TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BLOKZİNCİR TEKNOLOJİSİ İLE REKOLTE TAHMİN PLATFORMU TASARLAMAK

Tuncay DOĞANTUNA

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç. Dr. Gazi Erkan BOSTANCI

ANKARA
2019

ETİK BEYAN

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum "Blokzincir Teknolojisi ile Rekolte Tahmin Platformu Tasarlamak" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir. Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Tuncay DOĞANTUNA
Tarih: 20.08.2019
İmza:

KABUL VE ONAY

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Bilimler Anabilim Dalı
Adli Bilişim İkinci Öğretim Tezli Yüksek Lisans Programında

Tuncay DOĞANTUNA tarafından hazırlanan

"Blokzincir Teknolojisi ile Rekolte Tahmin Platformu Tasarlamak" adlı tez

çalışması

aşağıdaki jüri tarafından **YÜKSEK LİSANS TEZİ** olarak

OY BİRLİĞİ ile kabul edilmiştir.

20.08.2019

Prof. Dr. Erkan AFACAN
Gazi Ü. Mühendislik Fakültesi
Jüri Başkanı

Prof.Dr. İlkay DELLAL
Ankara Ü. Ziraat Fakültesi
Üye

Doç.Dr. Gazi Erkan BOSTANCI
Ankara Ü. Mühendislik Fakültesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof.Dr. Mehmet AKAN
Sağlık Bilimleri Enstitüsü Müdürü

İÇİNDEKİLER

ÖNSÖZ

Bu çalışmada, gıda fiyatları üzerinde direkt etkiye sahip olan rekolte tahmin süreci ile ilgili sorunlara işaret edilmiştir. Bu sorunun çözümü için son yıllarda popüler bir konu olan blokzincir teknolojisi ile çözüm modeline yer verilmiştir. Blokzincir teknolojisinin, dağıtık ağ yapısı, mutabakat protokolleri ve akıllı sözleşmeler ile ilgili sağladığı konsept alternatif model ve tasarım oluşturmada faydalı olmuştur. Bu sebeple çalışma başlığı "Blokzincir Teknolojisi ile Rekolte Tahmin Platformu Tasarımı" seçilmiştir.

Bu çalışmanın gerçekleştirilmesindeki destek ve katkılarından dolayı danışmanım Doç. Dr. Gazi Erkan BOSTANCI'ya teşekkürlerimi sunarım.

Blokzincir kavramını özümsememde ve çalışmanın şekillenmesinde büyük bir katkısı olan Dr. Murat OSMANOĞLU ve Dr. Öğr. Üyesi Bülent TUĞRUL hocalarıma bilhassa teşekkürlerimi bir borç bilirim. Adli Bilişim programı kapsamında ders veren Disiplinlerarası Adli Bilimler Anabilim Dalı ve Bilgisayar Mühendisliği bölümünde yer alan tüm hocalarıma teşekkür ederim.

Ayrıca tez sürecinde beni motive ederek beni cesaretlendiren çalışmada bana geri bildirim sağlayan iş arkadaşlarım; Buğra C. HOCAOĞLU, Çağatay KORKUÇ ve Dr. Suat ATAN'a müteşekkirim.

Tez çalışma süresince beni destekleyen aileme özellikle de sevgili anneme ve babama teşekkürlerimi bir borç bilirim. Elbette hayatımın her alanında olduğu gibi tez çalışma süresince de bana katlanan ve beni destekleyen ve yardımcı olan sevgili eşim Ebru DOĞANTUNA'ya sonsuz teşekkür ederim.

SİMGELER VE KISALTMALAR

⊥	Diklik sembolü
∑	Toplam sembolü
AB-28	Avrupa Birliği (28 ülke)
AI	Yapay Zeka
ABARES	Avustralya Tarım ve Kaynak Ekonomisi ve Bilimleri Bürosu
BFT	Bizans Hata Toleransı
BZT	Blokzincir Teknolojisi
DDT	Dağıtık Defter Teknolojisi
DEFRA	Birleşik Krallık Çevre, Gıda ve Köy İşleri Bakanlığı
EVM	Ethereum Sanal Makinesi
IOT	Nesnelerin İnterneti
ML	Makine Öğrenmesi
NASS	Ulusal Tarım İstatistikleri Servisi
NDVI	Normalleştirilmiş Vejetasyon İndeksi
PBFT	Pratik Bizans Hata Toleransı
PoW	İşin İspatı
RPC	Uzak Prosedür Çağrısı
SHA	Güvenli Özet Algoritması
TARBİL	Tarımsal İzleme ve Bilgi Sistemi
TCMB	Türkiye Cumhuriyet Merkez Bankası

TÜİK	Türkiye İstatistik Kurumu
TZOB	Türkiye Ziraat Odaları Birliği
USDA	Birleşik Devletler Tarım Bakanlığı
UTXO	Ödenmemiş İşlem Çıktısı
VCI	Bitki Koşul İndeksi
ZMO	Ziraat Mühendisleri Odası

ŞEKİLLER

ÇİZELGELER

1. GİRİŞ

Son yıllarda tarımsal ürünlerdeki yüksek fiyat artışları ve fiyat dalgalanmaları kamuoyunun dikkatini çekmektedir. Uluslararası tarım ekonomistleri, bu tarz astronomik fiyat artışlarının yükselme eğiliminde devamını öngörmekte ve ilerleyen süreçte tarımsal ürünlerin küresel krizi tetikleyebileceğini vurgulamaktadırlar (Eştürk ve Albayrak, 2018). Gelişmiş ülkelerde, enerji fiyatlarındaki artış gıda fiyatlarını etkiliyorken, az gelişen ülkelerde gıda fiyatlarındaki değişiklik daha etkilidir. Gıda fiyatları, Avrasya ve Afrika coğrafyasındaki ülkeleri politik ve özellikle toplumsal olarak etkileme potansiyeline sahiptir. Üretim ve tüketimdeki belirsizlikler, gıda fiyatlarındaki artışın ana nedenidir. İklim değişikliği ve küresel ısınma, üretimdeki dalgalanmanın ana nedeni olarak kabul edilmektedir. Yerel ölçekten bakıldığında ise düşük rekolteden yansıyan üretim miktarına bağlı olarak istikrarlı bir fiyat politikası oluşturulamamıştır (Kıymaz, 2008).

Herhangi bir tarımsal ürün için rekolte tahmini, yerel, ulusal veya küresel ekonomik planlama için önemli girdiler sağlamaktadır. Nüfus artışı nedeniyle, saha düzeyinde istatiksel rekolte verisi gerektiren hem mikro düzeyde planlama hem de hasat sigortası için artan bir talep bulunmaktadır (Chaffin, 2009). Bu veriler, tarımsal üretimdeki verimsizlikle ilgili sorunun kaynağını açıkça göstermektedir. Böylece politika yapıcılar daha doğru ve daha iyi kararlar verebilir. Birçok ülke, yıllardır saha raporlarından veri toplanmasına dayanan geleneksel yöntemleri kullanarak rekolte tahmin sürecini gerçekleştirmiştir (Guled, 2007). Bu teknikler gerçekçi olmayan tahmin çıktıları ortaya çıkaran hatalara neden olabilir.

Hasat gelişimini izlemek ve doğru tahminler yapmak için daha hızlı ve uygulanabilir yöntemler kullanılması gerekir. Uzaktan algılama verileri, küresel ölçekte neredeyse gerçek zamanlı mekânsal bilgi sağlama potansiyeli ve yeteneğine sahiptir (Thenkabail ve ark., 2018). Bu veriler gerçeğe daha yakın rekolte tahmini

üretebilirler. Rekolte tahmin yöntemlerinin amacı, minimum zaman ve bütçede doğru sonuçlar üretmektir. Uydu teknolojileri yaygınlaşmadan önce, sadece tarımsal yatırımcılara ve kamu görevlilerine rekolte tahmin verilerini temin etmek için kullanılan deneysel-istatiksel ve ürün gelişim modellerini kullanan geleneksel yöntemler revaçtaydı.

Bitcoin ile birlikte ilk blokzincir uygulamaları kriptoparalar (dijital paralar) sayesinde tanıtıldı. Bununla birlikte, bilim insanları blokzincirin 'fintech' dışındaki birçok alanda uygulanabileceğini düşünmektedirler. Blokzincir uygulamaları son günlerde hayatın her alanında daha görünür hale gelmiştir. Hatta Uluslararası Siyaset üstü bir organizasyon olarak, Birleşmiş Milletler Gıda ve Tarım Örgütü (FAO) de, tarımda blokzincir uygulamalarının önemini vurgulamıştır (Tripoli ve Schmidhuber, 2018). Bugün tarım ve gıda alanında karşı karşıya kalınan birçok sorunun bu teknoloji ile çözülebileceği düşünülmektedir. Buna mukabil tarım sektöründeki blokzincir uygulamaları daha çok tedarik zincirine yoğunlaşmaktadır (Ballantyne ve Chavez-Tafur, 2019). Böylece tarımsal ürünlerin tüm gelişim ve lojistik süreçleri şeffaf bir şekilde takip edilebilir. Sonuç olarak, tedarik zincirinin herhangi bir aşamasındaki hata kolayca tespit edilebilir ve müşterilere anında bir çözüm sağlanabilir.

Son yıllarda, özellikle blokzincir teknolojisi sayesinde sayısal ve akıllı sözleşmeler oldukça öne çıkmıştır. Blokzincir genel bir ifadeyle, katılımcıları arasında yerleşik bir güven tabanı gerekmeden çalışan merkezi olmayan bir veritabanı olarak tanımlanabilir. Halen kullanılmakta olan en göze çarpan blokzincir ağları Bitcoin (Nakamoto, 2008) ve Ethereum (Buterin, 2013) olarak görünmektedir. Blokzincir altyapısının ana karakteristikleri, herhangi bir işin ispatını sunarken, gayri merkezi, izlenebilir ve şeffaf işlemler olmasıdır. Bilinmeyen kullanıcıların birbirleri arasında güven artırması ve katılım sağlaması için teşvikler ile birlikte işlem geçmişini değiştirme çabası için oldukça yüksek bir maliyet gerekmektedir.

Bu çalışmanın hedefi, blokzincir teknolojisi kullanarak işlenmemiş tarımsal ürünlerin üretiminde ortaya çıkabilecek belirsizlikleri netleştirebilecek alternatif bir rekolte tahmin yöntemi modellemek ve böylece bu modeli geliştirerek etkili bir sistem mimarisinin tasarımını planlanmaktadır. Bu modelin ve bu kurgunun bu bağlamda ilk olması hedeflenmektedir. Önerilen çözümde, yaklaşan hasat mevsimi için, öncesinde platforma kayıtlı çiftçilerden tahmini rekolte verileri toplanmalıdır. Böylece devlet ve özel kurumlar elde edilen verileri değerlendirebilir, hatta fiyatları dengelemek için gerekli planları ve yatırımları yapabilirler. Verilerin blokzincirde depolanmasından dolayı, herkes verilere erişebilecektir. Açık kayıt defterinde sansüre ve kurcalamaya dayanıklı ve değişmez olan işlemlerin depolanması nedeniyle katılımcılar arasında güvenilir bir mutabakat sağlanacaktır.

Bu tez çalışmasında, birinci bölümde konunun önemi ve çalışmanın amacı anlatılmıştır. Bölüm 2'de; tarımsal üretimde rekolte tahmin kavramı, blokzincir teknolojisi, akıllı sözleşmeler ve tahmin piyasalarına teorik zeminin oluşması maksadıyla değinilmiştir. Bölüm 3'de, daha önce blokzincir teknolojisi ile rekolte tahmin yöntemlerine herhangi bir çözüm modeli geliştirilip geliştirilmediğine dair araştırmanın çıktıları paylaşılmış, aynı zamanda BZT dışında kalan diğer yeni nesil teknolojilerinin rekolte sorununa yaklaşımları ele alınmış, ayrıca tarım ve gıda sektöründe BZT kullanımına dönük bulgular paylaşılmıştır, sonrasında bu modelin gereksinimine yönelik tahmini ürün rekolte verileri kıyaslanmıştır. Bölüm 4'de önceki bölümde anlatılan mekanizmanın şekillenmesi için model kurgusu belirlenip sistem tasarımı ve örneklem için güvenlik analizi ile ilgili tartışmaya yer verilmiştir. Bölüm 5'de ise, sonuç ve öneriler başlığı altında değerlendirme ve gelecek çalışmasından bahsedilmiştir.

1.1 Problemin İfadesi

Günümüzde, ürün fiyatları serbest piyasa koşullarına göre belirlenmektedir. Bu durumun piyasalarda rekabetçiliği ve serbest teşebbüsü güçlendirme açısından

faydaları vardır. Fakat birçok ülkede serbest piyasa koşullarının denge ve denetime uymaması nedeniyle, tarımsal ürünlerin aşırı değerlenmesi veya gerçek değerinin altında satış yapılması gözlemlenmektedir. Dolayısıyla aşırı gıda fiyatı enflasyonu ve tarımsal ürünlerin karaborsada işlenmesi gibi sorunlar ortaya çıkmaktadır. Bu noktada, mahsulün ve bölgenin şartlarına göre yıllık ya da mevsimlik olarak rekolte tahmin çıktılarını gerçekçi yansıtmak lüzumlu görünmektedir.

