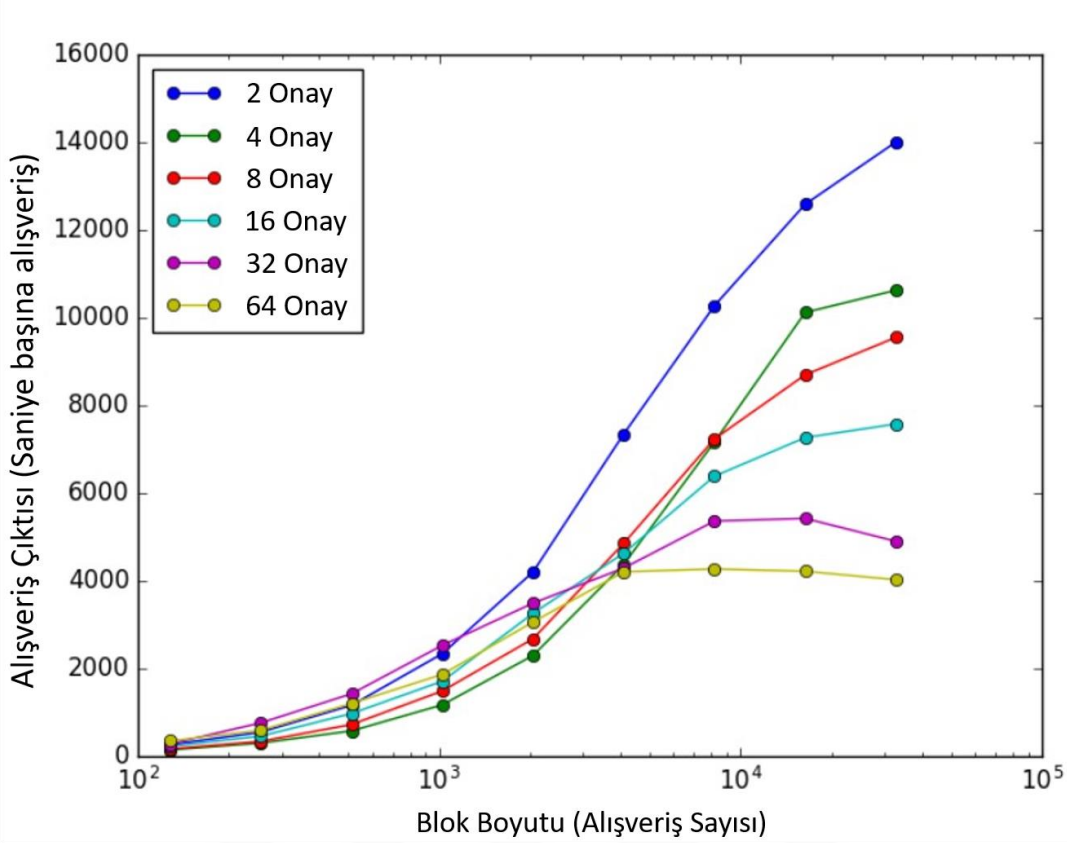
| | | |
|---|---|---|
| 2 | Li, Kang, Yu, Ye, Deng, Zhang | İş Kanıtı (Ayarlanmış) |
| 3 | Mengelkamp, Notheisen, Beer, Dauer, Weinhardt | Kimlik Kanıtı |
| 4 | Aytzhan, Svetinoviç | İş Kanıtı (Ayarlanmış) |
| 5 | Thakur, Breslin | İş Kanıtı (Ayarlanmış) |
| 6 | Thakur, Hayes, Breslin | İş Kanıtı (Ayarlanmış) |
| 7 | Energy Web Foundation | Yetki Kanıtı |
| 8 | Mengelkamp, Gärttner, Rock, Kessler, Orsini, Weinhardt | İş Kanıtı (→ Hisse Kanıtı) |
| 9 | Han, Zhang, Ping, Yan | İş Kanıtı (→ Hisse Kanıtı) |
| 10 | Thakur, Breslin | İş Kanıtı (→ Hisse Kanıtı) |
| 11 | Malik, Duffy, Thakur, Breslin | İş Kanıtı (→ Hisse Kanıtı) |
| 12 | Shukla, Thakur, Breslin | Tendermint BFT |
| 13 | Hayes, Thakur, Breslin | İş Kanıtı |
| 14 | Petri, Barati, Rezgui, Rana | İş Kanıtı (→ Hisse Kanıtı) |
| 15 | Siano, Rolan, Loia | Enerji Kanıtı |

İş Kanıtı algoritması, çeşitli nedenlerden dolayı incelenen makaleler arasında baskın uzlaşma algoritmasıdır. Bunun sebebi bu yöntemin veri değişmezliğindeki kanıtlanmış başarısıdır. Bitcoin üzerindeki çalışma kanıtı ile çıkarılan ve doğrulanan bloklar, ağın %51'ine hiçbir aktör sahip olmadığı sürece verilerin çok güvenli şekilde saklanabildiğini kanıtlamaktadır. Birinci makalenin önerilen modeli, Ethereum'dan devralınan İK'yı kullanmaktadır, bu nedenle Ethereum, Hisse Kanıtı modeline geçme planını tamamladığından bugün uygulandığında algoritma değişecektir. İkinci makale, tanıtılan dağıtık defter sisteminin özel ihtiyaçlarına göre ayarlanmış bir İş Kanıtı kullanmaktadır. Burada doğrulama yalnızca ödül kazanmak için hesaplama gücüne yatırım yapmaya istekli Enerji Toplayıcıları tarafından yapılır, bu nedenle ET'lerin katılımına uyacak şekilde değiştirilmiş bir İş Kanıtı kullanılmıştır. Özet fonksiyonu bulmacasının karmaşıklığı, yazarlar tarafından bir mikro şebekedeki ET'lerin işlem süresine ve güvenlik gereksinimlerine uyacak şekilde ayarlanmıştır. Üçüncü ve yedinci makaleler,

Kimlik Kanıtı veya Yetki Kanıtı adı verilen benzer bir uzlaşma algoritması kullanmaktadır. Bu uzlaşma yöntemi, yalnızca düğümlerin gerçek hayattaki kimliklerinin otorite tarafından bilindiği özel blokzincirleri için geçerlidir. Doğrulama için zaman ve hesaplama gücü harcamak yerine, doğrulayıcının itibarına göre bir yetki seçimi yapılmaktadır. Bu yöntem, kullanımı yalnızca özel ağa sahip zincirler için sınırlandırırken doğrulamayı çok daha basit ve hızlı hale getirmektedir. 4, 5 ve 6 numaralı makaleler, özet fonksiyonu bulmacasında küçük farklılıklar yaratan ayarlamalarla benzer İş Kanıtı algoritmaları kullanmaktadır. 4. Makale, daha basit bir İş Kanıtı ile aynı miktarda veri değişmezliğini sağlamanın yollarını derinlemesine incelemiş ve farklı özet algoritmaları kullanmanın etkilerini analiz etmiştir. Bulmaca karmaşıklığının değiştirilmesi, 4., 5. makalelerdeki modellerde bir ayarlama olarak verilmiştir; her ikisi de özel ağa sahip blokzincirlerdir. 8. Makalede bahsedilen Brooklyn Microgrid projesi, LO3 Energy'ye ait TransActive Grid'in Ethereum tabanlı blokzincir uygulamasını kullanmaktadır. Ethereum ağı, bu makalenin yayınlanma tarihinde ana zincirin uzlaşma algoritması olarak İK'a sahipti, ancak daha iyi enerji verimliliği ve ölçeklenebilirlik için 2022'de HK olarak değiştirildi [17].

9. ve 10. makalelerde sunulan çalışmaların her ikisi de Ethereum blokzincir akıllı sözleşmelerinin bir uygulamasını kullanmaktadır. Bu nedenle, bu çalışmaların yayın tarihinde kullanılan uzlaşma algoritması İK idi. Yazarlar önerilen modellerin enerji verimliliğine odaklanmadığından, her iki makale de standart Ethereum ana zincir dağıtılmış uygulamalarıyla KİG yapısında bir blokzinciri mimarisi sunmuştur. Hem 9. hem de 10. makaleler, güvenilir bir işlem defteri elde etmeye çalışırken, hesaplama açısından çok ağır bir uzlaşma yöntemine dayanmaktadır. Makaleler aynı hedeflere ulaşmak için 15 Eylül 2022'den sonra yayınlanmış olsaydı, Ethereum'un HK uyarlaması ile uygulamaları çok daha enerji verimli olacaktır. 9 numaralı makalede sunulan çalışma, daha iyi bir blokzinciri yönetişimi sağlamak için diğer birkaç ilgili çalışma ile birleştirilirse, verimli bir blokzinciri tabanlı P2P enerji ticaret platformu oluşturmak için kullanılabilecektir. Bu uygulama ve olası gelişmeler hakkında daha fazla bilgi ilerleyen bölümde bulunabilir.

11. Makale, önerilen blokzincir sisteminde kullanılan uzlaşma yönteminden özel olarak bahsetmez, ancak çalışma, akıllı sözleşmelerin kullanımından bahsetmektedir. Yazarların önceki çalışmaları, Ethereum blokzincirinin simülasyon ortamı için akıllı sözleşmelerin geliştirilmesi için kullanıldığını göstermektedir. Bu makale, Ethereum'un birleşmesinden önce yayınlanmıştır, bu nedenle simülasyon, ana uzlaşma yöntemi olarak İK'yı kullanmaktadır. Yazar, 9. ve 10. makalelere benzer şekilde, uzlaşma sürecinde kullanılan aşırı miktarda enerjiden bahsetmemiştir ve HK gibi daha az enerji tüketen bir protokole geçiş ile birlikte buradaki çalışmalar geliştirebilecektir. 12. Makale, Cosmos ağından uyarlanan akıllı sözleşmeleri kullanmaktadır. Cosmos, Tendermint [61] adlı başka bir blokzinciri uygulamasından uyarlanan Bizans Hata Toleransı adlı bir uzlaşma algoritması kullanmaktadır. Tendermint BFT algoritması, Dwork, Lynch ve Stockmeyer tarafından ortaya atılan DLS algoritmasından türetilmiştir ve kısmen senkronize bir BFT protokolüdür. Tendermint BFT uzlaşma algoritması, sabit ve bilinen bir doğrulayıcı grubuyla çalışmaktadır. Her blok, her doğrulayıcı düğümün bir blok için oy kullandığı sıralı turlarda birer birer doğrulanmaktadır. Bu uzlaşma mekanizmasının çalışma prensibinin detayları Cosmos Teknik İncelemesinde [61] mevcuttur. Tendermint BFT, bir blokzinciri ağındaki işlemler için yüksek güvenlik ve verim sağlamakta, ancak enerji ticareti için BİG yapıdaki blokzinciri uygulamaları için uygun olmayan sabit miktarda bilinen doğrulayıcı gerektirmektedir. 5 farklı kıtadaki 64 düğüm için Tendermint BFT'nin performansı Şekil 3.9'daki grafikte gösterilmektedir.




Şekil 3.9: Tendermint BFT'nin 5 farklı kıtada bulunan 64 düğüm için sergilenen performans [61].

Makale 12'nin simülasyonunda kullanılan uzlaşma algoritması İş Kanıtı'dır ve ağda 200 düğüm ve 40 madenci vardır. Bu çalışmanın ana amacı gerçek hayattaki bir şebeke için ağın operasyonel performansı üzerindeki etkileri bir simülasyon ile değerlendirmek olduğundan İK zincirinin kullanımı kabul edilebilirdir. Ancak, İK kullanımının getirdiği ekstra enerji tüketimi bu makalede de sunulmamaktadır. Benzer bir durum, Ethereum akıllı sözleşmelerinin uygulandığı 14 numaralı maddede görülmektedir. 14. makalenin uzlaşma algoritması da İK'dır, ancak yazarlar hesaplama açısından ağır protokol tarafından çıkarılan ek maliyetlerden bahsetmemiştir. İK nedeniyle oluşan ekstra maliyetler, karbon emisyonları ve elektrik tüketimi dikkate alınırsa, gerçek hayattaki şebekeler için bu tür bir uzlaşmanın kullanılması, küresel ısınma üzerinde büyük bir etkiye neden olacaktır.

15 numaralı makale, P2P enerji ticareti amacıyla geliştirilmiş tek yeni uzlaşma algoritmasını sunmaktadır. Önerilen Enerji Kanıtı uzlaşması, hisse alma mekanizmasında yapılan değişikliklerle birlikte HK uzlaşmasına dayanmaktadır. Enerji Kanıtı, bir pay

değeri oluşturmak için bağlı kullanıcıların elektrik üretimlerini ve tüketimlerini kullanarak HK protokolünü basitleştirmektedir. Doğrulayıcı olmak için para veya kripto para birimleri yerine, kullanıcıların yenilenebilir enerji kaynaklarına yatırım yapması ve elektrik üretmesi beklenmektedir. 15. makalede sunulan Tüketim-Üretim Fonksiyonu, kullanıcının kendi kendine yeterliliğine dayalı olarak ilgili düğüm için hisse değerini hesaplamak için kullanılmaktadır. Daha fazla kendi kendine yeten bir kullanıcı, HK protokolündeki pay miktarına benzer şekilde, doğrulayıcı olmaya daha yatkındır. Sunulan yöntem, önerilen P2P enerji ticareti sisteminin kullanımıyla HK uygulamasını basitleştirir. Önerilen uzlaşma algoritması, soruna gerçekten yeni bir yaklaşım getirmektedir ve İK ile ilgili enerji verimliliği sorunlarını başarıyla çözebilecek kapasitededir. Fakat 15. makalede sunulan modelle ilgili birkaç sorun mevcuttur. İlk sorun, blokzinciri yalnızca izin verilen varlıklarla sınırlandığından, özel ağa sahip bir blokzinciri türünün seçimidir. Bu kısıtlama, blokzinciri ekosistemine izinleri kontrol edecek bir yetkili ihtiyacı gerektirmekte ve piyasanın merkezileşmesine neden olduğu gibi operatörlere de ekstra bir yük getirmektedir. Bu modelde otorite, düğümlerin blokzincirine girmesini önlemek için kendi adına hareket edebilecek kapasitededir veya otorite, kötü amaçlı düğümleri doğrulayarak sistemin kontrolünü ele geçirmek isteyen saldırganlar tarafından yapılacak saldırılara açıktır. Sunulan modelle ilgili diğer bir sorun, EEYS'deki donanım kötü niyetli aktörler tarafından imzaları kopyalamak için hacklenebileceğinden, EEYS'lerin kimlik doğrulaması için dijital imzalarla kullanılmasıdır. EEYS internete bağlı olduğundan ve imza verilerini açık olarak gönderdiğinden, imzalar hareket halindeyken bilgisayar korsanları tarafından da ele edilebilecektir. Bu imzalar, kötü niyetli aktörler tarafından kötü niyetli veriler göndermek için tekrarlama (replay) saldırıları için kullanılabilecektir. Sunulan bu modeldeki farklı bir problem de EEYS donanımı üzerinde Tüketim-Üretim Fonksiyonunun hesaplanmasıdır. Bu işlevi uygulayan yazılım, sahte girdilerle beslenebilir veya kötü niyetli bir kullanıcı tarafından en yüksek değerle sonuçlanacak şekilde ayarlama yapılabilir. Bu, TÜF'ın geçersiz girdilerle beslenmemesini veya sonucunun değiştirilmemesini sağlamak için ayrı bir güvenlik önlemine ihtiyaç doğurmaktadır. Bu olası sorunların dışında, makale, düğümlerin gizliliğini korumakta ve incelenen makaleler arasında enerji verimliliği için en iyi çözümü sunmaktadır.