Son zamanlarda Türkiye'de gıda enflasyonu ile birlikte tartışmaya açık bir diğer konu ise, gerçekçi rekolte tahmini gözükmektedir. Sadece uydu verileri, uzaktan algılama sensörleri ya da nesnelerin interneti gibi hassas tarım teknolojilerine dayalı olarak anlık verileri toplayıp işleyen teknikler olarak değil de, rekolte tahminini çiftçinin yıllık planlarını kolektif tahmin ile bütünleştirecek gerçekçi tahminleri ortaya koyabilmesi, sorunu çözmekte bir kilometre taşı olabilecektir.

Her yıl Tarım ve Orman Bakanlığı, çiftçilere *"Tarımsal Desteklemeler"* olarak da adlandırılan sübvansiyon şeklinde milyonlarca Türk Lirası ödemektedir (Tarım ve Orman Bak., 2019). Mevcut tarımsal destekleme süreci çiftçilerin verdikleri rekolte beyanı ile birlikte TARBİL gibi uzaktan algılama teknikleri ile veri toplama yeteneği olan sistemin gücüne de dayanmaktadır. Ancak son gelişmeler, birçok işlenmemiş tarımsal üründe ekim alanlarının daraldığını ve rekolte tahminlerinin tam gerçekçi ortaya koyulamadığını göstermektedir. Çiftçiler, birçok temel gıda maddesi de olan bu işlenmemiş tarımsal ürünlerin bu derece fiyat artışı yapabileceğini tahmin edebilseydi, imkanı dahilinde ilgili tarımsal ürünlerin ekimini daha fazla yapabilirdi. Aynı şekilde, fiyat düşenlerin de ekimini düşürebilirdi.

Sorunları dikkatle takip edip yaklaşım geliştiren başka bir kurum olan Türkiye Cumhuriyet Merkez Bankası (TCMB) 2018 enflasyon raporunda, işlenmemiş gıda fiyatlarının enflasyonu ve bunun çözüme yönelik dinamik ürün rekolte takibi gereksiniminden bahsetmektedir. Raporda, işlenmemiş gıda ürünlerinde gözlenen aşırı artışların ardında yatan konjonktürel nedenler ile bunlara dair yapısal sorunların

temelini ve atılması gereken adımlar özetlendikten sonra; *"Tarımsal rekoltenin dinamik olarak izlenmesini ve tahmin edilmesini sağlayacak sistematik bir yapının kurulmasının da arzın sürekliliğini ve fiyat istikrarını korumak için gerekli önlemlerin zamanında alınmasına katkıda bulunacaktır"* görüşü paylaşılmıştır (TCMB Enflasyon Raporu, 2018).

1.2 Motivasyon ve Katkı

Gıda fiyatlarının istikrarını sağlamak için en önemli faktörlerden birisi, tarımsal ürünlerin üretimi için her ekim ve hasat sezonu öncesinde ortaya çıkacak verilere bağlı olarak planlama yapılabilmesidir. İster üretici ya da isterse yatırımcı konumunda olan tüketici olsun, gelecek dönemde ortaya çıkacak tablonun az çok belli olması beklenir. Elbette geçmiş yılların verisine bakarak, herhangi bir ürün için kaç dönüm ekilir ne kadar hasat edilir gibi gelecek döneme dair tahmin geliştirme yapılabilmesi mümkündür. Ancak serbest piyasa şartlarında yer alan aktörlerin en önemli amacı kar maksimizasyonudur. Kar elde etme söz konusu olunca, daha önce diğer oyuncularla mutabık kalınan noktalar önemsiz hale gelebilir. Diğer taraftan, merkezi devlet otoritesinin tarım ve gıda konusundaki yerel birimleri serbest piyasa aktörleri arasında denetleme, düzenleme ve hakemlik rolünü tam olarak yerine getiremeyebilir. Hatta resmi temsilci misyonunu yerine getiren kişilerin insan olması hasebiyle manipüle edilebilmesi de muhtemeldir. Özellikle tarım ve gıda sektöründeki aracı ve komisyoncuların bu tarz manipülasyonu yapmayacaklarının garantisi yoktur. Burada bir çözüm alternatifi üretebilmek, piyasada yer alan oyuncular arasında merkezi olmayan, dağıtık, şeffaf bir konsensüs mekanizması kurgulamak sayesinde sağlanabilir.

Diğer taraftan mevcut rekolte tahmin yöntemleri, ister geleneksel veya ister modern olsun fark etmeden, ekim ve hasat dönemlerinden itibaren sahada toplanan anlık veriler sayesinde rekolte tahmini gerçekleştirilebilmektedir. Diğer bir deyişle,

ekim ve hasat süreci gerçekleşmeden rekolte tahmini belirlemek için ihtiyaç duyduğumuz anlık veriler oluşmamaktadır. Dolayısıyla mevcut rekolte tahmin yöntemleri bu tip anlık verilere ihtiyaç duymaktadır. Bu şekilde gerçekleşen rekolte tahmin yöntemlerinin, üreticilerin gelecek üretim sezonu hakkında niyetlerini teyit edebilmesi mümkün değildir. Bu yüzden, üretim sezonu başlamadan çiftçilerin üretim planlarını birbirleriyle ve piyasanın diğer oyuncuları ile paylaşabilmesi bu sürece katılım sağlayan herkes için umumi menfaat meydana getirecektir. Bu noktada dikkat edilmesi gereken diğer husus ise, bu oyuncular arasında doğru bir mutabakat mekanizması üzerinde fikir birliğine varılması gereksinimidir. İlgili mutabakat mekanizması kimse tarafından sahiplenilemeyecek, kontrol edilemeyecek ve manipülasyona karşı dirençli olacaktır. Bu mekanizma son teknoloji ve kriptografi ile takviye edildiğinde mutabakatın bozulması imkansız hale gelecektir. Sonuç olarak bu özellikleri bir arada bulunduran blokzincir teknolojisi, bu yapıyı tasarlamada yol gösterici olacaktır.

Blokzincir teknolojisine dayalı birçok yeni tür dağıtık uygulama gerçeklenmektedir. Bu uygulamaların çoğu finansal sektördeki süreçlerin otomasyonu ve dijitalleşmesine odaklanmaktadır. Otomatik işlemler paradan tasarruf sağlayabilir ve şeffaflığı artırabilir. Verilerin işlenmesi, örneğin bir gözlem veya denetim esnasında, otomatikleştirilebilir ve sonuçlar güvenli ve dağıtık bir şekilde saklanabilir. Blokzincir teknolojisi sadece Türk tarımının verimliliği ve rekabet gücüne büyük katkı sağlamak için değil, aynı zamanda Afrika ve Avrasya bölgesindeki birçok ülke ve halkının tarımını güçlendirmek için potansiyel olarak kullanılabilir.

1.3 Araştırma Odağı ve Kapsamı

Rekolte tahmin yöntemleri, özellikle 1970lerden itibaren uydu haberleşme ve bilişim teknolojilerinin gelişimine paralel olarak modernleşerek daha komplike hale gelmiştir. Tarımın teknoloji ile daha fazla buluşur hale gelmesi de “Hassas Tarım” ve

“Hassas Tarım Teknikleri/Teknolojileri” şeklinde kavramlaştırılmıştır. Mevcut durumda geleneksel rekolte tahmin yöntemleri de birçok bölgede yaygın olarak yürütülmektedir. Çünkü bazı ürünlerin, sahada direkt uzmanları tarafından incelenmesi ve değerlendirilmesi gerekmektedir veya bazı bölgelerin ve çiftçilerin teknoloji olarak hassas tarım ile yeterince entegre olamaması da geleneksel yöntemlerin devamını bir sonuç olarak ortaya çıkarmıştır. Diğer yandan, büyük oranda modern rekolte tahmin yöntemleri olan uzaktan algılama teknikleri tarım sektöründe sermayenin artışı ve birikmesiyle iyice yaygınlaşmıştır. Aslında tez çalışmasında, rekolte kavramı ve tahmin yöntemleri hakkında yeterli temel bilgiler verilecektir, ancak rekolte tahmini konusunda anlık veri toplama kısmına odaklanılmayacaktır. Üreticilerin ekim planlarını rekolte tahmini olarak paylaşması noktasında; kişilerin deneyimsel tahmini ve saha gözlemleri olması hasebiyle geleneksel, toplanan verilerin blokzincir ağında tutulması ve ilgili tarımsal piyasa oyuncularının iletişim teknolojilerine sahipliği itibariyle de modern yöntemler şeklinde gözükmektedir.

Çiftçilerin yıllık veya dönemlik tarımsal planlarını paylaşmaları ve piyasanın diğer oyuncuları arasında kurulan mutabakata göre davranmaları mevcut rekolte yöntemleri kadar aynı zamanda tahmin piyasaları ile de benzerlik göstermektedir. Tahmin piyasaları aslında gelecek ile ilgili tahmin hisselerinin satıldığı piyasalardır. Fakat burada dikkat çekilen nokta “Kolektif Tahmin” olacaktır. Rekolte tahmin süreci, rekolte taahhüt mekanizması ile bağlantılı olduğu için, kolektif tahmin kavramına da kısaca değinilmiştir.

Bununla beraber, hem geleneksel hem de uzaktan algılama yöntemlerini birleştiren etkili alternatifler de mevcut olabilir. Ancak, başarılı bir tarımsal planlama için ülke ve bölge çapında konsensüs sağlayacak dağıtık ve şeffaf bir rekolte tahmini yöntemi gerektiği düşünülmektedir. Sonuç olarak bir model olarak ortaya çıkan çözüm, bu amacı gerçekleştirmeyi hedeflemektedir.

2. GEREÇ VE YÖNTEM

2.1 Tarımsal Üretimde Rekolte Kavramı

Tarımsal üretimde rekolte, bir üretim döneminde üretilen ürün miktarının toplamı olarak ifade edilebilir. Tarımsal üretimde rekolteyi doğru rakamlarla gerekli mercilere sunmak hem üretici tarafta olan çiftçi ve tarımsal yatırımcı için hem de tüketici tarafta bulunan vatandaş, devlet ve gıda endüstrisi için önemli bir meseledir. En basit haliyle, doğru rekolte tahminlerine ürün sigortası (Barnaby ve Russel, 2016), tahmini teslimat, hasat planlama ve depolama gereksinimleri, nakit akışı gibi birçok nedenden dolayı çiftçilerin ihtiyacı vardır. Benzer şekilde devlet açısından, ürün rekolte bilgisini öngörmek, karar vericileri ürün rekoltesindeki potansiyel azalma hakkında uyarır, böylece zamanında ihracat ve ithalat kararı vermesine imkan sağlar (Perrin, 1968).

Rekolte tahmini için başlıca iki yöntem tavsiye edilmektedir: Geleneksel yöntemler ve uzaktan algılama yöntemleridir. Geleneksel rekolte tahmin yöntemleri genellikle zaman alan saha ölçüm örnekleme tekniklerine dayanmaktadır. Bununla birlikte, mahsulün hasat edilmesine kadar rekolte tahmin sonuçları mevcut değildir.

Bunun yanı sıra, uzaktan algılama yöntemleri, eşzamanlı olarak geleneksel yöntemlerin dezavantajlarını ortadan kaldırmaktadır. Uzaktan algılama verileri, geniş alanlar üzerinde ürün rekoltesini tahmin etmek için yaygın bir şekilde kullanılmaktadır. Çünkü uydu tabanlı metotlar geleneksel ölçümlerden daha maliyet etkin ve zaman açısından elverişlidir. Fakat içerisinde bulunan bazı modellerin parametreleri karmaşık olduğu için onların çalıştırılması maliyetli ve zaman alıcı olabilmektedir (Shafian ve Valadanzouj, 2009).

2.1.1 Geleneksel Rekolte Tahmin Yöntemleri

Birçok ülkede rekolte tahmini, ürün için geleneksel veri toplama tekniklerine ve yer bazlı saha ziyaretleri ve raporlarına dayanan rekolte tahmin yöntemlerine dayanmaktadır. Bu tür raporlar genellikle öznel, maliyetli, zaman alıcıdır ve eksik arazi gözlemleri nedeniyle mahsulün yetersiz gözlemlenmesine neden olur. Ayrıca ürünün rekolte değerlendirmesine ve ürün alan tahminlerine yol açan büyük hatalara eğilimlidir (Reynolds ve ark., 2000). Çoğu ülkede verilerin işlenmesi, gıda kıtlığının önlenmesi ve uygun önlemlerin alınması için çok geç kalmaktadır.

Soğuk savaş yıllarından beri, ürün rekolte tahmini devlet için önemini giderek artan şekilde korumaktadır. Şimdiye dek ürün rekolte tahmininde birçok geleneksel yöntem ortaya çıkmıştır. Bu yöntemler saha raporlarına dayanmaktadır. Günümüzde ürün rekoltesini tahmin etmek için iki geleneksel yöntem vardır: Deneysel-istatistiksel modeller ve ürün büyüme modelleri (Jorgensen, 1994).

Belirli bir bölgede deneysel-istatistiksel modellerin, ürün rekoltesinin üzerinde etkili bir faktör olduğu uzun yıllardır hesaba katılmaktadır. Süreç içinde daha sonra ürün rekoltesi deneysel bir denklem ile etkin parametreye bağlanır ve her bir faktörün katsayısı bulunur. Sonrasında bu katsayılar ile ürün rekoltesi tahmin edilebilmektedir. Ürünle ilgili her deneysel model seti, başka bir faktör kümesine yol açar. Çoğu ilişkide etkili faktörler çevresel düzeyde olmaktadır (Shafian ve Valadanzouj, 2009).

Ürün büyüme modelleri ise, farklı fizyolojik süreçlerin çevre ile karmaşık etkileşiminin bir fonksiyonu olarak ürün rekoltesini tahmin etmektedir. Bu modeller günlük ürün büyüme simülatörü ile biokütle üretim potansiyelini tahmin eder. Bu yöntemlerin çalıştırılması, şu sayılanlar gibi çok fazla zorluğa sahiptir: Arazi üzerini dikkate almazlar, gerçek zamanlı değildir ve çok fazla maliyet gerektirir (Shafian ve Valadanzouj, 2009).

2.1.2 Modern Rekolte Tahmin Yöntemleri

Son günlerde çoğu ülkede hassas tarım yapılmaktadır. Geleneksel yöntemler tüm mahsulleri aynı anda değerlendiremez. Bu nedenle, bu eksikleri giderebilecek hedeflere yönelik bir yöntem belirlenmelidir. Uzaktan algılama teknikleri ise, geleneksel yöntemlerde ortaya çıkan hataları eş zamanlı olarak ortadan kaldırmaktadır (Mo X. ve ark, 2004).

Geleneksel yöntemlerin dezavantajlarını ortadan kaldıran uzaktan algılama teknikleri, 1970'li yıllardan beri ekinlerin ekimi ve hasadı arasında yakalanan uydu görüntülerini kullanır. Bu görüntüler, genellikle; Normalleştirilmiş Vejetasyon İndeksi (NDVI) ve Bitki Koşul İndeksi (VCI) olarak geçer. Ancak, rekolte tahmini hakkında hesaplanabilir veri sağlamazlar. İlk günlerde, uydu görüntülerinin yüksek maliyeti ve düşük çözünürlüğü nedeniyle yöntemler başarılı değildi. Bununla birlikte, teknolojideki ilerlemelere paralel olarak, birçok bilim insanı, gelişmiş uydu görüntülerine dayanarak daha doğru tahminler sağlayacak yeni yöntemler önermişlerdir. 1990'dan itibaren bu dezavantajlar kaldırılmış ve yüksek mekansal ve spektral çözünürlükte görüntüler üretilmiş ve çoğu araştırma bu yöntemleri kullanmıştır. Şimdi elektromanyetik dalga yansıması ile üretilmiş görüntülere sahip durumda olarak bu görüntülerden farklı bitki örtüsü endeksleri hesaplanmaktadır. Bu endeksler, bitki sağlığının ve verimliliğinin gerçek zamanlı olarak değerlendirilmesinde kullanılır, çünkü yeşil kütle ve su içeriği, protein, vb. dalganın yansımasını etkiler (Prasad ve ark., 2006).

Uyduların gelişmesiyle birlikte, uzaktan algılama görüntüleri küresel ölçekte mekansal bilgilere erişim sağlar; Dünya üzerindeki özelliklerin ve olayların neredeyse gerçek zamanlı olarak belirlenmesi sağlanır. Yalnızca ürün sınıflamada değil aynı zamanda ürün rekolte tahmin etme potansiyeline sahiptir (Sawasawa, 2003); mekansal değişkenlik hakkında bilgi tanımlayabilir ve sağlayabilirler ve alan araştırmasında

daha fazla etkinliğe izin verirler (Schuler 2002). Bu nedenle uzaktan algılama teknikleri, ürün gelişimi izlenmesi ve rekolte tahmini için kullanılabilir.

Bu yöntemler 3 kategoriye ayrılmıştır:

a. Deneysel-istatistiksel modellere dayalı uzaktan algılama yöntemleri
b. Su tüketen denge modeline dayalı uzaktan algılama yöntemleri
c. Biokütle tahmin modellerine dayalı uzaktan algılama yöntemleri

a. Deneysel-istatistiksel modellere dayalı uzaktan algılama yöntemleri:

Bu yöntemler geleneksel yöntemlere dayanmaktadır, ancak burada spektral endeksler, uydu ölçümlerinden değil yer ölçümünden hesaplanır. Bunları geleneksel yöntemlerle hesaplayan NDVI gibi endeksler zaman alıcı ve maliyetlidir.

b. Su tüketen denge modeline dayalı uzaktan algılama yöntemleri:

Bu yöntemler, mahsulün büyüme aşamalarında buharlaşma kesir işaretinin bir fonksiyonu olarak ürün rekoltesini tahmin eder. Buharlaşma kesir işaretini tahmin etmek için su tüketen denge modelini kullanır. İlk bütün büyüme periyodu on günlük sete bölünür ve daha sonra bu setlerde buharlaşma oranı hesaplanır. Büyüme periyodu 30 günlük sete bölünürse, model günlük formatta çalışıyorsa, ürün suyundaki bazı değişiklikler göz ardı edilir; bu durum pahalı ve zaman alıcı olacaktır.

c. Biokütle tahmin modellerine dayalı uzaktan algılama yöntemleri:

Biokütle tahmin yöntemlerine dayanan son yöntem ise iki gruba ayrılır: Ürün büyüme modelleri (Maas, 1988) ve Monteith modeli (Monteith, 1972).

I. Ürün Büyüme Modeli:

Ürün büyüme modelleri, farklı fizyolojik işlemlerin çevre ile karmaşık etkileşimlerine odaklanır. Aslında bu modeller büyüme aşamalarını açıklar. Ürün büyüme modellerini ve uydu verilerinden gelen spektral gözlemi birleştirmenin birçok yolu vardır (Maas, 1988). İlk başta tarif edilmiş ve sınıflandırmalar tekrar gözden geçirilmiştir (Delecolle, 1992). Gözlemlerin eşleşmesinde asıl strateji, çalışır modellerin veya doğrudan modelleme prosedüründe radyometrik gözlemlerden meydana gelen parametreleri içermektedir. Ürün büyüme modelleri, en etkili parametreleri dikkate alan bütün modellerdir. Büyük çapta çalıştırılabilirler ancak ziraat bilimi ile ilgili çok detaya girerler ve birçok parametresi vardır. Bu yüzden onların çalıştırılması maliyetli ve zaman alıcıdır.

II. Monteith Modeli:

Uzaktan algılama ile ürün rekoltesinin modellenmesi için basit ve kullanışlı diğer bir paradigma, Monteith'den (1972) elde edilir. Bu model, ürün rekoltesini tahmin etmek için biokütleyi kullanır. Monteith modelinde güneş ışınımının ve fotosentezin APAR hesaplaması, sıcaklık ve toprak neminin ürün rekoltesi üzerindeki etkisi göz önüne alınır.

2.1.3 Tarımda Dijital Dönüşüm ve Rekolte Tahminine Yansımaları

Son yıllarda birçok sektörlerde olduğu gibi tarım sektöründe de dijital teknolojiler sayesinde büyük bir dönüşüm süreci devam etmektedir. Tarım ve gıda sektöründe ortaya çıkan yüksek girdi maliyetleri, tarım arazilerinin sürdürülebilir yönetimi, verimlilik, pazarlama ve istihdam gibi birçok sorun tarım sektörünü dönüşüme zorlamaktadır. Tarımda ivmelenecek dijital dönüşüm, bilgi ve pratik tabanlı veriler sayesinde, teknolojik yöntemlerle çiftçinin hizmetine sunulup karşılaşılan birçok sıkıntıya çare bulunması, hatta üretilen ürün çıktılarının katma değerinin yükseltilmesi hedeflenmektedir.

"Endüstri 3.0", makineleşmiş sanayinin otomasyona dönüşümünü sağlamıştır. "Endüstri 4.0" ise otomatikleşmiş sanayinin dijital trendler ile yeni nesil teknolojileri bir araya getirmesiyle hibrit bir konsept ortaya koymaktadır. Tam aksine, "Tarım 3.0" mevzusunun arka planı pek doldurulmadan, "Tarım 4.0" konusu daha çok geçmeye başlamıştır. Bilindiği gibi, tarım sektörünün kendine has durumu, geleneksel yöntemlerden kopamayan süreçler ve hatta atadan dededen gözlemlenerek sürdürülen tekniklerin ihmal edilmemesini gerektirmektedir. Elbette tarım sektörü de "Tarım 3.0" süreçlerinden geçmiştir, makineleşme, otomatikleşme, dahası uzaktan algılama tekniklerine dayanan birçok faaliyet tarım için şüphesiz tecrübe edilip kayda geçen birikimlerdir. Özellikle gelişmiş ülkelerdeki bu dönüşüm sürecinde "Endüstri 4.0" ile kıyaslandığında bu sürecin "Tarım 4.0" noktasına ulaşmaya yakın olduğu söylenebilir. Benzer şekilde, son zamanlarda bahsi geçen diğer bir kavram olan "Akıllı Tarım" da bu kapsamda değerlendirilebilir. Açıkçası "Akıllı Tarım" kavramını "Hassas Tarım" dan ayrı tutmamak gerekir.

Hassas Tarım, önemli bir zihniyet değişimini kasteden "Reçeteli Tarım", "Yerine Göre Tarım", "Akıllı Tarım" gibi farklı farklı isimlerle anılmaktadır. Hassas Tarım şeklinde yaygın kullanılan bu kavram, öncelikle teknolojide güçlü olan ülkelerde görülen pratiklerin cazibesiyle, takip eden yıllarda da diğer ülkelere de

sıçramıştır. Bu tarımda dijital dönüşüm süreci olan Hassas Tarım; şehir planlanması ile ulaştırma, savunma sanayi ile meteoroloji gibi alanlarda şimdiye dek yoğun kullanılan teknoloji ve pratiklerin tarıma entegre edilmesidir. Hassas Tarımın; insanlığa tarımsal, teknik, çevre ve ekonomik açıdan yeni perspektifler sunduğu şu ifadelerle daha sarih izah edilmektedir (Öğüt, 2015):

- *Tarımsal Perspektif; bitkilerin özel isteklerine cevap verebilme,*
- *Teknik Perspektif; zamanın etkin kullanımı,*
- *Çevresel Perspektif; çevre dostu uygulamalar,*
- *Ekonomik Perspektif; tarımsal girdiler, emek ve suyun etkin kullanımını sağlayarak maliyeti azaltma ve üründe verim kalite artışı anlamına gelmektedir.*

Hassas tarımda asıl mesele, konvansiyonel tarım tarafından ihmal edilen zamansal ve mekânsal değişikliklerin yönetişimi gereksinimidir. Bu gereksinim; girdilerin yanlış ve aşırı kullanımının toprağa, suya ve havaya, yani daha geniş tabirle doğa ve çevreye uzanan tehlikenin limitlerini aşmasından zuhur etmektedir. Bu yüzden, çevreyi, iklimi ve toplumu ilgilendiren tüm disiplinlerin bu süreçlere katılımı zaruridir. Dolayısıyla hassas tarım; tek bir meslek disiplinin gayreti yerine disiplinler arası çalışmayı gerektiren bir alandır (Öğüt, 2015).

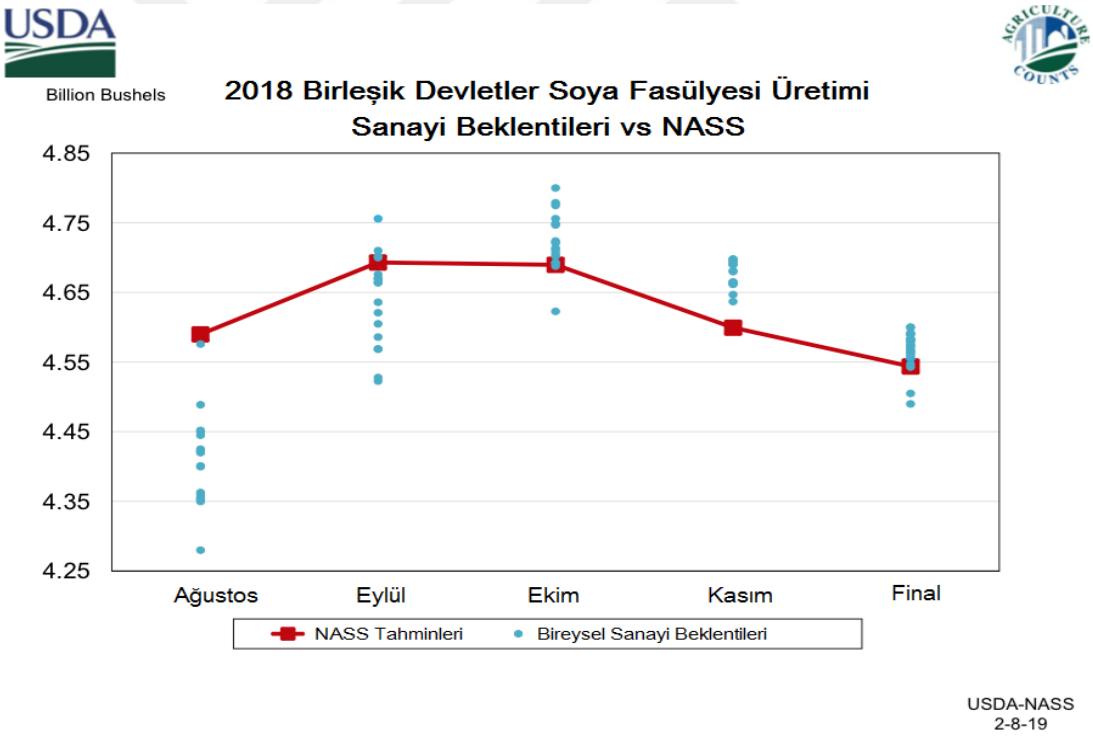
Tarım sektörü dijital dönüşüm dahilinde, hassas tarım ya da akıllı tarım gibi konseptlerle sürekli atılımlar yapsa bile, yeryüzündeki arazilerde üretilen gıda miktarı dünya nüfusunun önemli bir kısmını yeterli besleyememektedir. Şimdiye değin, gelişmiş ülkelerdeki nüfus ağırlıklı protein ile beslenirken, önümüzdeki yıllarda gelişmekte olan ülkelerden de artan gelirleri nispetince daha fazla protein talebi olacaktır. Sonrasında ortaya çıkacak üç temel sorun çözüm için göz önünde duracaktır: İlki tatlı su kaynaklarını etkin kullanmak, ikincisi tatlı su kaynaklarının %70 civarını tarımda kullanmak ve sonuncu ise küresel ısınma ile ona bağlı olan kuraklık olacaktır.