İş Kanıtı kullanımındaki en önemli sorun enerji tüketimi ve boşa harcanan hesaplama gücüdür. 2.3. bölümde de ayrıntılı olarak tartışıldığı gibi, İK'nın güç tüketimi, ölçeklenebilirlik açısında muazzam bir zorluktur. Ayrıca doğrulama sürecinde harcanan süre İK için çok uzundur ve anlık enerji ticaretini, sistemin doğrulama için harcadığı bekleme süresiyle sınırlandırmaktadır. Ayrıca, İK kullanan sistemler için saniye başına işlem sayısı nispeten daha düşüktür ve gerçekte yerel enerji piyasalarında meydana gelen büyük miktarda işlemle baş edemeyecektir. İK'nın en yaygın kullanılan alternatifi, ödül üretimi için avantaj elde etmek için bir miktar kripto paranın diğerinde hisse alınan Hisse Kanıtı'dır(HK). HK protokolü, verileri çok daha hızlı işlemekte ve uzlaşmaya varmak için daha düşük bir süre gerektirmektedir. Böylece, ihtiyaç duyulan işlem hızı ve doğrulamalar için bekleme süresi sorununu çözebilmektedir. Bununla birlikte, HK uzlaşmayı riske atan Nothing-at-stake sorununa sahiptir ve bazı uygulamalarda zengin daha zengin olur modeline neden olabilmektedir. Elektrik üretiminin büyük bir kısmı, daha iyi bir piyasaya katılım karşılığında daha fazla yatırım yapmak istemeyen evler ve tarlalar gibi küçük ölçekli katılımcılara dayandığından, enerjide yerelleşme, uzlaşma açısından daha demokratik bir çözüm gerektirmektedir. Kripto parayı hisse almak üzere yatırmak, yenilenebilir enerji için kaçırılmış bir yatırıma eşdeğer olacaktır ve bu, aynı zamanda üretilen elektriğin tüketicisi olduğu için sahibine uzun vadede daha fazla zarar getirecektir.

Bir sonraki çözüm, enerji ticareti piyasaları için Yetki Kanıtı veya Kimlik Kanıtıdır. Kimlik kanıtı, düğümlerin tümünün planlanmış bir süreç tarafından seçildiği ve düğümlerin gizliliğinin azaltıldığı özel bir blokzinciri gerektirmektedir. Blokzincir sistemine kimlik getirme fikri, anonim şekilde varlık ticareti sunan Bitcoin tarafından ortaya atılan blokzincir sisteminin temel ilkelerine doğrudan karşı çıkmaktadır. Energy Web Chain tarafından yazılmış gözden geçirilen makale, zincirin halka açık olduğunu ancak kötü niyetli saldırıları önlemek için temel tarafından kimlik tanıma gerektiren bir izin sistemine sahip olduğunu önermektedir. Kimlik Kanıtı kullanımı, uzlaşmaya İK'dan en az 2 kat daha hızlı ulaşan bir yöntem sağlar, ancak kullanıcı düğümlerinin mahremiyetini ortadan kaldırmaktadır ve klasik elektrik piyasalarındaki hükümet gibi hareket eden bir otorite ile sürekli iletişim gerektirmektedir. Büyük bir arazi üzerinde çok küçük nüfusa sahip kırsal bölgeler veya küçük alanlara sahip çok kalabalık şehirler gibi aşırı nüfus yoğunluğuna sahip alanlarda mikro şebekenin kullanımı, yetkiye dayalı bir

doğrulamanın eklenmesiyle oldukça sınırlı hale gelecektir. Ayrıca Kimlik Kanıtı kullanımı, kötü amaçlı düğümler var olduğunda blokzincirindeki işlem verilerinin tutarlılığını bozabilmektedir. Bu nedenle, kimliğe dayalı bir algoritma kullanmak, bir mikro şebeke ticaret platformunun gelecekte amaçlanan kullanımı için ölçeklenebilir değildir. İncelenen P2P enerji ticaret platformları için uzlaşma mekanizmalarında belirtilen sorunları çözmek için, bir sonraki bölümde yeni bir uzlaşma algoritmasına sahip yeni bir enerji ticaret sistemi modeli önerilmiştir.

# 4. ÖNERİLEN MODEL

Önerilen model, P2P blokzinciri tabanlı bir enerji ticareti sisteminin geliştirilmesi için beş önemli kavrama odaklanmaktadır:

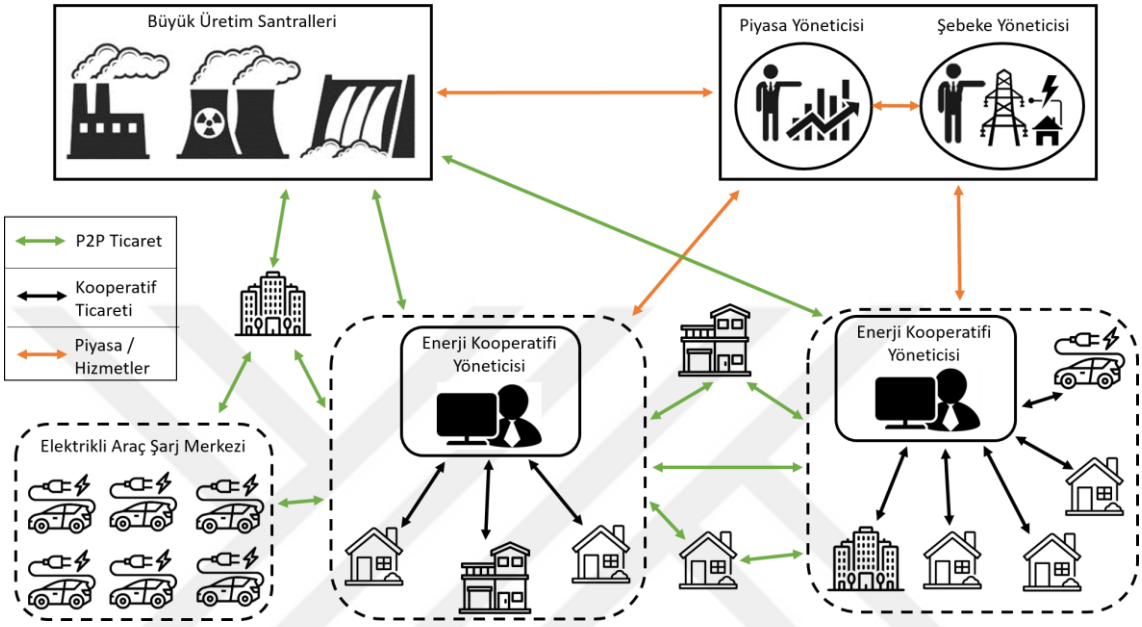
1. Enerji verimliliği
2. İşlem veri bütünlüğü
3. Elektrik tüketicilerinin/üreticilerinin mahremiyeti
4. İşlem verilerinin güvenliği
5. Onay hızı

Model, piyasa altyapısı, donanım çözümü, akıllı sözleşmeler ve uzlaşma algoritması ile aşağıdaki dört bölümde açıklanmaktadır.

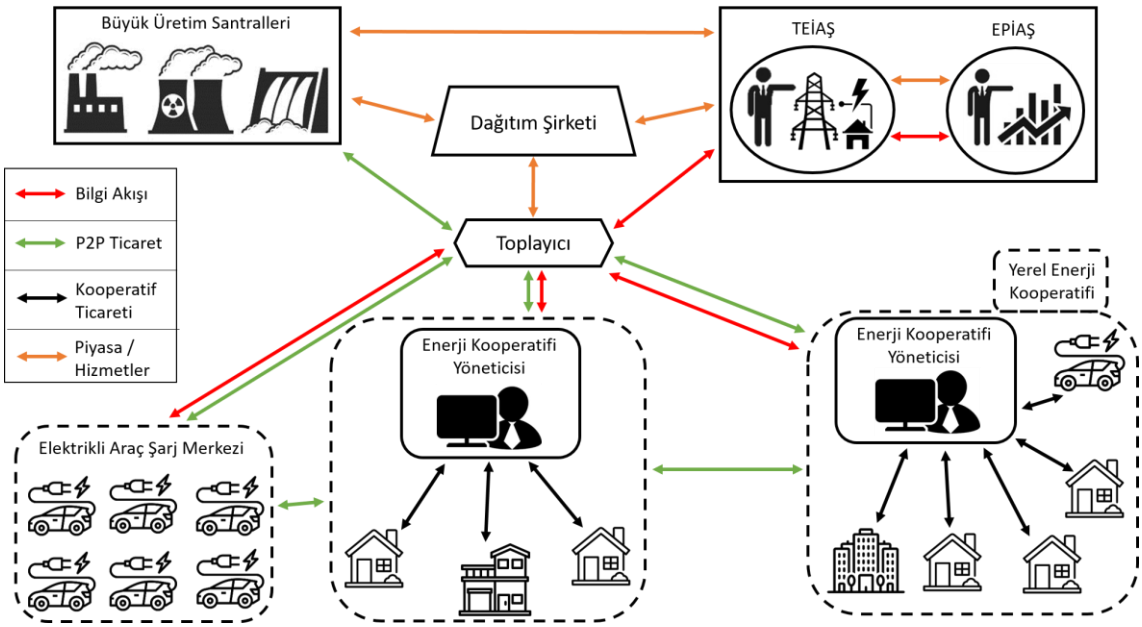
## 4.1 Enerji Piyasası Altyapısı

Liu ve Li tarafından yürütülen çalışma, blokzincir tabanlı bir çözümle enerji ticaretinin kullanıcıların mahremiyetini daha iyi koruduğunu ve yönetici tabanlı pazarlara kıyasla P2P tabanlı pazar tasarımları için daha esnek olduğunu göstermektedir [43]. Bu nedenle burada önerilen model için bir P2P enerji ticareti piyasası tasarımı uygulanmaktadır. Enerji piyasası altyapısı, sistemin çalışması için gerekli olan kabul edilebilir bir kendi kendine yeterlilik seviyesine sahip olmak için elzem olan yeterli üreten tüketiciye sahip akıllı mikro şebekelere dayanmaktadır. Tamamen P2P özelliğine sahip pazar tasarımları, artan sayıda pazar katılımcısıyla ölçeklenebilirlik sorunlarından mustarip olmaktadır, bu nedenle en iyi yaklaşım, topluluk temelli pazarların da dâhil olduğu hibrit bir piyasa yapısı olacaktır [41]. Hibrit piyasa yapısı, birçok talepkar üyenin sisteme dâhil edilmesi için daha ölçeklenebilir bir tasarım sağlamak üzere yerel enerji kooperatiflerinden ve P2P ticaret düğümlerinden oluşmaktadır. Önerilen pazar altyapısı Şekil 4.1'de gösterilmiştir. Bu modelde topluluk yöneticileri, yerel enerji topluluğu içindeki enerji ticaretinden sorumludur. Önerilen modelin ölçeklenebilirliğini artırmak için mevcut başka bir yerel topluluk içinde ayrıca bir yerel enerji topluluğu kurulabilmektedir. Piyasa ve şebeke işletmecileri, yalnızca şebeke veya piyasa operasyonlarını gerçekleştirmekte ve daha büyük aktörlerle ilgili iletişimi kurmak ve çeşitli şebeke hizmetlerinden sorumludur. Piyasa modeli aynı zamanda Türkiye elektrik piyasasının mevcut yapısına, düzenlemelere göre hâlihazırda yasal olan aktörleri dahil edecek şekilde uyarlanmıştır. Piyasa modelinin bu şekilde düzenlenmiş bir hali Şekil 4.2'de gösterilmektedir. Bu modelde, yakın zamanda yasallaştırılan toplayıcılar [62], dengeleyici güçleri ile enerji ticaretine katkıda bulunmak

için piyasa topolojisine eklenmiştir. Ayrıca toplayıcılar, blokzincir tabanlı enerji ticareti uygulamasının işletilmesinden sorumlu olacaktır. Üreten tüketiciler, tüketiciler ve enerji topluluğu yöneticileri, enerjilerini dengelemek ve elektrik ticareti yapmak için akıllı sözleşmeler yürütmek üzere toplayıcıyla sürekli iletişim halindedir.

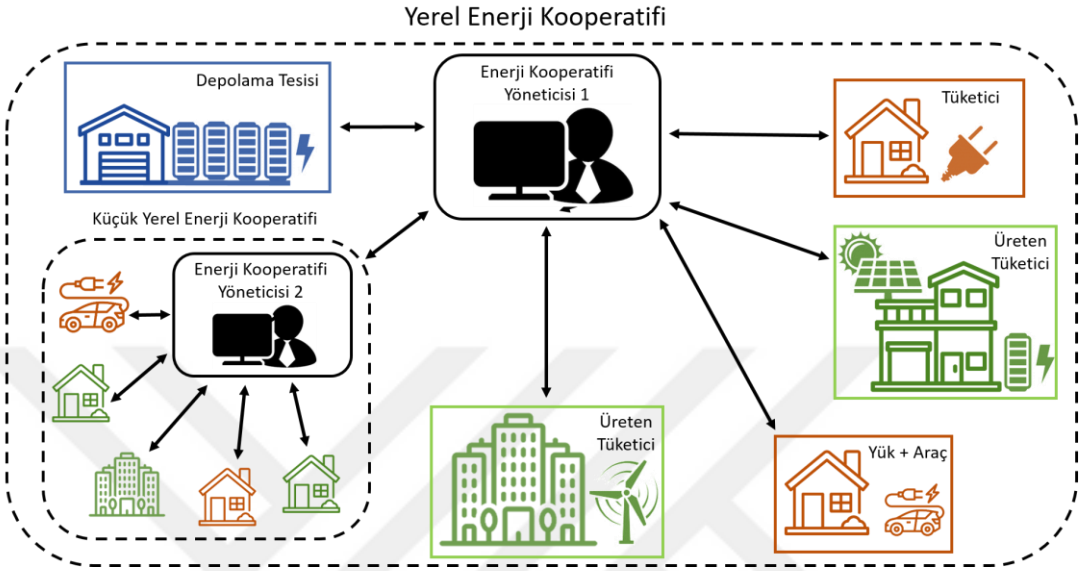



Şekil 4.1: Önerilen modelin piyasa yapısı.