Bu sorunların çözümü için beliren fırsat ise, tarımda da 4. devrimin eşiğinde olmaya çok yaklaşılmış olmasıdır. Tarımda dijital gelişim süreciyle beraber büyük veri kullanımına dayanan performans artışı mümkün görünmektedir. Doğal olarak bu performans, verimlilik ile doğru orantılıdır ve verim artışı için bitkinin iyi tanınması gerekmektedir. Bitkinin gelişimi ise öncelikle dört temel girdiye bağlıdır: Bunlar, ısı, ışık, su ve besin olarak sayılmaktadır. Bitkinin tohumdan hasada kadar gelişimi, fenoloji olarak adlandırılmaktadır. Yani tohum ekilir, önce çimlenir, sonra çiçek açar ve meyve tutar, ardından da meyveler olgunlaşınca da hasat edilir. Bu durumun ortaya çıkardığı noktada nesnelerin interneti bazlı tarımsal sensörler kullanılarak tarla bazında rekolte tahmini yapılabilir (Doktar, 2019). Diğer bir tabirle, çiftçilerin eksik ve yanlış pratiklerine engel olduktan sonra, verimlerini yükseltmeleri sağlanabilir. Kısaca tarım sektörü, yeni nesil ve yıkıcı teknolojilere dayanan dijital dönüşümde geçiş dönemini tecrübe etmektedir.

Rekolte tahmin süreçlerinde ise, hasattan önce ürün rekoltesinin iyi tahmin edilmesi ise, özellikle iklim belirsizlikleri ile karakterize edilen bölgeler için hassas tarımın önemine işaret etmektedir. Bu durum, planlamacıların ve karar vericilerin, eksiklik durumunda ne kadar ithalat yapacaklarını veya isteğe bağlı olarak fazlalık durumunda ihracat yapabileceklerini göstermektedir. Ayrıca, hükümetlerin kıtlık zamanlarında yiyeceklerin yeniden dağıtılması için stratejik acil durum planlarını ayarlamalarını sağlar. Bu nedenle, ürün gelişiminin izlenmesinde erken rekolte tahmini için hassas tarımdan yararlanılması mevzusu lüzumlu hale gelmiştir. Dijital dönüşüm ise, erken ürün rekolte tahmini için kullanılabilecek objektif, standart ve muhtemelen daha ucuz / hızlı modern yöntemlere zorlamaktadır. Dolayısıyla hasattan önce rekolteyi yaklaşık tahmin etmek için birçok deneysel model geliştirilmektedir. Bununla birlikte, bu yöntemlerin çoğu, kolayca bulunamayan veriler gerektirmektedir. Modellerin karmaşıklığı, veri talepleri ve analiz yöntemleri, bu tür modelleri özellikle saha seviyesinde pratik yapmamaktadır.

2.1.4 Dünya'da ve Türkiye'de Rekolte Tahmin Süreçleri

Bazı gelişmekte olan ve birçok az gelişmiş ülke, ekonomik kalkınmaları açısından yanlış ürün rekolte çıktılarının sonuçlarını düzeltmeye çalışırken, hemen hemen bütün gelişmiş ülkeler planlanan rekolte; yani *"Potansiyel rekolte-Yp"* ile gerçekleşen rekolte; yani *"Fiili rekolte-Ya"* arasındaki boşluğa bakmaksızın daha iyi seviyede performans göstermektedir. Yine de, gelişmiş ülkeler de zaman zaman ürün rekolte tahmini ve tespitinde birtakım sorunlarla yüzleşmektedir. Hassas tarımda öncü bir model olan ABD bile, piyasa oyuncuları arasında netleştirilemeyen ürün rekolte sonuçları gibi bir durumla zaman zaman karşı karşıya kalmaktadır. Bu duruma şekil 2.1 ile örnek verilebilir:



Şekil 2.1. Soya fasulyesi üretimi üzerine NASS tahminleri ve Sanayi beklentileri – ABD (NASS, 2019)

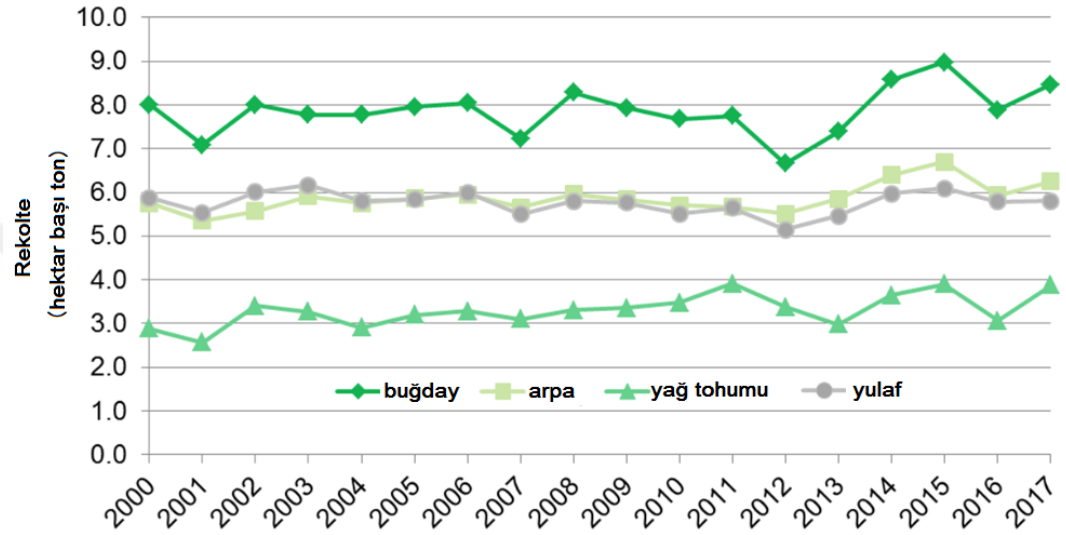
Amerika Birleşik Devletleri Tarım Bakanlığı (USDA), Ulusal Tarım İstatistikleri Servisi (NASS) aracılığıyla ürün rekoltesi ile ilgili tarımsal istatistiksel

verilerini sunmaktadır. USDA'nın kısmi ürün tahmin programındaki misyonu; ürün tahmin programı, çiftçilerin ekim yapma niyetini, fiilen ekilmesi ve hasat edilmesini beklediği mahsulleri, daha sonra da büyüme mevsiminde rekolte ve üretim tahminlerini raporlamaktadır. Ekinler toplandıktan sonra, hasat rekolteleri ve üretim tahminleri yapılır. Pazarlama yılı boyunca, ana ürünler için çiftlik içi ve çiftlik dışı stok tahminleri belirlenmektedir. Her Ocak ayı NASS, son 3 yılda başlıca ana ürünler için üretim ve değerleri gösteren iki rapor yayınlamaktadır. Yılın ortasındaki ve diğer üç aylık olasılık araştırmaları süresince, çiftliklerin rekoltesi, dönüm miktarı, üretimi ve tahıl stokları ile ilgili veriler toplanmaktadır. Çeyrekler arasında yapılan araştırmalar hasat koşulları ve rekolteler hakkında veri toplamak için kullanılır; ayrıca tarım dışı hububat stokları da ölçülmektedir (NASS, 2019).

USDA'nın 2018'deki aralık ayı raporu olan "Aralık ayı Tarımsal Araştırmaları" (DAS), belirli bir üretici listesinde bulunan ve ABD'deki tüm operasyonları seçme şansını gösteren yaklaşık 82.000 çiftlik işletmecisinden oluşan bir örneklem anketidir. Operatörlerden gelen veriler, 2018 mahsul yılı için ürünlerin rekoltesi ve üretimi hakkında bilgi edinmek için posta, internet, telefon veya kişisel görüşme yoluyla toplanmıştır. Ulusal ve eyalet düzeyinde çiftlik operatörünün raporladığı girdiler, tarihsel tahminleri ile tutarlılık ve karmaşıklık içinde analiz edildiler. Herhangi bir değişikliği meşrulaştırabilecek yeni bilgiler mevcutsa, bu rapordaki tahminler bir sonraki yılda revize edilebilir (USDA, 2018).

Sürdürülen diğer bir yerleşik tahmin sistemi olarak, Avustralya'nın rekolte tahmin programı üzerine de bahsedilebilir. Avustralya Tarım ve Kaynak Ekonomisi ve Bilimleri Bürosu (ABARES, 2018) proaktif yaklaşımla tahmin edilen ürün rekoltesi üzerinde çalışmaktadır. Avustralyalı çiftçiler ve yatırımcılar için düzenli olarak saha raporları ve analizleri hazırlarlar. Nispeten, Avrupa Birliği, mahsul üretim anketi konusundaki istatistiklerini EuroStat aracılığıyla sunmaktadır. Avrupa Birliği'ne üye ülkeler, Eurostat'ın "Yıllık Ürün İstatistikleri İçin El Kitabı"'na (EUROSTAT, 2018) uymaktadır. Brexit kararıyla birlikte Birleşik Krallık, EuroStat'ın AB-28 üyesi olan

diğer ülkeler tarafından karşılaştırmalı verileri yerine, Çevre, Gıda ve Köy İşleri Bakanlığı'nın ürün rekolte verisine odaklanmıştır. Bununla birlikte, İngiltere'de, Galler hesaplanmadığı için nihai sonuçları göstermemektedir. İngiltere rekolte tahmin sistemi bazı ürünler için uzun vadeli verileri sunmaktadır (Gov.uk, 2018). Şekil 2.2, İngiltere'de üretilen en popüler dört ürünün rekoltesini göstermektedir:



Şekil 2.2. Birleşik Krallık bazı belirli ürünlerin rekolte değerleri (DEFRA, 2018)

Hem tarım üreticisi hem de gelişmekte olan ülke olarak Türkiye, ürün rekolte tahmin belirlemesinde son günlerde bazı zorluklar yaşamaktadır. Aslında, Türkiye'de tarım sektöründe farklı güçlü oyuncular bulunmaktadır. Özellikle Türkiye'de resmi tarım kurumlarının yanı sıra; kooperatifler, dernekler, odalar ve emtia borsaları hem politika yapımında hem de ürün rekolte tahmini ve belirlenmesi konusunda önemli bir role sahiptir. Örneğin, sofralık zeytinleri daha iyi koşullarda yetiştirmek ve pazarlamak amacıyla, 1954 yılında bölge zeytin yetiştiricileri tarafından karşılıklı yardımlaşma ve işbirliği içinde kurulan Marmarabirlik; Tarım Satış Kooperatifleri Birliğidir (Marmarabirlik, 2019). Ürün rekolte tahmini ve tespiti konusundaki süreçlerine bakıldığında, ilk başta rekolte beyan kavramı dikkati çekecektir. Arazilerdeki ürün gelişimini izlemek ve belirlemek için Ulusal Zeytin/Zeytinyağı Konseyi, İl/İlçe Tarım Müdürlüğü ve Marmarabirlik'ten oluşan teknik bir ekip oluşturulur. Marmarabirlik, şu iki durum için de hassas davranmaktadır: Birincisi, bir taahhütle birlikte rekolte

beyanı, ikincisi ise kendi yetiştirme seviyesine göre gerçekçi bir taahhüttür. Mevcut dönemde ürün rekoltesi için taahhütte bulunduğunu beyan etmeyen herhangi bir ortağından zeytin almayı kabul etmemektedirler (Marmarabirlik, 2019).