Şekil 4.2: Türkiye elektrik piyasasındaki yasal düzenlemelere uyacak şekilde uyarlanmış piyasa yapısı.

Piyasalar ile ilgili önceki şekillerde sunulan enerji topluluğuna daha yakından bir bakış, Şekil 4.3'te gösterilmektedir. Yerel enerji topluluğu; üreten tüketiciler, tüketiciler, elektrikli araçlar, depolama hizmetleri ve enerji topluluğu yöneticisinden oluşmaktadır.




Şekil 4.3: Yerel enerji topluluğu yapısına daha yakından bir bakış.

## 4.2 Enerji Yönetimi Donanım Çözümü

Önerilen model, üretici ve tüketici düğümlerinin ölçüm altyapısına kurulacak bir donanımdan yararlanmaktadır. Donanımın, blokzincir teknolojisine dayalı bir P2P enerji ticaret modelinin ihtiyaçlarını karşılamak için 8 temel gereksinimi vardır. Bu gereksinimler şunlardır:

1. Toplayıcının enerji yönetimi sunucusuna bağlanmak için bir arayüz.
2. Akıllı sayaç ile iletişim kurmak için bir arayüz.
3. Akıllı sayaç verilerinin toplanması, protokol dönüşümleri, uzlaşma yöntemine göre verilerin işlenmesi, verilerin şifrelenmesi/şifresinin çözülmesi ve ağ arayüzlerine yönlendirme için yeterli bilgi işlem gücü.
4. Şifreleme anahtarları için güvenli bir depolama.
5. Akıllı sayaca bağlı yükleri kontrol edebilme, elektrik tüketen yükleri akıllı şebekeye bağlı ana güç hattından ayırabilme veya yeniden bağlayabilme yeteneği.
6. Enerji yönetimi yazılımını çalıştırmak için yeterli RAM.
7. Senkronizasyon için gerçek zamanlı bir saat.

8. Düşük güç tüketimi.

Belirtilen donanım gereksinimleri, piyasadan temin edilebilecek birçok farklı hazır donanımın birleştirilmesiyle oluşturulacak yapılandırmalar ile sağlanabilir ancak bu tür bir proje için özel bir donanımın geliştirilmesi gerçek kullanım senaryolarında çok daha ölçeklenebilir olacaktır. Verilen 8 temel donanım gereksinimini karşılayabilecek yöntemler veya çözümler sırasıyla aşağıdaki gibidir:

1. Bu arayüz Wi-Fi, Ethernet, fiber optik, 4G Hücresel, 5G Hücresel veya LoRaWAN teknolojisi olabilecektir. LoRaWAN teknolojisi, düşük güçlü IoT cihazlarıyla uzun menzilli iletişim sunmaktadır, ancak iletişim için gereken hız ve güvenilirlikten yoksundur. Teklif verme ve sunma sürecinde gönderilmesi gereken küçük boyutlu paketlerle düşünüldüğünde, fiber optik veya 5G Hücresel gibi yüksek hızlara sahip bir çözüm fazlasıyla pahalı olacaktır. En ucuz ve en sağlam çözüm, enerji yönetim sistemine ulaşmak için İnternete bağlanan donanıma yapılacak bir Ethernet bağlantısı olacaktır. İnternet bağlantı yönlendiricisi elektrik ölçüm kutusundan uzakta olmadığında Wi-Fi da kullanılabilir.
2. Bu arabirim kablolu veya kablosuz olabilir. Kablolu çözüm seçenekleri Ethernet, PLC veya M-Bus'tır. Kablosuz çözüm, Kablosuz M-Bus, Wi-Fi, LoRaWAN, MIOTY veya Zigbee [63] şeklinde olabilecektir. Akıllı sayaçların ölçüm ağ geçitleriyle iletişimi için özel olarak geliştirilen Avrupa standardı M-Bus'tur. Donanım için bu standardın benimsenmesi, herhangi bir yasal kaygı olmaksızın sistemin entegrasyonunu kolaylaştıracaktır. Diğer çözümler de nispeten ucuz ve uygulanması kolaydır, ancak piyasada önerilen donanıma bir modül olarak entegre edilmek üzere kablosuz veya kablolu M-Bus cihazları bulunabilmektedir.
3. İlgili bir minimum donanım gereksinimi, Bölüm 3'te incelenen önceki çalışmalardan çıkarılabilmektedir. Son teknoloji çalışmalarda bildirilen gerçek hayattaki kullanım durumları, uç düğümler için çok az bilgi işlem gücünün gerekli olduğunu göstermektedir. Bir Raspberry Pi Model 4, enerji yönetimi donanımı için ana işlem birimi olarak kullanılabilecektir [59]. Sistemin şifreleme/şifre çözme hızını artırmak için AES-NI'yi destekleyen bir CPU seçilebilir. Kriptografik hesaplamaların hızını daha da yükseltmek için Intel'in QuickAssist teknolojisine sahip bir CPU seçilebilir [64]. Bu daha yüksek performanslı CPU'lar, örneğin toplayıcının olduğu uçtaki birçok eşzamanlı bağlantıya sahip

düğümler için seçilebilir, ancak AES-NI desteğine sahip herhangi bir CPU, üreten tüketici tarafı için yeterli olacaktır.

4. Kriptografik anahtarların güvenli bir şekilde saklanması için modern bir TPM kullanılmalıdır. TPM'ler, son kullanıcıların özel anahtarları için yeterli miktarda güvenlik sağlamaktadır. Toplanan akıllı sayaç verileri için güvenli depolama, daha yüksek depolama kapasiteli geçici bir bellek kullanılarak genişletilebilecektir.
5. Elektrik yüklerinin bağlantısını kesmek ve yeniden bağlamak için enerji yönetim sistemi içerisinde elektrik devre kesicileri ve ilgili kontrol modülleri bulunmalıdır. Toplayıcı tarafından yapılan talep tarafı yönetimi talepleri, elektrik yükünü azaltmak veya artırmak için kontrolörler tarafından gerçekleştirilebilmelidir. Bu gereksinim, evdeki belirli yüklerin bağlantısını yönetebilen gelişmiş akıllı sayaçların kullanılmasıyla karşılanacaktır.
6. Bölüm 3'te incelenen önceki çalışmadan ilgili bir minimum donanım gereksinimi çıkarılmıştır. 3 numaralı gereksinim için seçilen donanım 2, 4 ve 6 gigabayt RAM seçeneklerine sahiptir. Raspberry Pi'nin 2 gigabaytlık bir sürümü, enerji yönetimi yazılımı için hesaplama gereksinimleri oldukça düşük olduğundan, belirli sayıdaki işlemler için yeterli bellek sağlayacaktır.
7. İşlemlerin zamanını doğru bir şekilde damgalamak için Ağ Zaman Protokolü sunucu bağlantısına sahip gerçek zamanlı bir saat modülü gereklidir. Donanıma harici olarak DS3231 gibi basit bir RTC modülü eklenerek bu ister karşılanabilecektir. Toplayıcı sunucularına ulaşmak için kurulacak İnternet bağlantısı, bir Ağ Zaman Protokolü sunucusu üzerinden saat senkronizasyonu için de kullanılabilmelidir.
8. Sistemin enerji açısından verimli olması için donanımın toplam elektrik tüketiminin düşük olması gereklidir. Diğer gereksinimler için önerilen Raspberry Pi donanımı da bunu karşılamaktadır çünkü bu tek kartlı bilgisayar yoğun CPU kullanımında dahi yalnızca 6W güç tüketmektedir [65].

Enerji yönetimi donanımı için seçilen çözümler Tablo 4.1'de özetlenmiştir. Önerilen modelin ana donanımı olacak olan tüketici tarafı için, ek modüller içeren bir Raspberry Pi Model 4 ile gereksinimler rahatlıkla karşılanmaktadır. Toplayıcı taraf için donanım gereksinimleri daha zorludur, bu nedenle Intel CPU'lu bir sunucu uygun olacaktır ve

gelecekteki bir çalışma olarak, bu ihtiyaçlar için özel bir donanım tasarlanması söz konusudur.

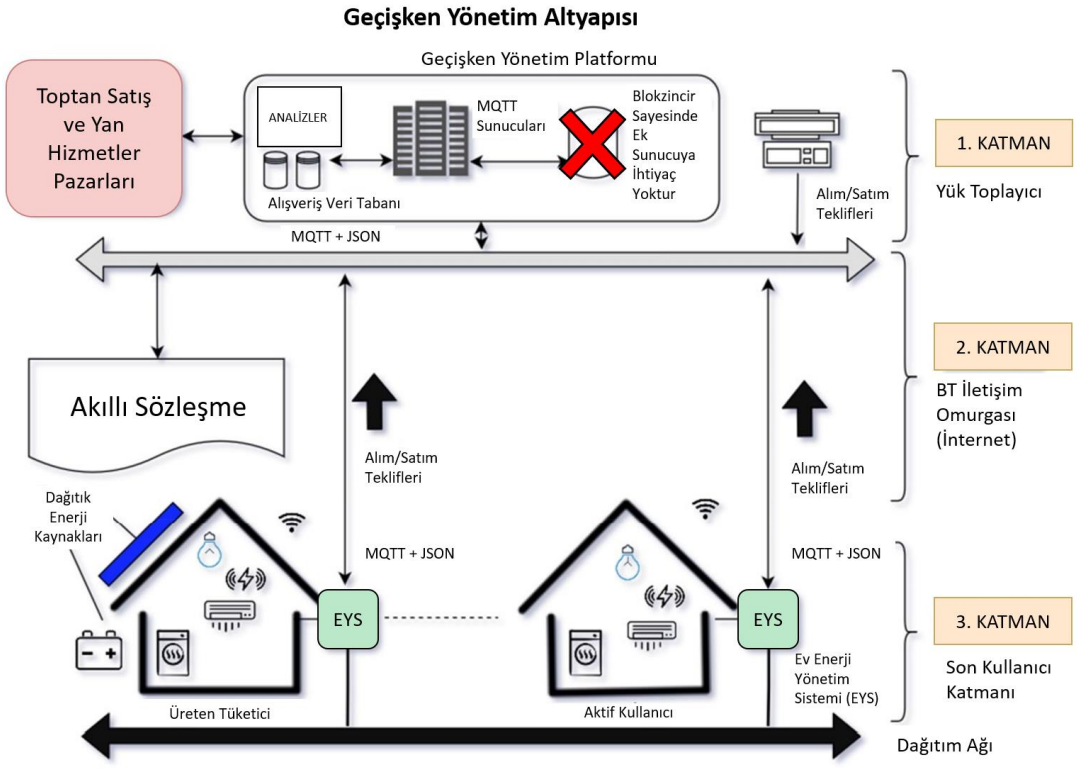
Tablo 4.1: 8 temel gereksinim için seçilen enerji yönetimi donanım çözümlerinin özeti.

| Gereksinim No. | Seçilmiş Çözüm |
|---|---|
| 1 | İnternete bir Ethernet veya Wi-Fi bağlantısı |
| 2 | Akıllı sayaç ile M-Bus bağlantısı |
| 3 | Raspberry Pi 4 (Son kullanıcı) / Intel QuickAssist özellikli CPU (Toplayıcı) |
| 4 | TPM - Güvenilir Platform Modülü |
| 5 | Gelişmiş akıllı sayaçların kullanımı |
| 6 | 2 Gigabayt RAM |
| 7 | DS3231 Modülü |
| 8 | Raspberry Pi 4 tarafından tüketilen 6,0W güç |

## 4.3 Akıllı Sözleşmelerin Uygulanması

P2P enerji ticareti için akıllı sözleşme uygulaması, 2 farklı akıllı sözleşme türüne dayanmaktadır: enerji ticareti için ASler ve mahremiyeti korumak için ASler. Enerji ticareti AS, Bölüm 3'teki gözden geçirilmiş bir makale ile aynı kodla uygulanmaktadır. Han ve ark. çifte müzayede piyasası modelinin uygulanması için oldukça verimli ASler sunmuştur [53]. Bu tez çalışması aslında enerji ticareti için konuşlandırılabilir yeni bir akıllı sözleşme sunmamakta, ancak doğrudan en son teknoloji ürünü çözümü kullanmaktadır. [53]'te verilen enerji ticareti mekanizması, teklif verme, enerji alışverişi, uzlaşma ve ödeme için dört farklı akıllı sözleşmeden oluşmaktadır. Bu AS mekanizmasının P2P enerji ticaretinde etkili olduğu kanıtlanmıştır ve bu belge kapsamında kullanım için daha fazla geliştirme gerektirmemektedir. Akıllı sözleşmeler, [59]'da önerildiği gibi geçişken bir yönetim altyapısı üzerinde konuşlandırılacaktır. Dağıtım altyapısının şeması Şekil 4.4'te verilmiştir. Burada EEYS, bu çalışmada sunulan enerji yönetimi donanımına eşdeğerdir. Bu altyapı üzerinde, toplayıcı ile üretici tüketiciler/tüketiciler arasında bir iletişim yolu olarak IoT mesajlaşma için geliştirilmiş MQTT standardı kullanılmıştır. Enerji ticaretine yönelik alış ve satış teklifleri, MQTT

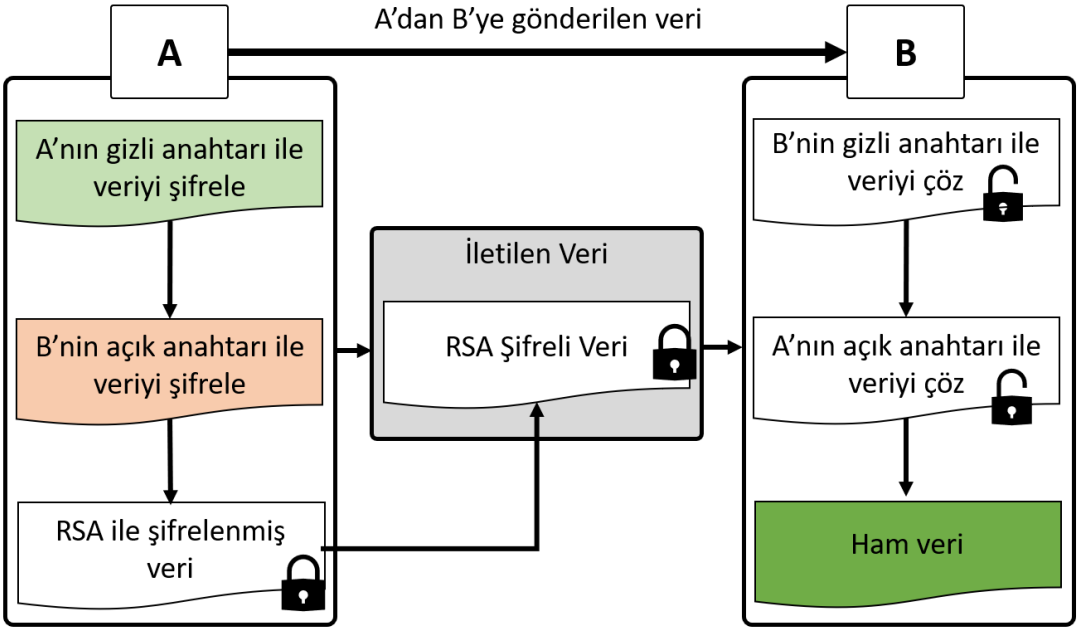
Yayınla / Abone Ol Mimarisi içerisinde JSON formatında gönderilmektedir. Bu mimari, akıllı sayaçların kimlik doğrulaması için bu belgede sunulan modelde kullanılmayacak olan bir "Sertifikalı Akıllı Sayaçlar Veritabanı" sunmuştur, aşağıda açıklanan başka bir yöntemle bu işlev gerçekleşeceğinden bu eleman mimariden çıkarılmıştır. Kimlik doğrulama için kullanılan kriptografik anahtarları veya imzaları saklamak için toplayıcı sunucusunda bir ayrı bir veritabanı kullanmak, siber güvenlik açısından uygun bir uygulama değildir, çünkü bu sunucu tehlikeye girebilir ve bu da blokzinciri için ciddi bir güvenlik açığına neden olacaktır. [59]'da verilen bu yöntem, dağıtık bir sistem için istenmeyen siber saldırılara açık bir zayıf nokta oluşturmaktadır. Önerilen model, anahtarları tek bir yerde depolamak yerine, enerji yönetimi donanımında bulunan TPM'leri kullanmaktadır. Bu, bir düğümün bir siber saldırı tarafından ele geçirilmesi durumunda tüm sistemin risk altında olmamasını sağlamaktadır.