Bunların haricinde, bazı aktörler de mahsulün ve bölgenin özelliklerine bağlı olarak rekolte tahmini ve tespiti konusunda inisiyatif almayı seçmektedir. TARBİL (Tarımsal İzleme ve Bilgi Sistemi), İTÜ UHUZAM (Uydu Haberleşmesi ve Uzaktan Algılama Merkezi) ile birlikte Tarım Bakanlığı'nın kurumsal niteliklerini bir araya getiren rekolte tahmin izleme konusunda güçlü bir platformdur. TARBİL, tarımsal üretimin hem gerçek zamanlı olarak izlenmesini hem de tahmin edilmesini yapabilmektedir. Ancak çalışma prensibi olarak hem merkezi altyapı gereksinimlerini hem de çiftçi, pazar ve hükümet arasındaki güven ve şeffaf uzlaşmanın sürekliliğini sağlamak zorundadır. Şekil 2.3'te TARBİL web sayfasından alınan gerçek zamanlı gözlem ve rekolte izleme sistemi arayüzü yer almaktadır (TARBİL, 2019):

Şekil 2.3. Gerçek Zamanlı Gözlem ve Rekolte İzleme Sistemi (TARBİL, 2019)

Türkiye'de rekolte tahmin süreçlerine katkı sunabilecek, aynı zamanda yerel ve kırsalda güçlü olan diğer aktörler ise; "Ticaret Borsaları", "Ziraat Odaları" ve "Ziraat Mühendisleri Odası" olarak sayılabilir.

2.2 Blokzincir Teknolojisi

Tüm Dünya'da internet erişiminin giderek yaygınlaşmasıyla birlikte, siber uzaydaki veri transferi de pek çok farklı amaçla yapılır hale gelmiştir. Blokzincir teknolojisi (BZT) de, bu veriler dışında kalan herkesin mutabık olduğu değerli görülen varlıkların transferini sağlayan bir tür dağıtık veritabanı olarak ortaya çıkmıştır. 2009 yılında BZT sayesinde dört farklı bilim alanı bir araya getirilmiştir. Veritabanı teorisi, Kriptografi, Ekonomi ve Para teorisi, Oyun teorisi olarak sayabileceğimiz bu bilimlerin hepsi mevcutta vardı, ancak hepsini bir arada kullanıp uyumlu bir ahenk göstermesi Bitcoin'in devrim niteliğinde olmasını sağladı (Tübitak BZLab, 12/5/2019). Sonrasında, Bitcoin ile dağıtık bir güven oluşturulup bankalardan bağımsız bir para transfer konsepti ortaya koyuldu.

2.2.1 Tarihsel Gelişimi

Blokzincir tarihi Bitcoin öncesi ve sonrası dönem olarak ikiye ayrılabilir. Blokzincirin tam olarak çalıştığının Bitcoin ile ispatlanmasının ardından, BZT'ye inanılmaya başlandığı için, Bitcoin ile ilgili 2008 yılında yazılan makale (Nakamoto, 2008), BZT için bir milat kabul edilebilir.

Bitcoin öncesinde Stuart Haber ve W.Scott Stornetta 1991 yılında dağıtık bilgisayarlara verinin kriptografi algoritmaları kullanılarak gönderilmesi konusunda çalışmalar yapmıştır. Blokların kriptografi algoritmalarıyla korunuyor olmaları, zaman damgalı olmaları günümüz blokzinciri teknolojisi ile bağdaşmaktadır (Haber ve Stornetta, 1990). Üstelik 1992 yılında, Merkle ağacı yapısını kullanan bloklar üzerinde daha çok veri depolaması başarılmıştır.

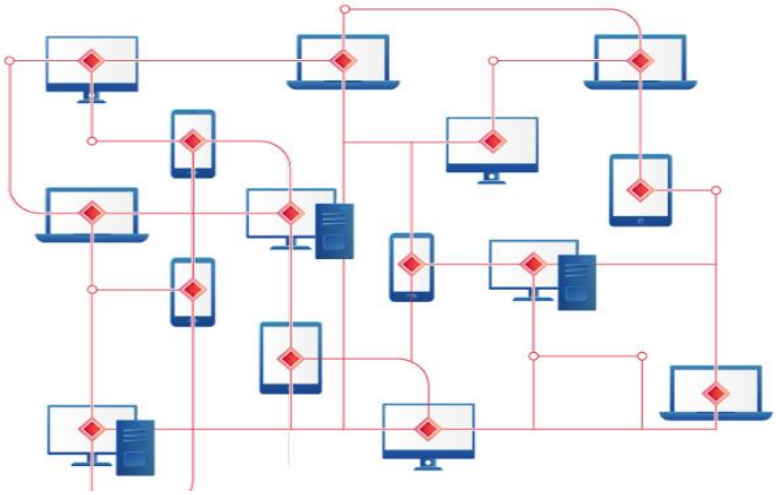
2008 yılında ise Satoshi Nakamoto rumuzlu kişi tarafından ortaya çıkarılan "*Bitcoin: Eşten Eşe Elektronik Nakit Sistemi*" adlı çalışmanın (Nakamoto, 2008) var olan bilim ve teknolojileri blokzincir kavramı altında bir araya getirmesiyle yeni bir teknoloji alanı hayat bulmuştur. Uçtan uca elektronik ödeme sistemi şeklinde kullanılabilecek öncü bir dijital veya kripto-para olarak tasarlanan Bitcoin; aracı olmadan, düşük komisyonlar ödenerek transfer yapabilmesi gücü nedeniyle, mevcut finans düzeni üzerinde yıkıcı ve dönüştürücü potansiyele sahip olduğu düşünülmektedir.

Blokzincir teknolojisine en büyük katkılardan birini sağlayan bir diğer çalışma ise Ethereum Blokzincir ağıdır. Ethereum Blokzinciri, üzerinde akıllı sözleşmeler ile birçok projenin çalıştırılabileceği büyük bir platform ağıdır. Bu teknoloji 2014 yılında fonlanmış ve 2015 yılında kullanılmaya başlanmıştır. Günümüzde birçok projeye üzerinde yer ve kaynak sağlayıp gelecekte Dünya'nın en büyük sanal makinesi olmayı hedeflemektedir.

2.2.2 Temel Kavramlar

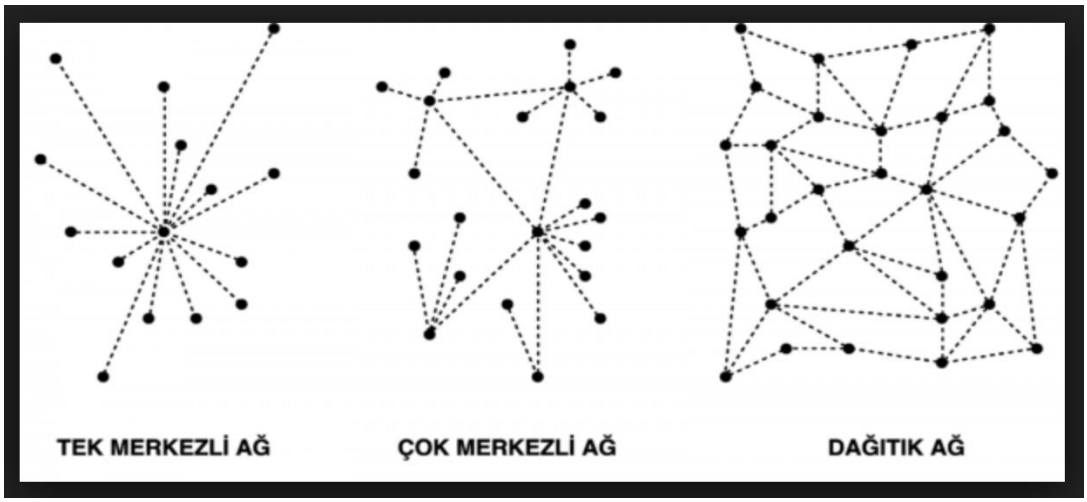
a.Uçtan Uca Ağ (Peer to Peer Network-P2P):

Blokzincir ağında bulunan uçlar (peer), sisteme dahil olan akıllı telefonunu, bilgisayarı ya da sunucuyu vb. temsil ederler. Uçtan uca ağ ise bu cihazların birbirleri arasında kurduğu ağ olarak tanımlanmaktadır. Şekil 2.4'de görüldüğü gibi BZT üzerinde, uçların dağılımı ve uçtan uca ağ yapısı aşağıdaki gibidir:



Şekil 2.4. Uçtan uca ağ (P2P Networks) yapısı (Lisk Academy, 2019)

Görüldüğü gibi, blokzincirde herhangi bir merkezi yapı ya da sunucu bulunmamaktadır. Aşağıdaki Şekil 2.5'te tek merkezli, çok merkezli ve dağıtık ağ arasındaki farkın gösterimine vurgu yapılmıştır.



Şekil 2.5. Verinin Tutulma Noktalarına Göre Ağ Çeşitleri (Usta ve Doğantekin, 2017)

b. Kayıtlar:

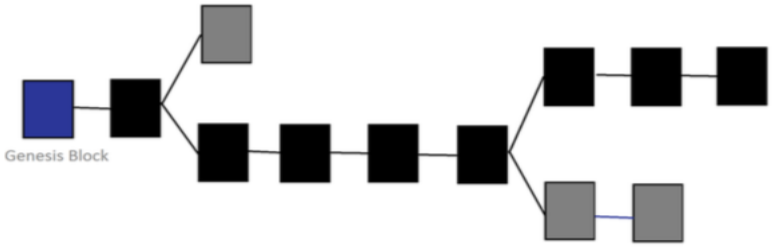
Blokzincir kayıtları, ait olduğu blokzincir ağında meydana çıkarılan her türlü içerik bilgisi gösterimi sunmaktadır. Bu içerikler tasarım şekline göre para transferi, müşteri kayıtları, demirbaş girdisi gibi değerler olabilir. Yeni transfer istekleri de sıraya konulduğunda, hemen sonraki işlem sıraya kaydedilip yerleşir.

c. İşlemler (Transactions):

İşlemler blok denilen dosyalarda depolanan veri yapılarıdır. Şifrelenmezler ve tipik olarak önceki işlemlere bağlanırlar, böylece bir zincir oluştururlar. Dijital para birimi sahibi, önceki işlemi açık anahtarı ile dijital olarak imzalar ve bunun dışında bir özet (hash) oluşturulur. Önceki işlemin sahibi daha sonra özeti kendi özel anahtarıyla imzalar.

d. Bloklar:

Blokzincir teknik olarak şimdiye kadar olan tüm işlemlerin kaydını sağlayan sıralı ve zaman damgalı bağlantılı bir bloklar listesidir. Bir zincirin ilk blokuna "genesis blok" adı verilir. Her blok birbirine matematiksel olarak bağlıdır. Örneğin, bir blok kendisinden önce gelen bloğun bilgilerinin özetini (hash) başlığında bulundurur. Bu şekilde zincir oluşmuş olur. Eğer zinciri bozan bir ihlal söz konusu ise, zincir oradan kopar ve başka bir yerden devam eder. Şekil 2.6'da genesis bloğu mavi, blokzincirin aktif blokları siyah olarak görülmektedir.



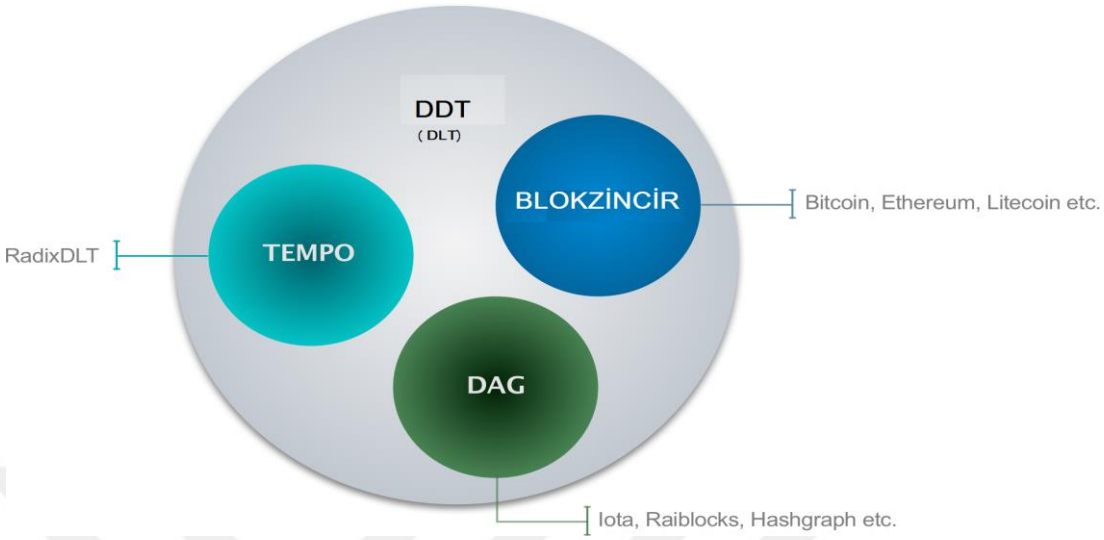
Şekil 2.6. Başlangıç (Genesis) Blok ve Zincirde Sıralanmış Bloklar

Bir bloğu tanımlamanın iki yolu vardır. İlk olarak, özet (hash) tarafındandır. Bu özet, her blok üretildiğinde ağdaki eş düğümler (peer nodes) tarafından hesaplanır. Özet, blokların daha hızlı indekslenmesi ve diskten alınması için bloğun meta verilerinde bulunan bir veritabanında saklanabilir. Bir bloğu tanımlamanın ikinci yolu, yüksekliği ile olacaktır. Başlangıç bloğunun yüksekliği 0'dır. Bu tanımlama yöntemi mutlak değildir, çünkü blokzincirdeki iki veya daha fazla blok aynı blok yüksekliğine sahip olabilir ve aynı yükseklikte iki bloğun aynı ebeveyne sahip olması da mümkündür.

e. Dağıtık Kayıt Defteri Teknolojisi (DDT):

BZT'nin en önemli noktalarından biri de dağıtık kayıt defterleri teknolojisini (DDT / DLT, Distributed Ledger Technology) kullanıyor olmasıdır. Dağıtık kayıt defterleri, verinin merkezi bir yerde saklanmasını engellemek maksadı ile ortaya atılmış, dağıtık bir yapıda verinin kaydedilmesi üzerine kurulmuş bir teknolojidir. Bu sayede verinin kaybolması, değiştirilmesi olasılığı düşmektedir.