Şekil 4.4: Akıllı sözleşmelerin dağıtımı için önerilen geçişken yönetim altyapısı [59].

Önerilen model, düğümlerin mahremiyetini korumak için asimetrik şifreleme tekniğini kullanmaktadır. Verilerin sağlam şekilde güvenliğini sağlamak için, tüm kriptografik işlemler enerji yönetimi donanımında tamamlanmalıdır. Blokzinciri halka açık

olduğundan, güvenlik için şifrelenmemiş hiçbir veri diğer düğümlere gönderilmemelidir. Toplayıcının sunucusuna gönderilecek verilerin içeriğinin güvenliğini sağlamak için tüm işlemlerin RSA algoritması kullanılarak şifrelenmesi gerekmektedir. RSA, OpenSSL yazılım paketi aracılığıyla enerji yönetimi donanımına uygulanabilmektedir. OpenSSL, donanım üzerinde güvenli bir açık ve gizli anahtar çifti üretimi sağlamaktadır. Rastgele bir RSA açık-gizli anahtar çifti oluşturulduktan sonra, enerji yönetimi donanımı açık anahtarı toplayıcı ile paylaşacaktır. Blokzincir için RSA tabanlı asimetrik şifrelemenin basitleştirilmiş bir şeması Şekil 4.5'te gösterilmektedir. Şekil 4.5'te enerji yönetim sistemi "A" olarak, toplayıcı ise "B" olarak gösterilmiştir. [66]'da verilen akıllı sözleşme 1, enerji ticareti blokzinciri içindeki iletişimleri güvence altına almak için kullanılabilecektir. Bu yöntem, kötü niyetli düğümlerin bulunabileceği blokzinciri ağına hiçbir özel verinin sızdırılmamasını sağlamaktadır. Aynı şifreleme anahtarları, işlemlerin kimlik doğrulaması için de kullanılabilecektir. Bu nedenle, son teknoloji blokzinciri tabanlı enerji ticaret platformlarındaki kritik bir gizlilik sorunu bu model ve yöntem ile çözülmektedir.




Şekil 4.5: RSA şifreleme tabanlı blokzinciri veri güvenliği örneği [66].

## 4.4 Önerilen Uzlaşma Modeli

Mikro şebekenin dinamikleri, blokzincirine katılımda her bir düğümü eşit tutarken uzlaşma sorununa güvenilir ve hızlı bir çözüm gerektirmektedir. Mikro şebekenin taleplerini karşılayan bir blokzinciri yönetimi oluşturmak için, bir ticaretin onaylanması için gereken sürede hiç değişiklik olmayan veya çok az değişiklik olması ve blokların doğrulanması için istikrarlı bir zamanlama bulunması gerekmektedir. Aşağıda önerilen model, risk-ödül sistemini dengeli bir seviyede tutmaya çalışırken belirli bir onay süresinin gerekliliğine odaklanmaktadır. Aynı zamanda, önerilen yerel enerji piyasasındaki aktörler yüksek oranda enerji sürdürülebilirliğine odaklandığından, kullanılan uzlaşma algoritması enerji verimli olmalıdır. Model, özet fonksiyonu bulmacası çözmeyi gerektirmeyen yeni bir uzlaşma algoritmasının uygulanmasıyla ticaret ağının enerji verimliliğini artırmayı hedeflemektedir.

Önerilen model, son teknoloji çözümlere benzer bir P2P enerji ticaret platformudur, ancak uzlaşma algoritması ve uygulama yöntemlerinde farklılık göstermektedir. Önerilen uzlaşma algoritması, doğrudan mikro şebekede üretilen yenilenebilir enerjiye ve hâlihazırda üreten tüketicinin şebekeye bağlantısında bulunan akıllı sayaçlara dayanmaktadır. Akıllı sayaçlar, verimli çalışmak için mikro şebekelerde sıklıkla kullanılmakta ve maliyeti, yenilenebilir enerji üreten cihazlar üreticinin mülküne kurulurken zaten ödenmektedir. Böylece bu modelin uygulanması açısından ek bir maliyet oluşturulmamaktadır. Bu model, blokzincirindeki her düğümün, bir üreticiye veya tüketiciye ait bir akıllı sayaçla bağlantılı enerji yönetimi donanımı olduğunu varsayar, böylece herhangi bir ekstra bilgi işlem gücü gereksinimi ortadan kalkmaktadır. Bu şekilde sistem, CPU veya ASIC cihazı gibi bilgi işlem gücü kaynaklarına daha fazla yatırım yapmadan çalışacaktır. Önceki bölümde açıklanan piyasa yapısı ve ağ yapısındaki farklılıklar ve bu bölümde sunulan uzlaşma algoritması dışında sunulan modelin ticaret için tercih edilen yapısı [50]'de sunulan ikili müzayede uygulamasına ilişkin en son teknoloji çözümlere oldukça benzerdir.

Model, blokzincirinin her bir düğümü tarafından üretilen yenilenebilir enerji üretim miktarına dayanan "Yeşil Enerji Kanıtı" (YEK) adlı yeni bir uzlaşma algoritması kullanmaktadır. Polkadot ekosistemi sistem için ana zincir olarak kullanılmakta, enerji

ticareti yapmak ve işlem verileri üzerinde uzlaşmaya varmak için ek akıllı sözleşmeler kullanılmaktadır. Enerji, yalnızca birbirine yakın konumdaki bir mikro şebeke içerisindeki üreten tüketicilerden ve tüketicilerden oluşan blokzincirinin üyeleri arasında alınıp satılacaktır. Diğer mikro şebekeler, enerji santralleri veya araçtan şebekeye tesislerle yapılacak enerji ticareti, mikro şebekede oluşturulan toplam enerjinin düğümlerdeki talebi karşılamak için yeterli olmadığı nadir durumlarla sınırlıdır. Şekil 4.2, ticaret platformunun temel yapısını ilgili düğümler ve araçlarla birlikte göstermektedir. Mikro şebeke kendi kendine yeterliyse, harici enerji santralleri ve diğer mikro şebekelerle bağlantı oldukça sınırlıdır. Şekil 4.2'de gösterilen üreten tüketici ve tüketici düğümlerinin şemadaki göreli mesafesi, muhtemelen gerçek hayat uygulamalarında farklılık gösterecek olan blokzinciri ağına bağlantı sürelerine göre gösterilmiştir. Üreten tüketici sayısının, tüketici sayısından daha fazla olması düğümler arasında geçerli bir ticaretin gerçekleşmesi için gereklidir ve modelin oluşturulmasında bu şekilde bir yapı olduğu varsayılmaktadır. Her bir üretici veya tüketici, yalnızca İnternet üzerinden bilgi alıp gönderebilen akıllı sayaçlara sahip enerji yönetim sistemi aracılığıyla ağa bağlıdır.

Ticaret platformu, enerji ticaretini ve uzlaşma algoritmasını düzenleyen Rust tabanlı akıllı sözleşmelere dayanan bir blokzincirinden oluşacaktır. Enerji Ticaret Blokzinciri'nin içyapısı bu bölümde daha detaylı bir şekilde verilmektedir. Blokzincir içinde [53]'te verilene benzer şekilde çalışan akıllı sözleşmeler vardır. Enerji yönetim sistemi tarafından çağrılan ilk akıllı sözleşme, kullanıcı tarafından belirlenen fiyatlara göre düğümler arasında enerji değişim oranlarının değiş tokuş edildiği kapalı tekliftir. Daha sonra enerji alışverişi ve yerleşimi için farklı AS'ler çağrılacaktır. Taraflar enerji ticareti konusunda anlaştıktan sonra ödeme AS çağrılacaktır. Bu modelde ticaret süreklidir ve her düğüm, sahibi katılmak istediğinde ticarete dâhil olmakta serbesttir. Verilen akıllı sözleşmeler, talep tarafı için mevcut en düşük fiyattan elektrik almakta ve üretici tarafı için en yüksek fiyattan elektrik satmaktadır. Fiyat için üst sınır başlangıçta piyasa otoritesi tarafından sağlanan resmi elektrik fiyatı, en düşük fiyat ise düzenleyici kuruluşun tarife alış fiyatı olarak belirlenecektir. Enerji ticareti sözleşmesi, ticaret isteyen düğüm tarafından tetiklenmekte ve bu sözleşme, bir ticaret başarılı olduğunda bir sonraki akıllı sözleşmeyi tetiklemektedir. Enerji miktarı, fiyatı ve zaman damgası ile alıcı ve satıcıya ilişkin ticaret bilgileri, yeni bir bloğun oluşturulması için blokzincirine gönderilecektir. Enerji ticareti tamamlandığında ve işlem bilgileri bir blok içinde güvence altına alındığında, veriler

değişmez bir şekilde saklanmış olacaktır. Bu işlem sırasında gizliliği koruyan AS aktiftir ve toplayıcı ile diğer düğümler arasındaki tüm iletişimi şifreleyerek güvence altına almıştır.

Yeşil Enerji Kanıtı uzlaşma algoritması, bir ticaret yapıldıktan ve yeni bir blok oluşturulduktan sonra gerçekleşecektir. Blok, Enerji Kanıtı'na benzer şekilde, ayarlanmış bir HK sürümü kullanılarak doğrulanacaktır. İlgili blok içinde bir ticareti tamamlayan blokzincirindeki her enerji yönetimi donanımı, daha önce bir genel anahtar almış ve daha sonraki işlemler için saklamış olmalıdır. Açık anahtarı aldıktan sonra, üreten tüketicinin enerji yönetim donanımı, belirli bir süre için toplam enerji üretim ve tüketim verilerini bu açık anahtarla şifrelemeli ve şifrelenmiş verileri toplayıcı sunucuya geri göndermelidir. Enerji üretim ve tüketim bilgileri tesis sahibi için özel bir kişisel bilgi olarak kabul edildiğinden, bu şifreleme işlemi düğümün mahremiyetini güvence altına almak için önerilmiştir. Bu yöntem, doğrulama için bir sıralama oluşturmak amacıyla bu özel verileri kullanan uzlaşma algoritması işlemi sırasında herhangi bir bilgi sızıntısını önlemektedir. Düğümün kimliği, başka bir kimlik doğrulamaya gerek olmadığı için hâlihazırda gizlenmiştir, ancak cüzdanla ilgili kimlik bilgileri bir siber saldırı ile sızdırılırsa, enerji verileri şifreleme tarafından yine de gizli tutulacaktır. Enerji yöneticisi donanımı, enerji üretim ve tüketim verilerini gönderdikten sonra, toplayıcı sunucu verilerin şifresini çözecek ve uzlaşma amacıyla verileri işleyecektir.

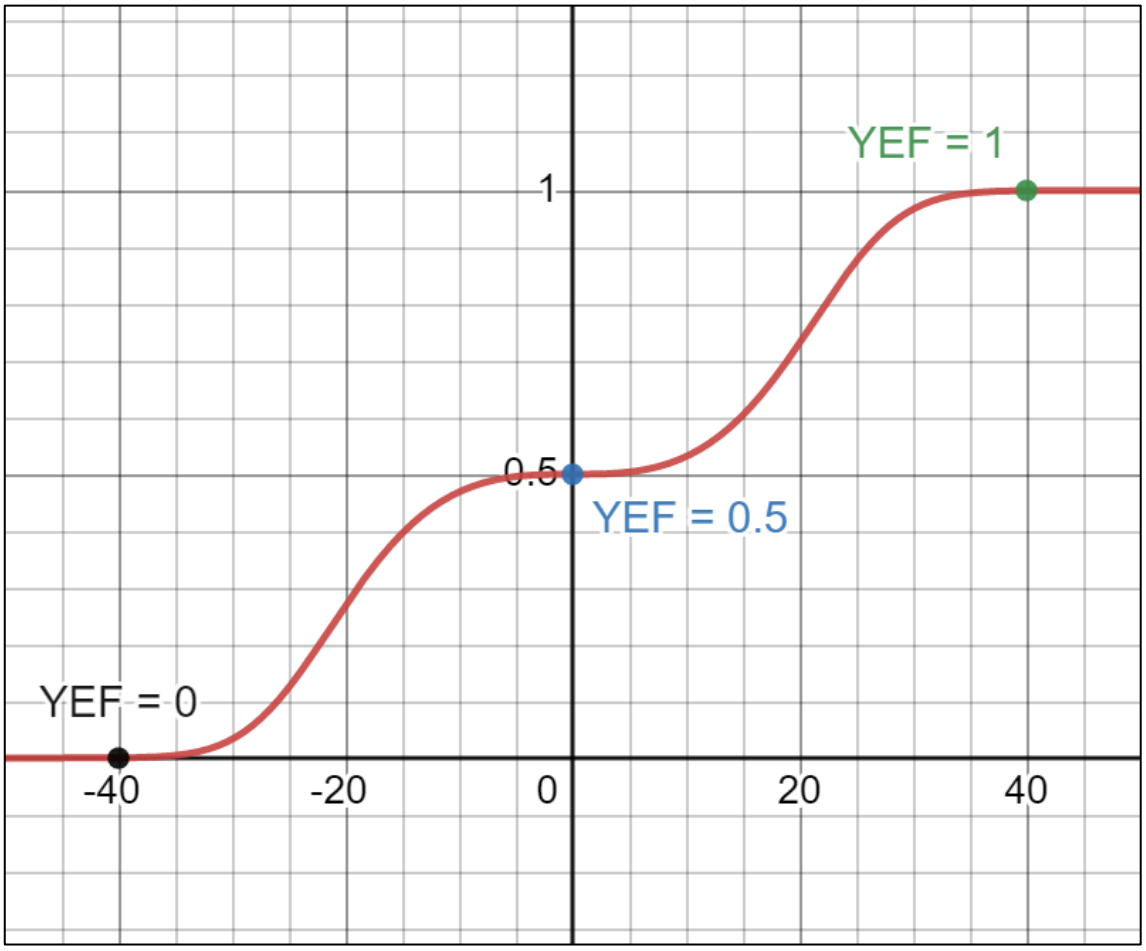
Yeşil Enerji Kanıtı uzlaşma algoritması, Bölüm 3'te açıklanan Enerji Kanıtı'na benzer şekilde çalışmaktadır. Bu yöntemde, Yeşil Enerji Fonksiyonu (YEF) için en yüksek puana sahip düğüm, bir sonraki doğrulayıcı olma şansı en yüksek düğüm olmaya adaydır. Genel olarak seçilecek doğrulayıcı, en düşük tüketim ile 1 dakika aralığında en fazla yenilenebilir enerji üretimine sahip düğümdür. YEF şu şekilde hesaplanır:

$$YEF = \frac{1}{1 + e^{(-(P-C)\times 0.05)^3}} \quad ve\ YEF = [0,1]$$

Burada $P$ düğüme ait üretim miktarını, $C$ ise tüketim miktarını ifade etmektedir. Burada YEF değeri [0,1] aralığında sınırlandırılmıştır. YEF değerinin bu aralıkta kalması ve uç noktalara yakın olduğunda yuvarlanması için yazılımsal olarak aşağıdaki kriterler uygulanacaktır:

$$Eğer\ YEF \leq 0.0006\ ise\ YEF = 0\ ve$$
$$Eğer\ YEF \geq 0.9994\ ise\ YEF = 1$$

Oluşan YEF değeri yazılımda virgülden sonra en fazla 5 basamak içerecek şekilde saklanacak ve hesaplamayı hızlandırmak için uç değerlerde yukarıda verilen kurala göre yuvarlanacaktır. Böylece ürettiği enerji değeri ile tükettiği enerji değeri arasında 40 Wh'lik bir fark olan kullanıcı için YEF değeri maksimum olacak; tükettiği enerji ürettiği enerjiden 40 Wh daha fazla olan kullanıcı için ise YEF değeri minimum olacaktır. YEF değerinin hesaplanması için kullanılan formülün $(P - C) = [-50,50]$ aralığı için çizilen grafiği Şekil 4.6'de gösterilmiştir.




Şekil 4.6: YEF Fonksiyonunun (P-C) için -40 ile 40 arasındaki grafiği

Düğümlerin YEF'e göre puanlanmasından sonra, her düğüm kendi puanına doğrusal bir hisse değeri alacaktır. Burada aynı düğümlerin sürekli olarak aynı zincir için doğrulayıcı olarak seçilmesini engellemek amacıyla Eşit Katılım Sağlaması adında ek bir tedbir

alınmıştır. Son 3 bloğu doğrulayan düğümlerin ilgili adresleri alınarak Eşit Katılım Sabiti adı verilen bir sabit hesaplanmakta ve bununla YEF değeri çarpılarak bir hisse değeri hesaplanmaktadır. Eğer son 3 bloğun onaylayıcısı ile mevcut aday eşleşiyorsa EKS 0, eğer son 3 bloktan 2'sinin onaylayıcısı ile aday eşleşiyorsa EKS 0.25 ve eğer yalnızca 1'i ile eşleşiyorsa bu değer 0.5 olacaktır. Burada bir düğümün sonraki onaylayıcı olma ihtimali şu şekilde hesaplanır:

$$Eşit\ Katılım\ Sabiti = EKS = \begin{bmatrix} Eğer\ Son\ 3\ Blokta\ 3\ eşleşme\ varsa\ EKS = 0 \\ Eğer\ Son\ 3\ Blokta\ 2\ eşleşme\ varsa\ EKS = 0.25 \\ Eğer\ Son\ 3\ Blokta\ 1\ eşleşme\ varsa\ EKS = 0.5 \end{bmatrix}$$

$$P_{Onaylayıcı} = YEF\ \times EKS$$

Bu yöntemle birlikte aynı doğrulayıcının blokzincirinde baskın olması engellenmekte ve tüm düğümlerin sisteme eşit katılım hakkı elde edebilmesi sağlanmaktadır. Bu durumda bir ev sahibi son 30 dakikadır o yerel piyasadaki baskın üretici olur ise bir sonraki bloğu onaylama ihtimali yoktur. Bu durumda ikinci en iyi üreticinin de sistemden ödül kazanma şansı doğacak ve sistemin ekonomik getirisi daha demokratik olarak paylaşılacaktır.

Uzlaşma protokolünün geri kalan işleyişi Ethereum'da uygulanan HK yöntemleri ile aynıdır, ancak paylar YEF'teki ve EKS'deki puanla elde edilen ilgili hisse değerleridir. Hissenin değeri ne kadar yüksek olursa, bir sonraki doğrulayıcı olma şansı da o kadar yüksek olmaktadır. Düğüm daha sonra ödül hakkında bilgilendirilmekte ve blok doğrulama için düğüme bir mesaj gönderilmektedir. Kazanan düğüm doğrulama için uygun değilse (Güç kesintisi vb.), uzlaşma protokolü derhal bölgedeki en iyi ikinci üreticiyi seçecek ve ilgili verileri ona gönderecektir. Bir düğüm oluşturulan bu yeni bloğu doğruladıktan sonra, bu blok blokzincirine eklenecek ve ticaret süreci tamamlanacaktır. Görüldüğü üzere, bu uzlaşma yöntemi, mikro şebeke düğümlerinin enerji üretimine ve tüketimine dayalıdır ve ödülün eklenmesiyle mikro şebeke içinde daha fazla yenilenebilir enerji üretimi ve ticareti için bir teşvik yaratılmıştır. Bu teşvik, insanları yenilenebilir enerjiye yatırım yapmaya ve/veya elektrik tüketimini azaltmaya teşvik etmektedir; çünkü yüksek üretim ve düşük tüketime sahip düğümler için ödül kazanma oranı daha yüksektir. Enerji Kanıtı yönteminin ana odak noktası kendi kendine yeterlilik olduğu için aynı teşviki sağlamamaktadır. Enerji Kanıtı protokolüyle ilgili sorun, kullanılan tüketim-üretim işlevinin kendi kendini idame ettiren düğümleri teşvik etme eğilimi, ancak yüksek enerji üretimi ve düşük enerji tüketimi ile üreten tüketicileri ödüllendirmekte başarısız

olmasıdır. Önerilen uzlaşma yöntemi olan Yeşil Enerji Kanıtı, bir uzlaşma doğrulayıcı grubu oluşturmak için kripto para birimlerine para yatırmanın, yenilenebilir enerji üretimine yönlendirilebilecekken yanlış harcanmış bir yatırım olduğu fikri üzerine inşa edilmiştir.

Doğrulayıcı atamasının zamanlaması, tüm düğümlerin seçim sistemine eşit şekilde katkıda bulunduğundan emin olmak için 1 dakika olarak ayarlanmıştır. Enerji depolaması maliyetli olduğundan ve anlık ticaret boşa harcanan enerjiyi azaltabileceğinden, enerji ticareti akıllı sözleşmesi herhangi bir zaman kısıtlaması ile sınırlı değildir. Ticaret süreci, yeni blokları işlem bilgileriyle doldururken, aynı zamanda üreten tüketici havuzundan 1 dakikalık aralıklarla bir doğrulayıcı seçmektedir. Doğrulayıcı atandıktan sonra, kötüye kullanımları sınırlamak ve kazanana ödülü alma şansı vermek için kazanandan bir dakika içinde yanıt vermesi beklendiğinden doğrulama hızlıdır. Belirlenen bu zaman sınırları oldukça teoriktir ve gerçek hayattaki uygulamalarda daha hızlı veya daha yavaş doğrulamaları hesaba katmak için yazılım üzerinden kolayca değiştirilebilecektir. Sistem bir Polkadot yan zincirine dayanacaktır, böylece blokzincirinin güvenilirliği ve ölçeklenebilirliği sağlanmıştır.

# 5. MODELİN DEĞERLENDİRİLMESİ

Önerilen modelin enerji tüketiminin değerlendirilebilmesi için modelin yazılımının hazırlanmış ve bir donanım üzerinde çalıştırılmıştır. Yapılan benzer çalışmalardan gözlemlendiği üzere bir blokzinciri uygulamasının enerji tüketimini belirlemek için temelde teknik olarak iki farklı yöntem mevcuttur. Birinci yöntem, yukarıdan aşağıya olarak adlandırılmakta ve hâlihazırda çalışmakta olan bir blokzincir ağının genel yapısından yola çıkarak birim başına ne kadar enerji tüketimine sebep olduğunu tahmin ederek yürütülmektedir. Bu yöntemde bir ağı kullanan düğüm sayısı, işlem hacmi, finansal beklentiler, enerji fiyatları, kullanılan donanımlar, düğümlerin coğrafi konumu gibi belirteçler kullanılarak bu ağı kullanmanın ne kadar enerji tüketimine neden olduğu belirlenmektedir. Bu yöntemin uygulanabilmesi için blokzincir ağının geniş bir kullanım hacmine sahip olması ve tüm belirteçlerin sağlıklı biçimde toplanabilmesi gerekmektedir. İkinci yöntem olan aşağıdan yukarıya tekniğinde ise bir blokzincir ağında kullanılan ortalama bir donanım ile bu ağın yürütülmesi için kullanılan yazılımın ne kadar enerji tüketimine sebep olduğu tahmin edilmekte ve bu değer toplam ağ kullanıcı sayısı ile çarpılarak sonuçlar ölçeklendirilmektedir. Bu tez çalışması kapsamında önerilen modelin henüz yaygın kullanımda olmaması, coğrafi olarak çeşitli yerlere dağıtılarak ilgili verilerin toplanması için gerekli finansal kaynağın bulunmaması gibi sınırlayıcı nedenlerden dolayı enerji tüketiminin değerlendirilmesi için aşağıdan yukarıya yaklaşımı benimsenmiştir. Bu tez çalışmasının 5.3 bölümünde en yaygın kullanılan uzlaşma algoritmaları için her iki teknikle de yapılan çalışmaların sonuçları hakkında daha detaylı bilgi verilmiştir.

## 5.1 Model Değerlendirme Yazılım Altyapısı

Önerilen modelin enerji tüketiminin değerlendirilmesi için model çalışan bir yazılım haline getirilmiş ve bir blokzincir ağı olarak uygulanmıştır. Bu amaçla, özel blokzincir ağları oluşturmak ve özel olarak geliştirilen yazılımlar ile bu ağın yönetimini kişiselleştirebilmek adına kullanılan “substrate” yazılım platformu kullanılmıştır. Bu yazılım platformu Parity Technologies tarafından geliştirilmiş ve sıra dışı özelliklere sahip blokzincir ağlarının çok hızlı bir şekilde geliştirilip test edilmesini sağlamaktadır. Bu bağlamda substrate platformunun arka planda kullandığı Polkadot teknolojisi ile uyumlu çalışan Rust geliştirme dilinde yazılmış akıllı sözleşmeler ve bir blokzincir test

platformu geliştirilmiştir. Yazılan akıllı sözleşmeler substrate içerisinde palet olarak adlandırılan yapıların içerisine entegre edilerek farklı cihazların birbiri ile eşler arası iletişim kurabildiği ve ticaret gerçekleştirebildiği özel bir blokzincir ağı oluşturulmuştur. Geliştirilen bu özel blokzincir yapısında substrate içerisinde uzlaşma amacıyla kullanıma hazır olarak bulunan Aura ve GRANDPA paletlerinden de faydalanılmıştır. Önerilen modeli uygulamak için hazır paletlere ek olarak bir Yeşil Enerji Kanıtı paleti oluşturulmuş ve belirlenen uzlaşma mantığı Rust geliştirme dilinde bir algoritma haline getirilmiştir. Daha sonra birlikte kullanılan paletler ile birlikte önerilen model bu tez çalışmasında hedeflenen enerji verimliliği açısından değerlendirme yapılabilecek bir test yazılımı haline getirilmiştir.

Aura, yani Yetkilendirme Tabanlı Çevrimsel Sıralı Listeleme (Authority-based round-robin scheduling) paleti uzlaşma sağlamak için önceden belirlenen bir onaylayıcı grubunun adreslerini kayıt altına alarak yetkilendirme tabanlı bir çevrimsel sıralama yöntemi uygulamaktadır. Yani kendisine bir dosya içerisinde adresleri iletilen ve Yetki Kanıtı yönteminde olduğu gibi fiziksel bir yetkilendirme ile tanınmış kullanıcıları sırasıyla onaylayıcı olarak atamaktadır. Son onaylayıcıya gelindiğinde ise tekrar listenin başına dönerek işlemi devam ettirmektedir. Önerilen modelde YEF ve EKS değerleri kullanılarak oluşturulan onaylayıcı adayları grubu Aura paletine tıpkı önceden belirlenmiş ve yetkilendirmesi bulunan onaylayıcılar gibi iletilerek dinamik bir uzlaşma yöntemi oluşturulmuştur. Burada Yetki Kanıtı uygulaması için kullanılan Aura paleti tercih edilerek oluşabilecek ek gecikmelerin önüne geçilmiş ve önerilen model hızlı bir şekilde substate içerisindeki hazır bir palete entegre edilmiştir. Yeşil Enerji Kanıtı paletinde üretilen onaylayıcı olma ihtimali değerlerine dayanarak bloklar üzerinde uzlaşmayı başlatmak için en yüksek ihtimali olan kişiden başlayarak sırayla onaylayıcı belirleme işlemi gerçekleşmektedir.