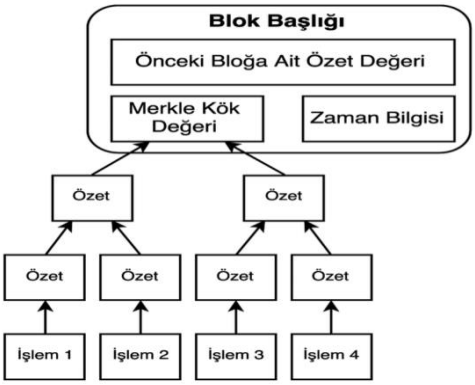
DDT'nin, BZT'den farkı kriptoloji altyapısının olmamasıdır. Şekil 2.7'de görüldüğü gibi aslında BZT, DDT'nin bir alt kümesidir.



Şekil 2.7. Blokzincir ve DDT Arasındaki Farklılığın Gösterimi (Mango Research, 2019)

f. Merkle Ağacı:

Blokzincirindeki her blok, işlem bilgilerini saklayan bir Merkle ağacı içerir. Merkle ağacı veya bir hash ağacı, büyük veri kümelerinin doğrulanmasına ve özetlenmesine yardımcı olan bir veri yapısıdır. Tüm işlemleri blokta verimli bir şekilde saklarlar ve kökleri bloktaki tüm işlemlerin bir karmasını içerir. Merkle ağaçları, çift SHA-256 hash kullanarak arka arkaya aşağıdan yukarıya doğru oluşturulur. Bu yüzden, bir Merkle ağacının yaprakları, işlemlerin kendisinden ziyade bir bloğa ait işlemlerin özetlerini depolar. Şekil 2.8'de bir blok başlığına, önceki işlemlerin özet olarak yazılması işlemi gösterilmiştir.



Şekil 2.8. Merkle Kök Değerinin blok başlığına yazılması (Teknochain, 2019)

2.2.3 Blokzincir Teknolojisi için Kriptografi Altyapısı

Blokzincirde Kriptografi, öncelikle iki amaç için kullanılır:

. İşlem gönderenin kimliğini güvence altına almak.
. Geçmiş kayıtların tahrif edilemeyeceğinden emin olmak.

BZT, tüm bilgileri ve değer depolarını güvence altına alırken işlemlerin güvenli bir şekilde yapılmasını sağlamak için kriptografiyi kullanır. Bu nedenle, blokzincir kullanan herkes bir kez zincir üzerine kaydedildiğinde, o kadar meşru ve güvenliği koruyacak şekilde yapıldığına tamamen güvenebilir.

Benzer bir çerçevede kurulmasına rağmen, blokzincirde kullanılan kriptografi türü, yani açık anahtar kriptografisi, teknoloji ile ilişkili fonksiyonlara simetrik anahtar kriptografiden çok daha uygundur.

a. Açık Anahtar Kriptografisi:

Asimetrik şifreleme olarak da bilinen açık anahtar kriptografisi, standart simetrik anahtar şifrelemesine nazaran, herkesle paylaşılabilen bir ortak anahtar aracılığıyla bilgilerin aktarılmasına olanak sağlayan bir ilerlemeyi temsil eder.

Simetrik anahtar şifrelemesinde olduğu gibi şifreleme ve şifre çözme için tek bir anahtar kullanmak yerine, ayrı anahtarlar (açık anahtar ve özel anahtar) kullanılır. Bir kullanıcının açık anahtarı ve özel anahtarın bir arada kullanılmasıyla bilgileri şifreler, alıcıların özel anahtarı ve gönderenin açık anahtarı şifresini çözer. Özel anahtarın açık anahtara dayanarak hesaplanması mümkün değildir. Bu nedenle, bir kullanıcı açık anahtarını birisinin özel anahtarına erişebileceğinden endişe etmeden herkese gönderebilir. Gönderen, yalnızca hedeflenen tarafın şifresini çözeceğinden emin olarak dosyaları şifreleyebilir.

Ayrıca, açık anahtarlı şifreleme ile gösterilen verilerin bütünlüğünü güvence altına alan dijital bir imza üretilir. Bu, bir kullanıcının özel anahtarını imzalamak istedikleri verilerle matematiksel bir algoritma kullanarak birleştirerek yapılır. Gerçek verilerin kendisi dijital imzanın bir parçası olduğu için, herhangi bir kısmı tahrif edilmişse, ağ geçerli olduğunu kabul etmeyecektir. Verinin en ufak bir kısmını bile düzenlemek, tüm imzayı yeniden şekillendirir, yanlış ve eskimiş yapar. Bu sayede BZT, üzerine kaydedilmiş herhangi bir verinin doğru, doğru ve etiketsiz olduğunu garanti eder.

b. Dijital İmza:

Dijital imzalar, blokzincir üzerine kaydedilen verilerin güvenliğini ve bütünlüğünü sağlamanın ana yönlerinden biridir. Bunlar, temel olarak işlemlerin ve işlem bloklarının güvence altına alınması, bilgi aktarımı, sözleşme yönetimi ve herhangi bir dış kurcalamanın tespit edilmesi ve önlenmesinin önemli olduğu diğer durumlar için kullanılan standart bir güvenlik protokolüdür. Dijital imzalar asimetrik kriptografi kullanır, bu da bilgilerin açık anahtar kullanılarak herkesle paylaşılabileceği anlamına gelir.

Dijital imzalar, blokzincirde bilginin saklanması ve aktarılması için üç önemli avantaj sağlar. Her şeyden önce bütünlüğü garanti ederler. Teorik olarak, gönderilen veriler zorunlu olarak bir bilgisayar korsanı tarafından görülmeden bile değiştirilebilir. Bununla birlikte, bu durum dijital imza ile birlikte gelen verilerde gerçekleşirse, imza geçersiz hale gelir. Bu nedenle şifrelenmiş ve dijital olarak imzalanmış verilerin görülmesi sadece güven sağlamaz, aynı zamanda tahrif edilmiş olup olmadığını ve bozulmadığını ortaya çıkarır.

Dijital imzalar yalnızca verileri güvence altına almakla kalmaz aynı zamanda gönderen kişinin kimliğini de güvence altına alır. Dijital bir imzanın mülkiyeti her zaman belirli bir kullanıcıya bağlıdır ve bu nedenle, istedikleri kişiyle iletişim kurduğundan emin olabiliriz. Örneğin, en yetkin siber korsan bile başkasını para göndermeye ikna etme aracı olarak başka birinin dijital imzasını taklit edememiştir, bu basitçe matematiksel olarak imkanlar dahilinde değildir. Bu nedenle, dijital imzalar yalnızca iletilen verileri değil, aynı zamanda onu ileten bireyin kimliğini de garanti eder.

Dijital imzalar imzalayana özeldir ve üç algoritma kullanılarak oluşturulur:

. Özel ve açık anahtar sağlayan bir anahtar üretme algoritması,
. İmza oluşturmak için verileri ve özel anahtarı birleştiren bir imza algoritması,

. İmzaları doğrulayan ve mesajın orijinal olup olmadığını belirleyen bir algoritma ile mesaja, açık anahtara ve imzaya dayalı olup olmadığını belirler.

BZT kullanırken, bir kullanıcının bir açık anahtarı ve her ikisi de rastgele sayılar ve harflerin dizeleri olarak görünen özel bir anahtarı vardır. Açık anahtar bir e-posta adresiyle, onun giriş şifresi de özel bir anahtarla karşılaştırılabilir. Özel bir anahtarı asla kimseyle paylaşmamak gerekir. Özel anahtarın güvenli bir yere yazılması ve saklanması aynı derecede önemlidir. İdeal olarak, bir kağıt parçası veya donanım cüzdanı üzerinde, bu ikisini birden kırmak neredeyse imkansızdır. Özel anahtarların metin belgelerinde veya notlarda saklanması tavsiye edilmez, çünkü bunlar nispeten kolay kırılabilir. Bu yüzden "Özel Anahtarımı Unuttum" opsiyonu mevcut olamaz. Çünkü özel anahtar kaybolursa, anahtar tarafından kontrol edilen her şey de kaybolur.

2.2.4 Mutabakat Protokolleri

Mutabakat protokolleri, BZT'nin en önemli ve devrimci yönlerinden biridir. Bu protokoller, sistemin sömürülmesini engellerken, dağıtılmış bir ağdaki çeşitli cihazlar arasında reddedilemez bir anlaşma sistemi yaratır. Blokzincir mutabakat protokolleri, bir ağdaki tüm düğümleri birbirleriyle senkronize tutan, soruyu cevaplayan şeydir: gerçeğin ne olduğu konusunda hemfikir olduğumuzdan nasıl emin olabiliriz? Sonuçta, herhangi biri bir blokzincirde saklanacak bilgileri gönderebilir ve bu nedenle, bu bilginin eklenip eklenmeyeceği konusunda bir fikir birliği şeklinde gözden geçirme ve onaylama yapılması önemlidir.

Protokol, düğümler gibi elektronik cihazlar arasında veri iletişiminin ve iletiminin nasıl çalışması gerektiğini açıklayan bir kurallar kümesidir. Bu kurallar, herhangi bir veri gönderilmeden önce tanımlanmalı, bilgilerin nasıl yapılandırılacağına ve her cihazın onu nasıl göndereceğine veya alacağına dair

detaylar verilmelidir. Mutabakat, dağıtık sistemlerde, hesaplama amaçları için gereken belirli bir değer üzerinde karşılıklı olarak anlaşmaya varmak için iki veya daha fazla aracı gerektiren temel bir problemdir. Bu aracıların bazıları güvenilir olmayabilir ve bu nedenle konsensüs sürecinin güvenilir olması gerekir.

Bir terim olarak, "mutabakat"; ağdaki düğümlerin kendi kendini denetleyen ekosisteme sahip bir blokzincir ağı ile aynı fikirde olduğu anlamına gelir. Bu, iki temel işlevi yerine getiren teknolojinin kesinlikle çok önemli bir yanıdır. İlk olarak, mutabakat protokolleri bir blokzincirin güncellenmesine izin verirken, zincirdeki her bloğun doğru olmasını sağlamanın yanı sıra katılımcıları teşvik etmeyi sağlar. İkincisi, herhangi bir kuruluşun tüm blokzincir sistemini kontrol etmesini veya çıkarmasını önler. Mutabakat ya da Konsensüs kurallarının amacı, tek bir zincirin kullanılmasını ve izlenmesini sağlamaktır.

Mutabakat kuralları ise, ağdaki düğümlerin söz konusu bloğu ve içindeki işlemleri doğrularken bloğun izlemesini sağlayacak belirli bir kurallar kümesidir. Bir konsensüs elde etmenin kilit şartı, ağdaki düğümler arasında tek bir veri değeri için bir oybirliği kabulüdür, hatta bazı düğümlerin başarısız olması veya güvenilmez olması durumunda bile böyledir (Lisk Academy, 2019).

Her kripto para birimi blokzincirinin saldırılara karşı korumanın bir yolu olmalıdır. Örneğin, bir saldırgan biraz para harcamayı deneyebilir ve daha sonra işlemi içermeyen bu blokzincirin kendi versiyonunu yayınlayarak işlemi tersine çevirebilir. Bu çifte harcama olarak bilinir. BZT güvenlik için merkezi bir otoriteye dayanmadığından, kullanıcılar kaydın hangi versiyonunun geçerli olduğunu önceden bilmezler. Mutabakat protokolleri ayrıca, ağda devam etmeleri için ödülleri ve teşvikleri olan bir blokzinciri koruyan katılımcıları da motive eder. Bu ödüller, son derece kazançlı olabilen kriptopara birimleri veya jetonlar şeklinde gelir, öyle ki, bir zincirdeki bir sonraki bloğu onaylamak için rekabet son derece şiddetlidir.

Mutabakat protokolleri, zaman ve ihtiyaç duyulan bilgi işlem kaynaklarını veya belirli bir kripto para birimini elinde bulundurmak için oldukça masraflı olmak suretiyle taklit edilmesi veya kopyalanması zor olacak şekilde tasarlanmıştır. Mutabakat yöntemleri, içindeki blokları doğruladıkları blokzincirine bağlı olarak değişir ve en etkili ve verimli yöntemin ne olduğuna dair sürekli bir tartışma ile çeşitli fikir birliği biçimleri oluşur.