Aura paleti ile belirlenen onaylayıcıya onay işlemini gerçekleştirmesi için ilgili mesajlar gönderilmekte ve onaylanma sonrası kontroller Aura yöntemiyle aynı şekilde gerçekleşmektedir. Onaylanarak blokzincirine eklenen bloklar daha sonra farkı düğümler arasında oluşabilecek farklı zincirlerden ayırt edilerek nihai bir zincir haline gelmektedir. Burada üretilen ve onaylanan son bloğun katıldığı zincirin nihai blokzinciri olarak tanınması için GRANDPA yöntemi kullanılmaktadır. GRANDPA yöntemi, kötü niyetli düğümlerin bulunma ihtimali olan blokzincirlerde blok sonlandırma için kullanılmaktadır

[67]. Bu yöntem Aura ile yazılan blokların ağ üzerindeki dedikodularını dinlemekte ve oy kullanma hakkına sahip doğrulayıcıları kullanarak hangi zincirin nihai zincir olacağına karar vermektedir. GRANDPA doğrulayıcıları, en iyi olduğunu düşündükleri bir bloğa oy vermekte ve oyları geçişli olarak önceki tüm bloklara uygulanmaktadır. GRANDPA yetkililerinin üçte ikisi belirli bir blok için oy kullandıktan sonra, o zincir nihai kabul edilmektedir. Bu yöntemle uzlaşma sona ermekte ve sistem yeni bloklar üretmeye devam etmektedir. Geliştirilen yazılım paketleri ve önerilen modelle ilgili Rust kodları Ek-1'de verilmiştir.

## 5.2 Model Değerlendirme Donanım Altyapısı ve Test Yapısı

Önerilen modelin enerji tüketiminin değerlendirilmesi için aşağıda verilen özelliklere sahip bir donanım kullanılarak bir test düzeneği oluşturulmuştur.

- Intel Core i7-6700 3.40 GHz 8 Çekirdekli işlemci
- 8 GB DDR4 RAM
- NVIDIA GeForce GTX 970 ekran kartı
- 512 GB Kingston SUV400s27120 SSD
- Windows 10 Pro işletim sistemi

Bu donanım üzerinde kurulan Windows için Linux Altsistemi yazılımı ile Ubuntu 22.04.1 LTS işletim sistemi üzerinde hazırlanan blokzincir yazılımı çalıştırılmıştır. Fiziksel olarak ayrık donanımlar üzerinde yapılacak testler yerine sanal makineler üzerinden aynı cihaz üzerinde çalışan alt sistemler kullanılarak test düzeneği basit ve hızlı hale getirilmiştir. Gerçekleştirilecek enerji tüketimi ölçümlerinin doğru ve tutarlı sonuçlar üretebilmesi için bu donanım üzerinde bulunan ekran kartının yazılım sürecine dâhil olması engellenmiştir. Ekran kartına ait sürücüler geçici olarak devre dışı bırakılarak sistem işlemci üzerinde bulunan görüntü işleme yongaları kullanılarak çalıştırılmıştır. Enerji ölçümünde temel olarak 3 farklı değer ele alınmış ve kullanılan donanımda bulunan işlemcinin geliştiricisi olan Intel'e ait "Power Gadget 3.6" yazılımı kullanılmıştır. Bu yazılımla birlikte cihaz üzerinde çalışan işlemciye ait görüntü işleme ve ana yongalar üzerindeki elektrik tüketimine ek olarak RAM kullanımı nedeniyle oluşan enerji sarfiyatı ölçülerek kayıt altına alınmıştır.

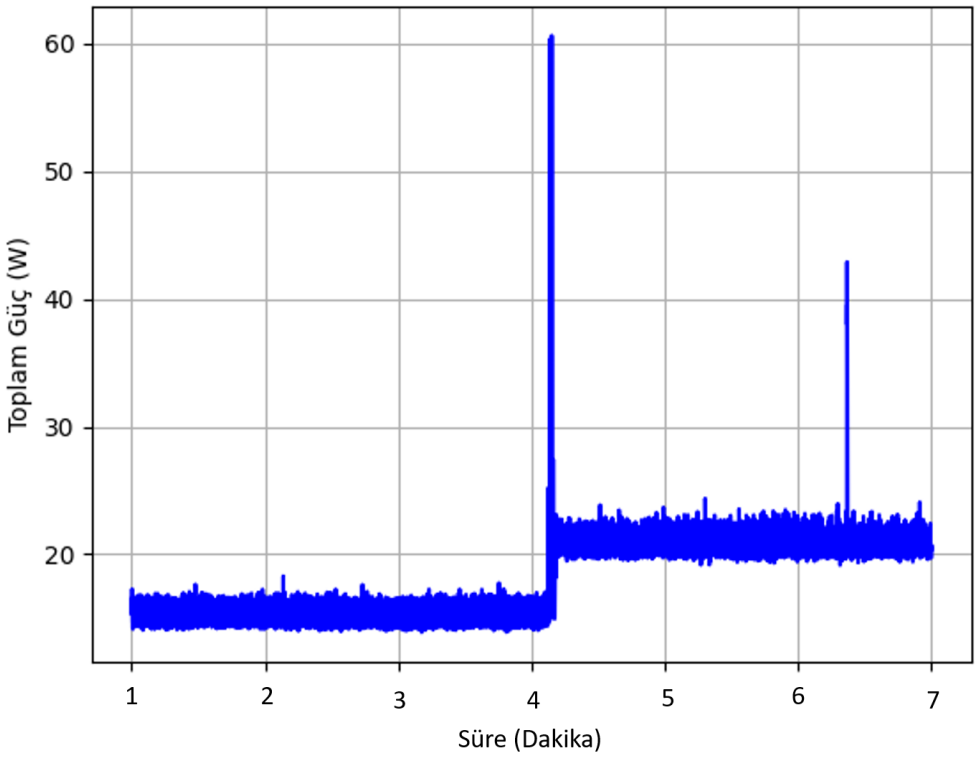
Önerilen modelin çalışması süresince oluşan elektrik tüketimini ölçmek için aşağıdaki test adımları sırasıyla gerçekleştirilmiştir.

- Donanım üzerinde çalışan ve test için ihtiyaç duyulmayan tüm servisler, uygulamalar ve sürücüler devre dışı bırakılmıştır. Böylece çalışan blokzincir yazılımı izole edilerek işlemci ve RAM üzerindeki etkisi daha net bir şekilde gözlemlenmiştir.
- Windows Güvenliği ve İnternet bağlantısı devre dışı bırakılarak ek enerji yükleri azaltılmıştır. Sistemin ürettiği her türlü uyarı ve zamanlanmış görev geçici olarak devre dışı bırakılmıştır.
- Ubuntu işletim sistemi üzerinde 4 farklı terminal arayüzü oluşturularak 4 farklı düğümü temsil eden 4 sanal makine oluşturulmuştur. Kullanıma hazır bir biçimde bekletilerek tek tuşla 4 makinenin aynı anda çalışabileceği basit bir yazılım düzeneği kurulmuştur.
- Sistemin anlık enerji tüketimini ölçmek ve kayıt etmek için Power Gadget 3.6 yazılımı her 100ms için ölçüm yapacak, 5 dakikalık aralıklarla ölçümlerini kaydedecek ve bir csv dosyası olarak Windows işletim sistemi üzerinde bir dosyaya kaydedecek şekilde hazırlanmıştır.
- Daha sonra Power Gadget'a ait alt yazılım Windows Powershell üzerinden çalıştırılmıştır.
- Sistem hiçbir etki ve işlem olmadan 4 dakika çalıştırılarak baz enerji tüketim değerli gözlemlenmiş, daha sonra ilgili modeli içeren blokzincir yazılımı 4 sanal makine için aynı anda çalıştırılarak otomatik ticaret işlemleri gerçekleştirilmiştir. 3 dakikalık çalışmanın ardından sistemler kapatılmıştır.

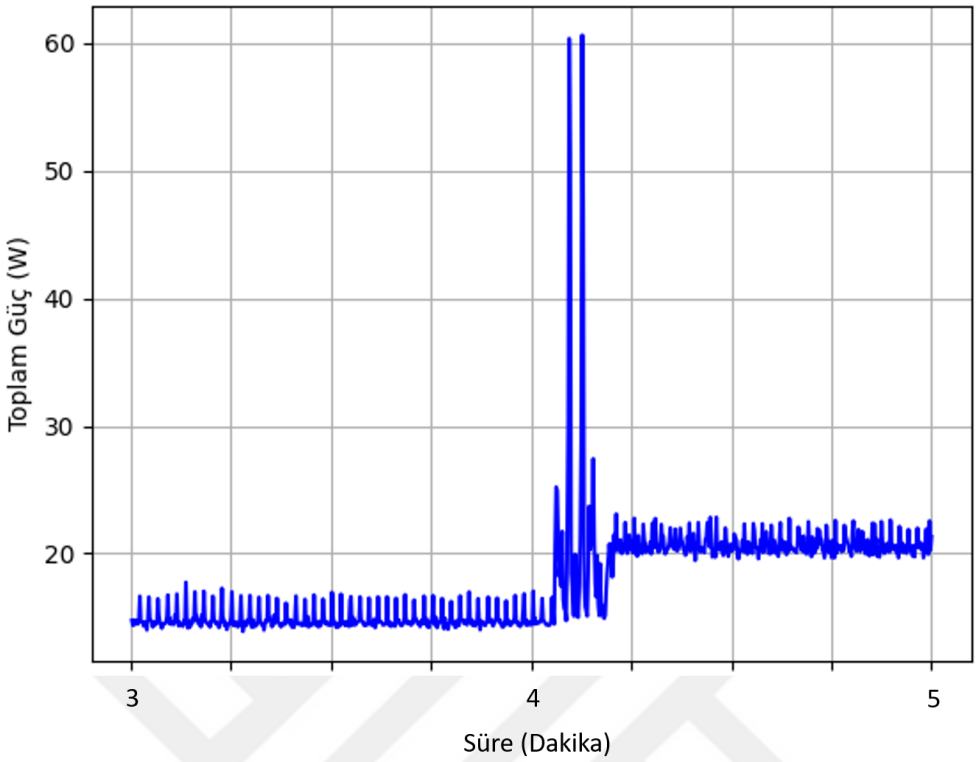
Deney sonuçlarının tutarlılığını ölçmek ve doğruluk payını artırmak amacıyla bu test yöntemi kullanılarak deney 5 kez tekrarlanmıştır. Elde edilen verilen csv dosyalarında kaydedilerek Python üzerinde yazılan bir görselleştirme kodu ile birlikte grafik haline getirilmiş ve işlenmiştir. İlgili test sonuçları tez çalışmasının bir sonraki bölümde değerlendirilmiştir.

## 5.3 Test Sonuçları ve Karşılaştırma

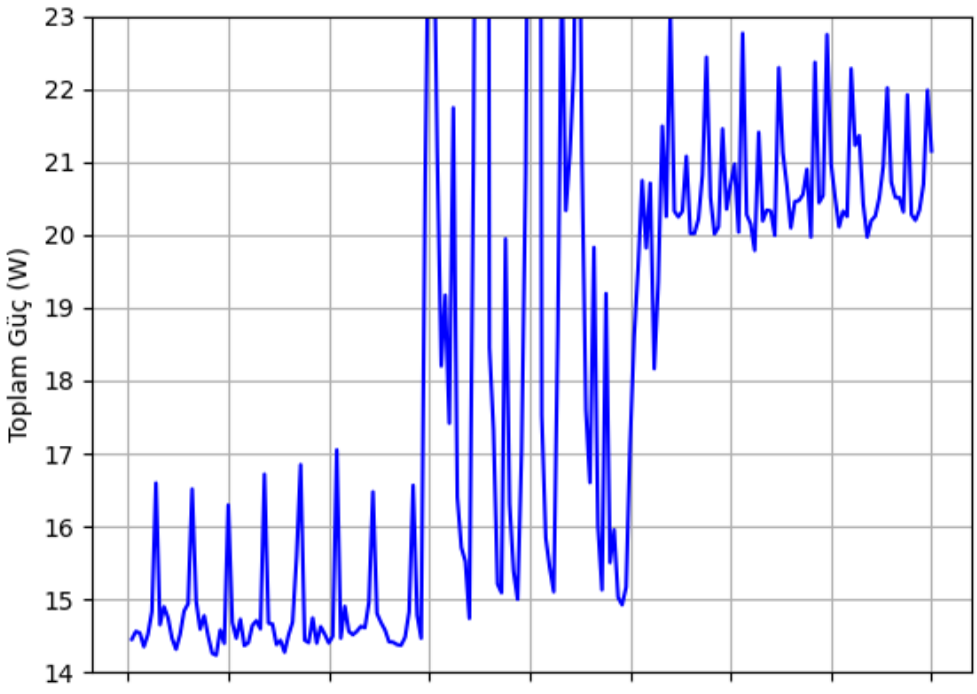
Ölçülen elektrik tüketimi verileri, işlemci ana gücü, işlemci görsel işleme çekirdek güçleri ve RAM güçleri olarak 3 farklı tüketim kalemi üzerinden toplanarak toplam enerji tüketimi elde edilmiştir. Bu toplam enerji üzerinden, önerilen modelin kullanıldığı blokzincir yazılımının çalışması ile birlikte sistemde oluşan elektrik tüketimi ile baz tüketim değerleri karşılaştırılarak modelin uygulandığı yazılımın neden olduğu ek tüketim değerleri elde edilmiştir. Elde edilen ham veriler, Python programlama dili kullanılarak görselleştirilmiş ve daha anlamlı hale gelmesi için işlenmiştir. Örnek olarak 1. deneyle ilgili ham verileri gösteren grafikler Şekil 5.1'de verilmiştir. Burada çalışma anında ani bir yükselme olmasının nedeni sanal makinelerin başlatılması ile ilgili olup, algoritmanın neden olduğu bir artış değildir. Bu grafiklerde işlemci üzerindeki yüklerin sıkça değişmesi nedeniyle rahatça görülemeyen değişim verilerin 5 ve 10 satırlık ortalamaları alınarak tekrar görselleştirildiğinde daha görünür hale gelmektedir. Görselleştirme açısından işlenmiş bu verileri içeren grafikler ***'de verilmiştir. Burada yazılımın çalışmaya başlaması ile birlikte ortaya çıkan anlık enerji yükü ve sonrasında baz tüketime göre oluşan ek elektrik sarfiyatı daha net bir şekilde gözlemlenebilmektedir.