Blokzincir mutabakat modelleri, çevrimiçi dünyada istikrar ve uygunluk oluşturma stratejileridir. Bu anlayış için kullanılan fikir birliği çerçeveleri bir konsensüs hipotezi olarak bilinir (Pahlajani ve ark., 2019). Mutabakat algoritmaları ise, ispat temelli ve oylama temelli olmak üzere iki türlüdür. Bunlara aşağıdaki bölümlerde değinilecektir.

a. İspat Tabanlı Mutabakat Algoritmaları

İspat tabanlı mutabakat algoritmasında, ağa katılan düğümlerin bloğu ekleme hakkını elde etmek için bir şifreleme problemini çözmesi gerekir. Açık blokzincirde, düğümler bloğu blokzincire ekledikten sonra ödüller kazanır. İspat temelli algoritmanın ilk versiyonu Satoshi Nakamoto (Nakamoto, 2008) tarafından önerilen "İşin İspatı" algoritmasıdır. Bugüne kadar, aşağıda yer alan ispat temelli mutabakat protokol versiyonları kullanılmıştır.

. İşin ispatı: Matematiksel bir bulmacayı çözmek,
. Hissenin ispatı: Blokzincirde daha fazla hisseye sahip olmak,
. Geçen sürenin ispatı: Zamanlama ile ayarlanmış zaman-aşımı süresi,
. Boşluk alan ispatı: Daha büyük boyutlu bir sabit disk gerekir.

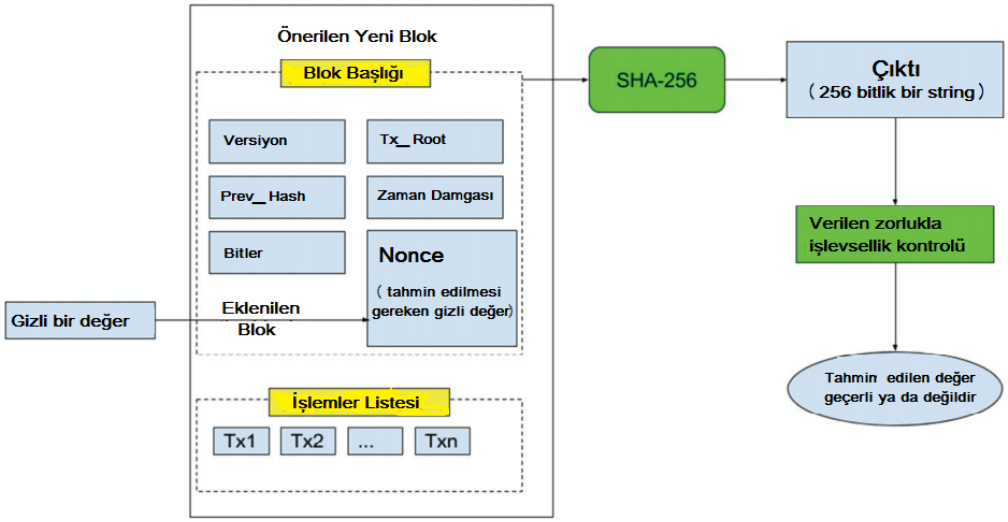
İlaveten, bunların hibrit versiyonları, yani yukarıdaki mutabakat tiplerinden herhangi birinin kombinasyonu olarak düşünülebilir.

İşin İspatı (Proof of Work – PoW):

Dağıtık bir ağdaki cihazlar arasında mutabakata varmak için "İşin İspatı" protokolünü oluşturmak, tartışmasız Bitcoin kurucusu Satoshi Nakamoto'nun başarısıdır. Bunu yaparken, blokzincir gibi devrimci bir teknolojinin de temelini atmıştır. "İşin ispatı" matematiksel bir soruna cevap olarak gelir; bu, ulaşılması gereken önemli bir çalışmayı gerektirir, ancak cevaba ulaşıldığında doğru olduğu kolayca doğrulanır.

Bu matematiksel bilmeceleri çözmenin tek yolu, ağdaki düğümler aracılığıyla, deneme yanılmalarına cevap vererek uzun ve rastgele bir süreç yürütmektir. Teknik olarak bu durum, problemin çözümü pratikte imkansız olmasına rağmen, ilk denemede çözülebileceği anlamına gelir. Bu sorunun cevabı, 'hedef özet' olarak bilinen kabul edilmesi gereken bloğun özet değerinden daha küçük bir sayı olmalıdır.

Hedef özet, özetlenmiş bir bloğun başlığının, bir madenciye verilecek ödül ile birlikte yeni bir bloğa eşit veya daha az olması gereken bir sayıdır. Hedef ne kadar düşükse, blok oluşturmak o kadar zor olur. Bir madenci, uygun bir değer üretilinceye kadar farklı benzersiz değerleri (nonce olarak bilinir) test etmeye devam eder. Bilmeceyi çözmeyi başarabilen madenci, bir sonraki bloğu zincire ekleyerek ve içindeki işlemleri onaylayarak blokla ilişkilendirilen ödülü alır.



Şekil 2.9. İşin İspatı (PoW) protokolü (Pahlajani ve ark., 2019)

Şekil 2.9'da gösterildiği gibi, düğüm / madenci tarafından gizli bir değer hesaplanacaktır (Pahlajani ve ark., 2019). Nonce denilen bir değerin tahmin edilmesinden sonra, SHA-256'nın yardımı ile özetleme yapılır ve verilen zorluk seviyesi ile çıktı kontrol edilir. Eğer özet değeri kabul edilirse, nonce de doğru tahmin edilir, aksi halde tüm süreç tekrarlanır, yani doğru olanı buluncaya kadar başka bir nonce değeri tahmin edilir. Doğru nonce değeri bulunduktan sonra, blokların özet değerini ve nonce değerini ağda diğer düğümlere doğrulatmak ve kendi defterlerine eklemek için yayınlamalarına izin verilir. PoW'un olumlu tarafı oldukça güvenli olmasıdır ve olumsuz tarafı ise yüksek işlem gücü gerektirmesidir. Dezavantajları nedeniyle "Hissenin ispatı" ve daha birçok ispat temelli mutabakat algoritması geliştirilmiştir.

b. Oylama Tabanlı Mutabakat Algoritmaları

Oylama mutabakat algoritması, düğümlerin bilindiği özel blokzincir ağlarında tercih edilir. Düğümlerin düzenli olarak kontrol sistemine katılmalarına ve geri

çekilmelerine bu algoritma tiplerinde izin verilmesi, ispat bazlı mutabakat hesaplamaları ile karşılaştırıldığı temel noktadır. Oy tabanlı mutabakatta, bloğu blokzincire eklemeden önce sonuçların ağda paylaşılması gerekir. Bir eş (peer) zincire bir blok eklemek isterse, en azından x'in (x eşik değeridir) eşlerin üzerinde hemfikir olduğuna dair bir kontrol yapılmalıdır. Başarısız (f) düğümleri varsa, o zaman bir karar için başarısız düğüm artı bir (f+1) çalıştırılabilir olmalıdır.

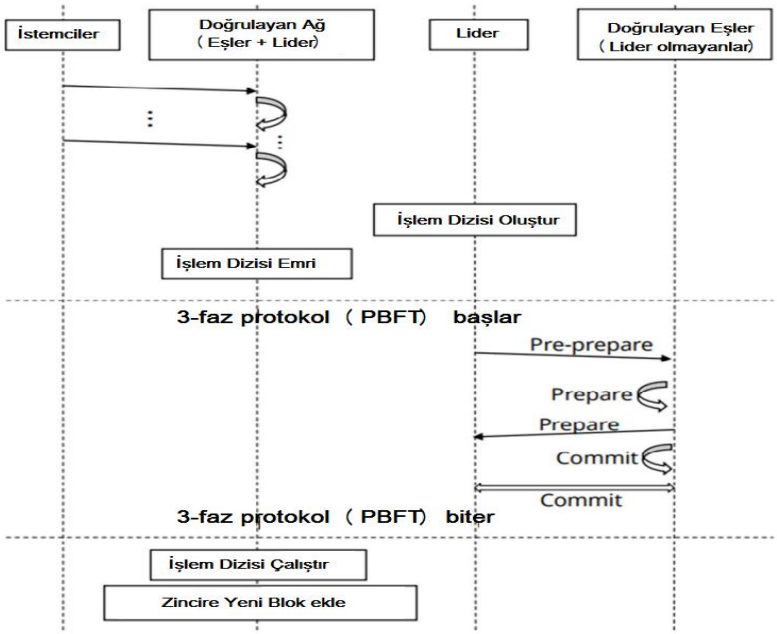
Oylama tabanlı mutabakat algoritmalarının çalıştırılması, dağıtık sistemde kullanılan hataları tolere etmek için geleneksel yöntemlere çok benzer. Bu nedenle, oylamaya dayalı bir konsensüs bazı kötü durumlara direnecek şekilde tasarlanmalıdır. Sonuç olarak, bu kötü durumlara dayanarak, oylamaya dayalı mutabakat algoritmaları iki ana tür altında sınıflandırılabilir:

. Bizans hata tolerans bazlı mutabakat: düğümlerin çökmesini ve bozulan düğümlerin sorunlarını önleyebilecek bir tür uzlaşma, (BFT, PBFT)
. Çökme hata tolerans bazlı mutabakat: sadece çöken düğümlerin sorunlarını önleyebilecek bir tür uzlaşma, (Paxos, Raft)

I. Bizans Hata Toleransı Tabanlı Mutabakat (BFT - PBFT):

Pratik Bizans Hata Toleransı (PBFT), BFT'nin optimizasyonlarından biridir ve Miguel Castro ve Barbara Liskov tarafından 1999 yılında "Pratik Bizans Hata Toleransı" başlıklı bir akademik makalede tanıtılmıştır (Castro ve Liskov, 1999). Orijinal BFT fikir birliği mekanizmalarını iyileştirmeyi hedeflemektedir ve bazı popüler blokzincir platformları da dahil olmak üzere birçok modern dağıtık bilgisayar sisteminde uygulanmış ve geliştirilmiştir.

PBFT'de iki tür düğüm vardır: Bir lider düğüm ve bazı onaylayıcı eşler (düğümler); ve bu eşler, Şekil 2.10'da (Sukhwani ve ark., 2017) açıklanan zincire bir blok eklemek için bazı turlar gerçekleştireceklerdir. Başlangıçta, istemciler işlem taleplerini ilgili onaylayan eşlerine gönderirler. Buradan, alıcı eş işlemleri doğrular, ardından lider de dahil olmak üzere diğer eşlere yayınlar. İşlem sayısı parti büyüklüğü denilen bir eşiğe ulaştığında veya bir aralıktan sonra, lider düğüm işlemleri oluşturdukları süreye göre sıralayarak blok haline getirir. Daha sonra, üç faz PBFT yürütülür:



Şekil 2.10. Hyperledger Fabric'de PBFT mutabakat süreci kontrolleri (Sukhwani ve ark., 2017)

II. Çökme Hata Tolerans Tabanlı Mutabakat (Paxos – Raft):

Paxos (Lamport, 2001) adlı klasik ve anlaşılması zor mutabakat algoritması tarafından motive edilen Raft (Ongaro ve Ousterhout, 2014), Quorum (Baliga ve ark., 2018) tarafından çökmelerine tolerans göstermek için kullanılan bir mutabakat

algoritmasıdır. Paxos'tan farklı olarak Raft, pratik sistemlerde anlaşılması ve kullanılması daha kolay olacak şekilde meydana getirildi. Paxos gibi, Raft da her seferinde toplam düğümlerin [n/2 + 1] normal çalıştığı varsayımına dayanır.

Raft temelli mutabakat mekanizması, Bizans hatasının gerekli olmadığı özel blokzincirde, daha hızlı blok oluşturma ve işlem kesinliği için kullanılır. Talep üzerine bloklar oluşturur ve kopyalanan log kaydını yönetir. RPC çağrılarını kullanarak iletişim kurar (Ongaro ve Ousterhout, 2014). Raft'ta üç tip eş vardır:

. Takipçi
. Aday
. Lider

Şekil 2.11. Raft'ta düğümün rol geçişleri (Ongaro ve Ousterhout, 2014)

Şekil 2.11, düğümlerin rollerini farklı durumlarla nasıl değiştirdiğini açıklamaktadır. Temel olarak, bir düğüm sahibi lider rolünün görev süresinin sonuna kadar sorumluluğunu elinde tutacağı, ardından izleyici rolüne geri döneceği sıralı olarak numaralandırılmış bazı zaman periyotları olacaktır.

2.3 Akıllı Sözleşmeler

Akıllı sözleşme, yasal sözleşmelerin yerini almayı amaçlayan kendi kendini zorlayan ve kalıcı bilgisayar yazılımları oluşturmak için 1994 yılında Nick Szabo tarafından geliştirilen teorik bir konsepttir (Szabo, 1994). Onun açıklamasına göre;

"Akıllı bir sözleşme, bir sözleşmenin koşullarını yerine getiren bilgisayarlı bir işlem protokolüdür. Genel hedefler, müşterek sözleşme şartlarını (ödeme koşulları, hacizler ve hatta yaptırım gibi) yerine getirmek, hem kötücül hem de kazara olan istisnaları en aza indirmek ve güvenilir aracılara duyulan ihtiyacı asgariye indirgemektir. İlgili iktisadi hedefler arasında usulsüzlük, tahkim ve yaptırım maliyetlerini ve diğer işlem masraflarını azaltmak yer almaktadır."