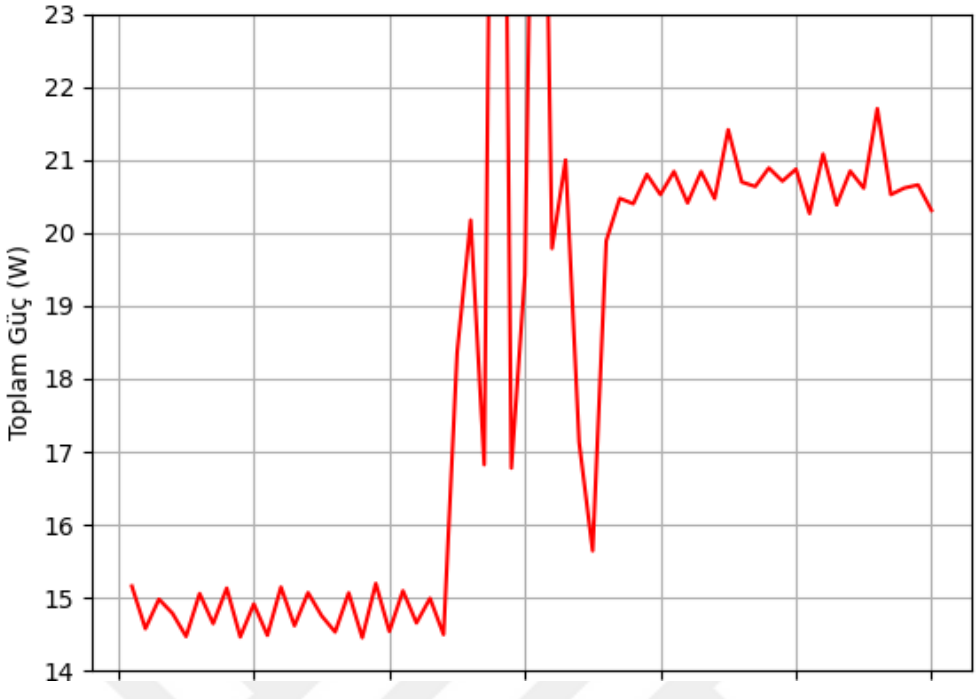

Şekil 5.1: Toplam Güç (W) ham verisi 1. deney



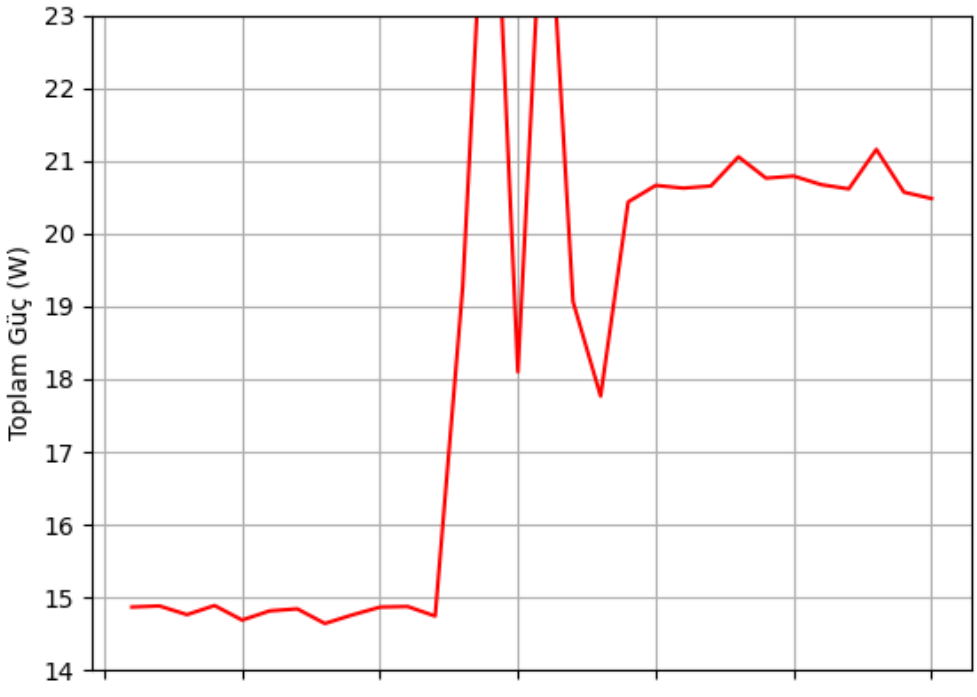

Şekil 5.2: Toplam Güç (W) ham verisi 1. deney çalışma anına yakınlaştırılmış.



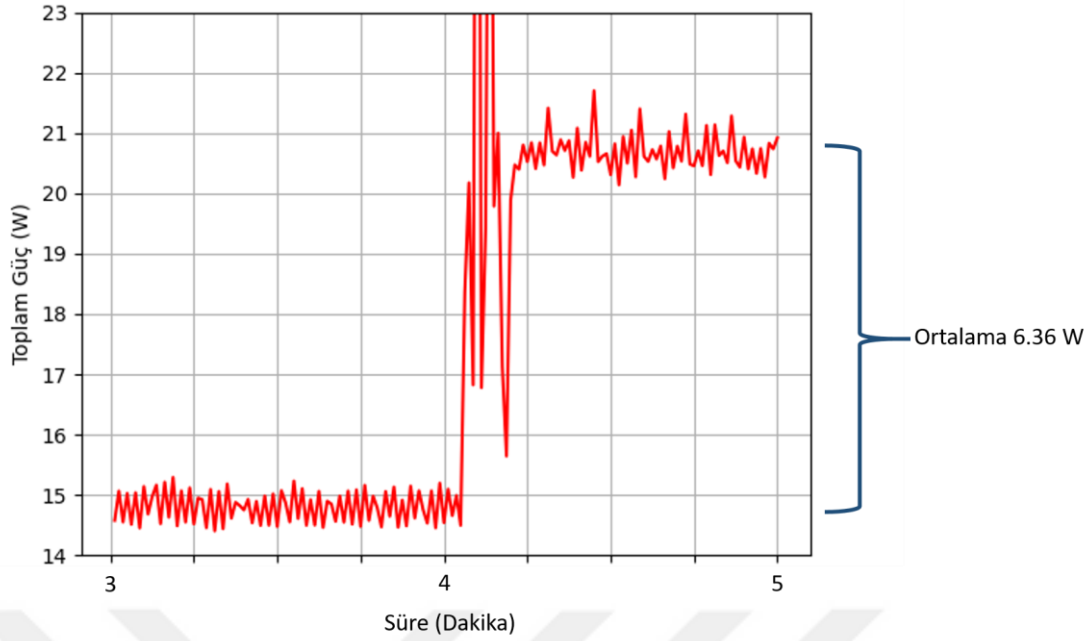

Şekil 5.3: Toplam Güç (W) ham verisi 1. deney çalışma anına ait detaylı veriler.




Şekil 5.4: Şekil 5.3'te gösterilen verilerin 5 satırlık ortalaması alınmış versiyonu.




Şekil 5.5: Şekil 5.3'te gösterilen verilerin 10 satırlık ortalaması alınmış versiyonu.




Şekil 5.6: Şekil 5.2'de gösterilen verilerin 5 satırlık ortalaması alınmış hali ve güç farkı.

Yapılan testlerde önerilen modelin toplamda ortalama olarak 6.36W kadar güç harcanmasına neden olduğu gözlemlenmektedir. Bu değer tez çalışması kapsamında incelenen diğer uzlaşma algoritmalarının kullanıldığı blokzincir teknolojileri ile karşılaştırıldığında önerilen model, İş Kanıtı'na göre oldukça düşük, Hisse Kanıtı'na ise yakın bir tüketim değerine sahiptir. Bitcoin ve farklı pek çok blokzincir uygulamasında kullanılan İş Kanıtı yönteminin neden olduğu ortalama donanımsal elektrik tüketimi "The Carbon Footprint of Bitcoin" adlı çalışmada incelenmiştir [68]. Bitcoin'in enerji tüketimini araştıran 2019 yılındaki çalışmada bu tez çalışmasına benzer şekilde aşağıdan yukarıya tekniğini kullanılmıştır. Bu nedenle elde edilen elektrik tüketim verilerini karşılaştırmak adına uygun bir çalışma olarak bu makale seçilmiştir. Bu makalenin eklerinde sağlanan veriler incelendiğinde İş Kanıtı kullanan Bitcoin ağı için ortalama bir donanımın neden olduğu yük 88W olarak ve bir alışveriş için ortalama enerji tüketimi 468kWh olarak verilmiştir. Mc Cook ve ark. Tarafından yapılan, aşağıdan yukarıya tekniğini kullanarak Bitcoin ağını inceleyen başka bir çalışmada bir alışverişin kaydedilmesi için toplam 535kWh enerji harcandığı tahmin edilmiştir [69]. Benzer şekilde Ethereum'un Hisse Kanıtı yöntemine geçmesinden sonra tükettiği enerji miktarlarını inceleyen bir çalışma Crypto Carbon Ratings Institute tarafından gerçekleştirilmiştir. Aşağıdan yukarıya tekniğini kullandığı için bu tez çalışmasının sonuçlarıyla karşılaştırılabilecek bu raporun bulguları Hisse Kanıtı'nın İş Kanıtı'na göre

çok düşük bir enerji tüketimi oluşturduğunu göstermektedir. Bu çalışma sonucunda Ethereum ağında bir alışverişin gerçekleşmesi için 6.29Wh enerji harcandığı ve ağa dâhil olan ortalama bir donanımın yıllık enerji tüketiminin 547.01kWh olduğu belirtilmiştir [70]. Bu raporda farklı Ethereum yazılım düğümleri ve farklı donanım seçenekleri için baz değerler ve yazılım nedenli ek tüketim değerleri incelenerek aşağıdan yukarıya doğru bir tahmin yapılmıştır. Ayrıca burada elektriksel yük olarak en az 20W ve en çok 150.06W'lık bir ölçüm gerçekleştirilmiştir. Ethereum Vakfı'nın resmi sitesinde kaynak olarak gösterilen bu raporda kullanılan yöntem ile bu tez çalışmasında kullanılan değerlendirme yöntemi oldukça yakındır fakat raporda farklı güçlere sahip donanımlar kullanılarak ağın genel yapısına dair daha kapsayıcı sonuçlar elde edilmiştir. Önerilen modelin İş Kanıtı kullanan Bitcoin ile ve Hisse Kanıtı kullanan Ethereum ile aşağıdan yukarıya tekniğiyle yapılmış enerji tüketim ölçümlerinin karşılaştırması Tablo 5.1'de verilmiştir.

Tablo 5.1: Yeşil Enerji Kanıtı ile en yaygın uzlaşma algoritmalarının karşılaştırılması

| **Uzlaşma Algoritması** | **Güç (W)** |
|---|---|
| İş Kanıtı | 88.00 |
| Hisse Kanıtı | 6.29 |
| Yeşil Enerji Kanıtı | 6.36 |

# 6. SONUÇ VE GELECEKTEKİ ÇALIŞMALAR

Önerilen model, uzlaşma algoritmasının enerji verimsiz yöntemler yerine yenilenebilir enerji üretimine dayalı olması nedeniyle en son teknolojilerden farklıdır. Blokzinciri işlemlerinin aşırı enerji kullanımı engellenirken, düğümlerin gizliliği güvenli ve değerli akıllı sayaç verileri şifrelenmiş halde tutulmuştur. Bu yeni modelin incelenen diğer modellere göre ana avantajı, İş Kanıtı veya Kimlik Kanıtı yöntemi yerine enerji üretimine dayalı Yeşil Enerji Kanıtı uzlaşma algoritması ile gelen doğrulama sistemidir. Önerilen model, yenilenebilir enerji üretiminin teşvik edilmesi için mikro şebeke içindeki en fazla enerji üreten düğümün ödüllendirilmesini sağlamaktadır. Süreç için enerji israf etmek yerine, P2P enerji ticareti için bu modelin kullanılmasıyla enerji verimliliği ve sürdürülebilirlik teşvik edilmektedir. Önerilen model, gerçek hayattaki düğümler gibi davranan birçok düğümün simülasyonu ile daha derinlemesine değerlendirilmeli ve ödül sistemi buna göre dengelenmelidir. Gerçek hayattaki bir uygulama için modelin verimliliğini daha gerçekçi olarak test etmek üzere 200 üreten tüketici ve 100 tüketici ile yeni bir simülasyon tasarlanabilir. Simüle edilmiş veriler, blokzincirinde çalışan mekanizmalara veya sözleşmelere ince ayar yapmak için yapılacak analizler için temel oluşturacaktır. Ayrıca sistemin ülke çapında uygulandığı bir senaryoyu test etmek amacıyla çok daha yüksek sayıdaki düğüm ile kapsamlı bir simülasyon yapılacaktır.

Önerilen model, blokzincir tabanlı enerji ticaretine katılmak isteyen tüm düğümlere akıllı sayaçların kurulmasını varsaymıştır. Sistem, bağlantı hızlarının ve kullanılabilirliğin kritik olduğu kırsal alanlarda bir problem unsuru olabilecek akıllı sayaç ağına bağlantıya dayalıdır. Önerilen model, bir gün içinde kendi enerjisini üretebilen ve tüketebilen birçok düğüme sahip, birbirine yakın bir şehir için daha uygundur. Enerji ticaretinin, yeterli üreten tüketiciye sahip kırsal kesimlerde yapılabilmesi için, sistemin veri toplama ve aktarma özelliklerine sahip bir uzak alan iletişim sistemleri ile entegre edilmesi gerekmektedir. Gelecekte bu sorunu çözmek için LoRaWAN teknolojisinden de yararlanan benzer bir model önerilebilir. Önerilen modelle ilgili bir diğer sorun, düğümlerin özel verilerine yönelik saldırılar olabilir. Enerji üretim verileri, blokzincirinin sözleşme verilerine yapılan bir saldırı nedeniyle mahremiyetleri kaybolursa düğümlere karşı kullanılabilir. Bu veriler blok içinde özel olarak ayarlanabilir ancak son zamanlarda Ethereum ağına bilgi sızıntısına neden olan bazı saldırılar yapılmıştır. Model, sözleşme

verileri için daha uygun bir gizlilik sağlamak üzere Ethereum yerine yepyeni bir kripto para birimini kullanmak üzere daha da geliştirilebilir.

# 7. KAYNAKÇA

[1] Renewable Energy At-a glance, https://www.c2es.org/content/renewable-energy/, (Erişim Tarihi: 21.04.2021)

[2] A.F. Michael Armbrust, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, A view of cloud computing, Communications of the ACM, 53 (2010) 50-58.

[3] P.H. Victor Ahlqvist, Thomas Tangerås, A survey comparing centralized and decentralized electricity markets, Energy Strategy Reviews, 40 (2022).

[4] D.W.G. Jixuan Zheng, Li Lin, Smart Meters in Smart Grid: An Overview, 2013 IEEE Green Technologies Conference, IEEE, Denver, CO, ABD, 2013.

[5] J.R.T.-p. Zekeriya Erkin, R.L. Lagendijk, Fernando Perez-Gonzalez, Privacy-preserving data aggregation in smart metering systems: an overview, IEEE Signal Processing Magazine, 30 (2013) 75-86.

[6] P.V. Brian O'Regan, Subhasis Thakur, John G. Breslin, EnerPort: Irish Blockchain project for peer- to-peer energy trading, Energy Informatics, 1 (2018).

[7] Mastercard Corporate Sustainability Report 2017, 2017, pp. 64.

[8] How much electricity does an American home use?, https://www.eia.gov/tools/faqs/faq.php?id=97&t=3, (Erişim Tarihi: 14.01.2023)

[9] D. AI, Total publications from full data by term 'Blockchain energy trade' between 2013 and 2022, 2023.

[10] E. Cohen, Microgrids could prevent need for planned power outages, https://theclimatecenter.org/opinion-microgrids-could-prevent-need-for-planned-power-outages/, (Erişim Tarihi: 12.05.2021)

[11] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[12] P.M. Dylan Yaga, Nik Roby, Karen Scarfone, Blockchain Technology Overview, National Institute of Standards and Technology, 2018.

[13] S. Likens, PWC, PWC Fintech, 2023.

[14] M. Oettler, Anonymity vs Pseudonymity, https://blockchain-academy.hs-mittweida.de/courses/blockchain-introduction-technical-beginner-to-

intermediate/lessons/lesson-4-privacy-in-blockchain-2/topic/anonymity-vs-pseudonymity/, (Erişim Tarihi: 15.01.2023)

[15] M.V. Blesson Varghese, Omer F. Rana, Philip Michael James, Realizing Edge Marketplaces: Challenges and Opportunities, IEEE Cloud Computing, 5 (2018) 9-20.

[16] A. Baliga, Understanding Blockchain Consensus Models, Persistent Systems Ltd., 2017.

[17] The Merge, https://ethereum.org/en/upgrades/merge/, (Erişim Tarihi: 08.01.2023)

[18] S. Nakamoto, "Re: Bitcoin P2P e-cash paper" E-mail, https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html, (Erişim Tarihi: 21.07.2022)

[19] S.G. contributors, PROOF-OF-WORK (POW), https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/, (Erişim Tarihi: 09.01.2023)

[20] Proof-of-work, and its flaws, explained, https://hedera.com/learning/consensus-algorithms/proof-of-work-and-its-flaws-explained, (Erişim Tarihi: 12.11.2022)

[21] A.O. James Lovejoy, 51% attacks, https://dci.mit.edu/51-attacks, (Erişim Tarihi: 01.01.2023,

[22] PROOF-OF-STAKE (POS), https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/, (Erişim Tarihi: 11.01.2023)

[23] L.K. Giulia Fanti, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, Gerui Wang, Compounding of Wealth in Proof-of-Stake Cryptocurrencies, arXiv, 2018.

[24] F.S. Ioanid Rosu, Evolution of Shares in a Proof-of-Stake Cryptocurrency, SSRN Electronic Journal, (2019).

[25] U.n.h.o. Dune, Ethereum ETH Staking Deposits, https://dune.com/hildobby/ETH2-Deposits, (Erişim Tarihi: 11.01.2023)

[26] L.A. Stefano De Angelis, Roberto Baldoni, Federico Lombardi, Andrea Margheri, Vladimiro Sassone, PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain, Italian Conference on Cyber Security Milan, İtalya, 2018, pp. 11.

[27] A.D. Vries, Bitcoin Energy Consumption Index, https://digiconomist.net/BITCOIN-ENERGY-CONSUMPTION, (Erişim Tarihi: 07.07.2022)

[28] L.K.U.G. Christian Stoll, The Carbon Footprint of Bitcoin, Working Paper Series, MIT Center for Energy and Environmental Policy Research, 2018.

[29] L.K. Ulrich Gallersdörfer, Christian Stoll, Energy Consumption of Cryptocurrencies Beyond Bitcoin, Joule, 4 (2020) 1843-1846.

[30] R.L.R. Camilo Mora, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada, Erik C. Franklin, Bitcoin emissions alone could push global warming above 2°C, Nature Climate Change, 8 (2018) 931-933.

[31] A.D. Vries, Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin, Patterns, 100633 (2022).

[32] C. Herzner, A last-minute attempt in Europe to ban Bitcoin fails in key vote, https://fortune.com/2022/03/14/attempt-ban-bitcoin-europe-fails-key-vote/, (Erişim Tarihi: 09.01.2023)

[33] N.L. Jingming Li, Jinqing Peng, Haijiao Cui, Zhibin Wu, Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies, Energy, 168 (2019) 160-168.

[34] T. Swanson, How much electricity is consumed by Bitcoin, Bitcoin Cash, Ethereum, Litecoin, and Monero?, https://www.ofnumbers.com/2018/08/26/how-much-electricity-is-consumed-by-bitcoin-bitcoin-cash-ethereum-litecoin-and-monero/, (Erişim Tarihi: 13.01.2023)

[35] A.d. Vries, Ethereum Energy Consumption Index, https://digiconomist.net/ethereum-energy-consumption, (Erişim Tarihi: 13.01.2023)

[36] S.M. Xi Fang, Guoliang Xue, Dejun Yang, Smart Grid – The New and Improved Power Grid: A Survey, IEEE Communications Surveys & Tutorials, 14 (2012) 944-980.

[37] The NETL Modern Grid Initiative, in: U.S.D.o. Energy (Ed.), National Energy Technology Laboratory, 2007.

[38] M.U.T. Santiago Grijalva, Prosumer-Based Smart Grid Architecture Enables a Flat, Sustainable Electricity Industry, Innovative Smart Grid Technologies (ISGT), (2011) 1-6.

[39] L.W. Soma Shekara Sreenadh Reddy Depuru, Vijay Devabhaktuni, Nikhil Gudi, Smart meters for power grid — Challenges, issues, advantages and status, 2011 IEEE/PES Power Systems Conference and Exposition, (2011) 1-7.

[40] V.R. Merlinda Andoni, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, Andrew Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews, 100 (2019) 143-174.

[41] T.S. Tiago Sousa, Pierre Pinson, Fabio Moret, Thomas Baroche, Etienne Sorin, Peer-to-peer and community-based markets: A comprehensive review, Renewable and Sustainable Energy Reviews, 104 (2019) 367-378.

[42] G.D. Hakem Beitollahi, Peer-to-Peer Networks Applied to Power Grid, 2007.

[43] Z.L. Congcong Liu, Comparison of Centralized and Peer-to-Peerv Decentralized Market Designs for Community Markets, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, 58 (2022) 67-77.

[44] J.W. Chenghua Zhang, Chao Long, Meng Cheng, Review of Existing Peer-to-Peer Energy Trading Projects, Energy Procedia, 105 (2017) 2563-2568.

[45] S.J.P. Eung Seon Kang, Jae Geun Song, Ju Wook Jang, A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid, 3rd International Conference on Computers, Communications, and Systems, IEEE, Nagoya, Japonya, 2018.

[46] J.K. Zhetao Li, Rong Yu, Dongdong Ye, Qingyong Deng, Yan Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 14 (2017) 3690-3700.

[47] B.N. Esther Mengelkamp, Carolin Beer, David Dauer, Christof Weinhardt, A blockchain-based smart grid: towards sustainable local energy markets, Computer Science - Research and Development, 33 (2018) 207-214.

[48] D.S. Nurzhan Zhumabekuly Aitzhan, Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams, IEEE Transactions on Dependable and Secure Computing, 15 (2016) 840-852.

[49] J.G.B. Subhasis Thakur, Peer to Peer Energy Trade Among Microgrids Using Blockchain Based Distributed Coalition Formation Method, Technology and Economics of Smart Grids and Sustainable Energy, 3 (2018).

[50] J.G.B. Subhasis Thakur, Barry P. Hayes, Distributed Double Auction for Peer to Peer Energy Trade using Blockchains, 2018 5th International Symposium on Environment-Friendly Energies and Applications (EFEA), IEEE, Roma, İtalya, 2018.

[51] T.E.W. Chain, Accelerating the Energy Transition with an Open-source, Decentralized Blockchain Platform. Energy Web Foundation, https://energyweb.org/reports/the-energy-web-chain/, (Erişim Tarihi: 30.04.2021)

[52] J.G. Esther Mengelkamp, Kerstin Rock, Scott Kessler, Lawrence Orsini, Christof Weinhardt, Designing microgrid energy markets: A case study: The Brooklyn Microgrid, Applied Energy, 210 (2018) 870-880.

[53] C.Z. Dong Han, Jian Ping, Zheng Yan, Smart contract architecture for decentralized energy trading and management based on blockchains, Energy, 199 (2020).

[54] M.B. Ioan Petri, Yacine Rezgui, Omer F. Rana, Blockchain for energy sharing and trading in distributed prosumer communities, Computers in Industry, 123 (2020).

[55] J.G.B. Subhasis Thakur, Cost Analysis of Blockchains-based Peer to Peer Energy Trade, 2020 IEEE International Conference on Environment and Electrical Engineering Madrid, İspanya, 2020.

[56] M.C.D. Sweta Malik, Subhasis Thakur, John G. Breslin, Blockchain based Decentralized Home Energy Management System using Double Auction, IARIA - eKNOWPortugal, 2022.

[57] S.T. Saurabh Shukla, John G. Breslin, Secure Communication in Smart Meters using Elliptic Curve Cryptography and Digital Signature Algorithm, 2021 IEEE International Conference on Cyber Security and Resilience (CSR) İtalya, 2021.

[58] S.T. Barry P. Hayes, John G. Breslin, Co-simulation of Electricity Distribution Networks and Peer to Peer Energy Trading Platforms, International Journal of Electrical Power & Energy Systems, 115 (2020).

[59] G.D.M. Pierluigi Siano, Alejandro Rolán, Vincenzo Loia, A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets, IEEE Systems Journal, 13 (2019) 3454-3466.

[60] GridWise Transactive Energy Framework, https://gridwiseac.org/, (Erişim Tarihi: 18.01.2023)

[61] E.B. Jae Kwon, Cosmos Whitepaper, https://v1.cosmos.network/intro, (Erişim Tarihi: 15.01.2023)

[62] A.T. Mehmet Suat Kayıkçı, İrem Ezgi Çavuşoğlu, Turkey: Aggregation Activity In The Electricity Market, https://www.mondaq.com/turkey/oil-gas--electricity/1267220/aggregation-activity-in-the-electricity-market, (Erişim Tarihi: 17.01.2023)

[63] D. Garcia, How do smart meters communicate?, https://www.emnify.com/blog/how-smart-meters-communicate, (Erişim Tarihi: 17.01.2023)

[64] Intel® QuickAssist Technology Overview, https://www.intel.com/content/www/us/en/architecture-and-technology/intel-quick-assist-technology-overview.html, (Erişim Tarihi: 10.01.2023)

[65] H. Neukirchen, Power consumption of Raspberry Pi 4 versus Intel J4105 system, https://uni.hi.is/helmut/2021/06/07/power-consumption-of-raspberry-pi-4-versus-intel-j4105-system/, (Erişim Tarihi: 07.01.2023)

[66] S.B.G. Nwosu Anthony Ugochukwu, Anand Singh Rajawat, Sardar M. N. Islam, Jiao He, Muhammad Aslam, An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method, Mathematics, 10 (2022).

[67] E.K.-K. Alistair Stewart, GRANDPA: a Byzantine Finality Gadget, Arxiv, 2020.

[68] L.K. Christian Stoll, Ulrich Gallersdörfer, The Carbon Footprint of Bitcoin, Joule, 3 (2019) 1647-1661.

[69] H. McCook, The Cost & Sustainability of Bitcoin, Academia, 2018.

[70] The Merge - Implications on the Electricity Consumption and Carbon Footprint of the Ethereum Network, Crypto Carbon Ratings Institute, 2022.

# EKLER

## EK 1 – Geliştirilen Yazılım Paketleri ve Kodlar

Bu tez kapsamında geliştirilen yazılım Rust programlama diliyle yazılmış bir substrate düğümüdür. Yazılımın tamamına ve çalıştırılabilir Web Assembly dosyalarına https://github.com/mertbilici/substrate-node-thesis adresinden erişilebilmektedir. Bu yazılımın önerilen modelle ilgili olan kod parçacıkları aşağıda verilmiştir.

```
--“// YEF Fonksiyonu Hesaplayıcı
   fn green_contribution_calculator(
      production: <T as Config>::GreenContribution,
      consumption: <T as Config>::GreenContribution,
   ) -> <T as Config>::GreenContribution {
      let value = 1.0 / (1.0 + (-((production - consumption).saturated_into::<f64>() * 0.1).powi(3)).exp());
      let rounded_value = match value.partial_cmp(&0.0006) {
         Some(Ordering::Less) => 0.0,
         _ => match value.partial_cmp(&0.9994) {
            Some(Ordering::Greater) => 1.0,
            _ => value.round_to_five_decimal_places(),
         },
      };
      rounded_value.saturated_into()
   }
“--
--" // Eşit Katılım Sabiti Hesaplıyıcı
   fn calculate_eoc<T: Config>(account_id: &T::AccountId, last_three_validators: &[T::AccountId]) -> f64 {
      let count = last_three_validators.iter().filter(|&validator| validator == account_id).count();
      match count {
         3 => 0.0,
         2 => 0.25,
         1 => 0.5,
         _ => 1.0,
      }
   }
“--
--“   // Doğrulayıcı olma ihtimali hesaplayıcı
   fn validator_probability<T: Config>(
      account_id: &T::AccountId,
      green_contribution: <T as Config>::GreenContribution,
      eoc: f64,
   ) -> f64 {
      green_contribution.saturated_into::<f64>() * eoc
   }
```

```
“--
--“ // Doğrulayıcı sıralama ve seçme fonksiyonu
 #[pallet::weight(10_000 + T::DbWeight::get().reads(1))]
       pub fn select_validator(origin: OriginFor<T>) -> DispatchResultWithPostInfo {
          let sender = ensure_signed(origin)?;
          // Ensure the sender is the beacon node by checking some condition (e.g., a specific account ID)
          ensure!(LatestBeaconIds::<T>::get().contains(&sender), "Not a valid beacon node");

          // Calculate the validator-probability for each node
          let mut probabilities: Vec<(T::AccountId, f64)> = Vec::new();
          for (account, green_contribution) in GreenContributions::<T>::iter() {
             let probability = validator_probability(green_contribution);
             probabilities.push((account, probability));
          }

          // Sort the nodes by the calculated probabilities
          probabilities.sort_by(|a, b| b.1.partial_cmp(&a.1).unwrap());

          // Select the node with the highest probability as the validator
          let (validator, _) = probabilities
             .first()
             .ok_or("No validators found")?;

          // Emit the event
          Self::deposit_event(Event::ValidatorSelected(validator.clone(), GreenContributions::<T>::get(validator)));

          // Send a message to the selected validator to validate the block
          // (This would involve using offchain workers, network communication or some other method)
          // For example:
          // send_validation_request(validator);

          Ok(().into())
       }
“
```