Akıllı Mülkiyet ise, akıllı sözleşmeler kullanılarak kontrol edilen mülktür. Bu mülk, ev veya kutu gibi fiziksel şeyler veya pazar payları gibi fiziksel olmayan bir varlık veya hatta bir dosya sunucusuna verilen izinler olabilir. Akıllı mülkün temel işlevi, güvenilir bir şekilde ele alınabilmesidir. Mülkiyetin akıllı hale getirilmesi, daha az güven ile işlem görmesini sağlar. Bu durum, dolandırıcılık ve arabuluculuk ücretlerini azaltır ve başka türlü gerçekleşmeyecek olan işlemlerin yapılmasını sağlar. Örneğin, yabancılara teminat olarak akıllı mülkünüzü teminat alarak, internet üzerinden borç para vermenizi sağlar; bu da borç vermeyi daha rekabetçi hale getirebilir ve böylece kredi kullandırmayı daha ucuz hale getirmek mümkündür (Bitcoin.it Wiki, 2019).

Akıllı mülkün ilkel biçimleri bir süredir zaten yaygındı. Mesela, bir araba satın alırsanız, muhtemelen mekanik ve otomobilin elektrik devresini hırsızlığa karşı kilitleyen kriptolu bir elektronik sistem olan akıllı kumanda (immobilizer) ile birlikte gelmektedir. Immobilizer anahtarı, yalnızca doğru şifreleme belirtecinin motoru çalıştırabilmesini sağlayan bir protokol değişimi ile güçlendirilir. Bu sistem sayesinde

araba hırsızlığı önemli ölçüde azaltılmıştır. Örneğin, Interpol verilerine göre 2008 yılında 4.2 milyon araç hırsızlığı mevcut iken (Abuzalata ve ark., 2012), 2011 yılında yapılan çalışmada immobilizerin artışıyla araç hırsızlığı %9.8'den %5.2'ye kadar düşmüştür (Farrell ve ark., 2011). Bunlar kriptografi için zafer olsa da, kriptografik olarak bu aktif özelliklerin potansiyeli tam olarak araştırılmamıştır.

2.3.1 Teori

Bu bölümde Bitcoin blokzincir protokolünün bilindiğini ve sözleşmelerin iyi anlaşıldığını varsayarak bir örnek üzerinde teoriyi güçlendirelim:

Araba örneği ile devam edelim; bir mülkiyet anahtarı kullanarak kimlik doğrulaması arabanın bilgisayarı için gereklidir. Mülkiyet anahtarı ise düzenli bir Bitcoin ECDSA-256 anahtarıdır. Bu anahtara *T* miktarı olarak isimlendirilen küçük bir miktar Bitcoin yatırılır (örneğin, 0.0001 BTC olabilir). İlaveten, otomobilin üreticisinin dijital bir sertifikası ve sertifikada açık kısmı olan bir tanımlama anahtarı vardır. Bu, otomobilin varlığı, yaşı veya kilometresi gibi şeylerin üçüncü şahıslara kanıtlanmasını sağlar (Bitcoin.it Wiki, 2019).

Otomobil satıldığında, aşağıdaki protokol kullanılır:

i. Alıcı tek seferlik bir anahtar (nonce - rastgele sayı) üretir ve satıcıdan onlara araç verilerini göndermesini ister.

ii. Satıcı araca tek kullanımlık anahtarını verir ve araç kimlik anahtarıyla imzalanmış bir veri yapısı döndürür. Veriler, tek kullanımlık anahtarı, araba açık sertifikasını, araba hakkındaki verileri, mevcut sahibin açık anahtarını ve

mülkiyeti en son devretmiş olan merkle ağacıyla işlemleri içerir. Bu, alıcının ne aldığını ve gerçek satıcıdan geldiğini bilmesini sağlar (bir tekrarlama olmadan).

iii. Satıcı ödemeyi almak için bir anahtar olan k_1 seçer ve fiyatı *P* olarak isimlendirir.

iv. Alıcı yeni bir sahiplik anahtarı k_2 üretir.

v. Alıcı, iki giriş ve iki çıkış ile bir işlem yaratır. *P* fiyatı (koin) için ilk girdiyi imzalar. İkinci girdi, sahiplik adresi için *T* koinlerini tutan çıktıya bağlanır. İlk çıktı *P*'yi k_1'e, ikinci çıktı da *T*'yi k_2'ye gönderir. Bu işlem yalnızca ilk girdi imzalanabildiği için geçerli değildir. Alıcı bu kısmen tamamlanmış işlemi satıcıya iletir ve ardından ikinci girişi otomobilin mevcut sahiplik anahtarıyla imzalar ve işlemi yayınlar.

vi. Daha sonra onlar bazı onayları beklerler.

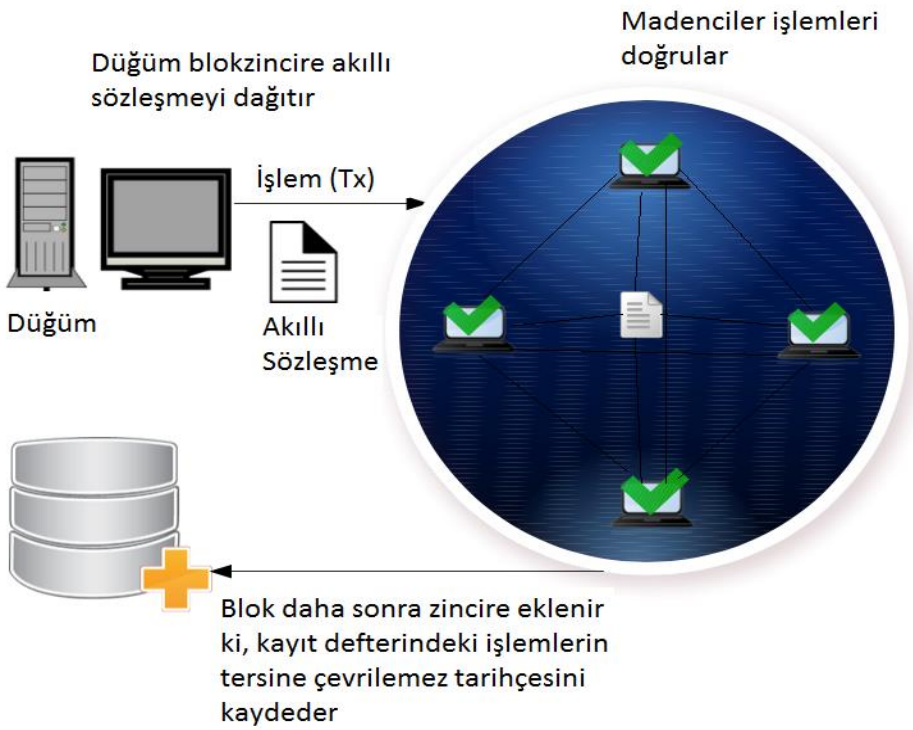
vii. Alıcı Bitcoin işlemiyle otomobili, onu blok başlığına bağlayan bir merkle ağaç dalı ve daha sonra otomobillerin şu anki mülkiyet işlemindeki boşluğu doldurmaya yetecek kadar blok başlığı sunar. Otomobil, yeni işlemin mülkiyeti yeniden devraldığını ve zincirinde mevcut olandan daha ileride olduğunu görür, üstelik *Tx*'in (işlem) tersine çevrilmeyeceğinden emin olmak için üste yığılmış yeterli işi vardır. Daha sonra sahiplik bilgilerini günceller. Otomobilin, ne zincirin tam bir kaydını ne de tüm başlıklarını tutması gerekmez, fakat gelecekte blok başlıklarını önceden sunulmuş olana bağlayabilecek kadar veri yeterlidir.

Uygulamada, bu işlem muhtemelen NFC donanımı olan akıllı telefonlar kullanılarak ele alınacaktır - kontrol paneline mülkiyet anahtarını içeren telefona dokunma işlemi, cüzdan uygulamasına fiyat girdikten sonra akıllı mülkiyet işlemlerinin nasıl yapılacağını bilen özel bir modda başlatır. Alıcı ve satıcı daha sonra

anlaşmayı sonuçlandırmak için telefonlarına dokunacaktır. Kriptografi karmaşık olmasına rağmen, onların bunun hakkında hiçbir şey bilmeleri gerekmez.

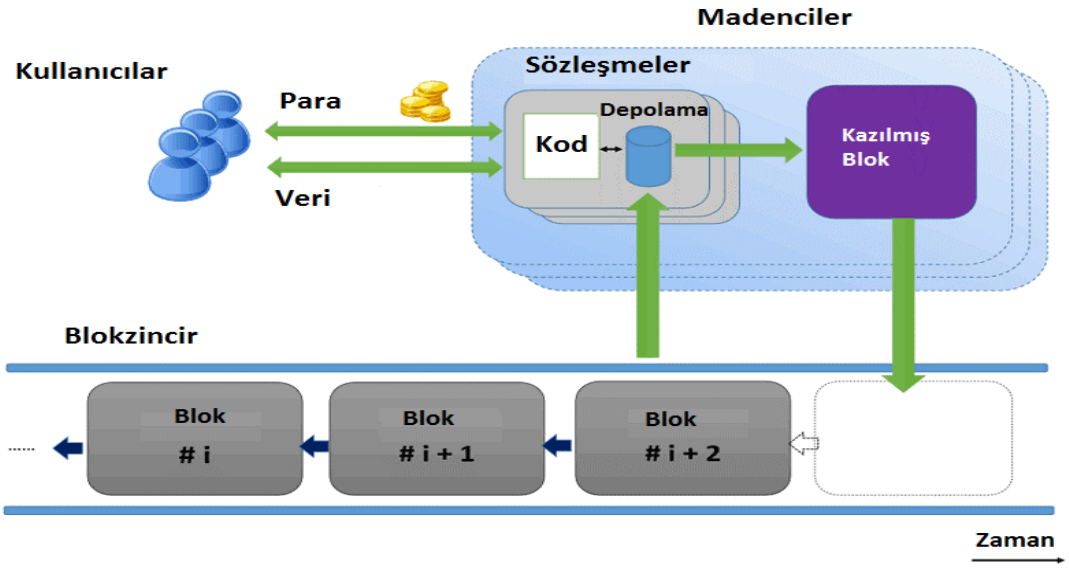
2.3.2 Bitcoin Blokzincirden İtibaren Akıllı Sözleşmeler

Blokzincir ağı üzerinde yer alan akıllı bir sözleşme denildiğinde, her iki tarafın da birbirine güvenme şartı olmadan düğümler ve blokzincir ağı arasında servis verebilecek dağıtık bir sözleşme olduğu anlaşılmış olur. Blok doğrulama işlemi sırasında her madenci, mevcut sözleşmeye göre işlemlerden sorumlu akıllı sözleşme kodunun bir kısmını doğrulamaya çalışır. Şekil 2.12, akıllı bir sözleşmenin blokzincir ağında nasıl bulunduğunu göstermektedir. Akıllı sözleşmeler, geleneksel sözleşmelerden, düşük yasal işlem maliyetleri taşıdıkları anlamında öne çıkmakta ve kullanıcılar için giriş bariyerini düşürebilmektedir.



Şekil 2.12. Blokzincirde akıllı sözleşmelerin yerleşim ve dağıtımı (Bagchi, 2017)

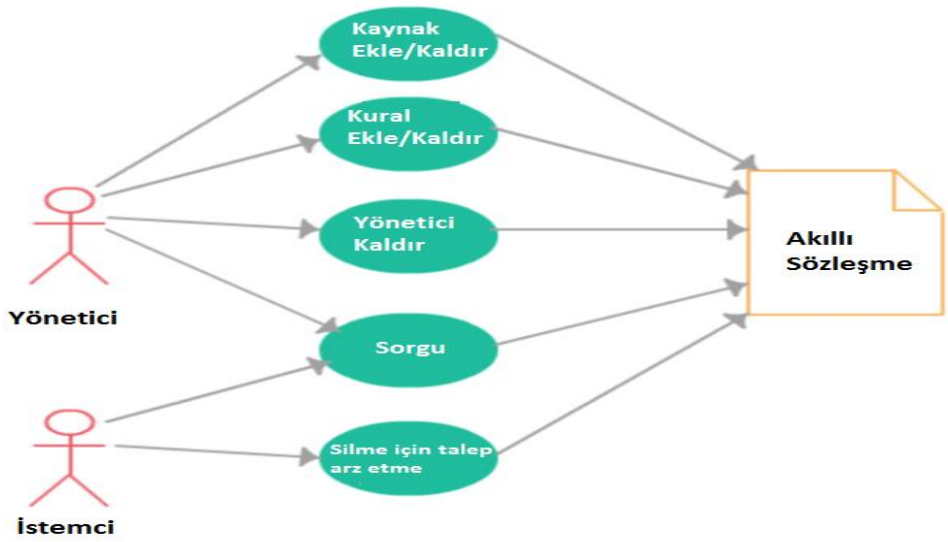
Bir sözleşme; bir kod, dahili depolama ve hesap bakiyesinden oluşur. Bir sözleşmenin durumu, sözleşmenin bakiyesinden ve dahili depolamadan oluşur. Sözleşme her çağrıldığında durum güncellenir. Şekil 2.13 böyle bir sözleşmeyi göstermektedir. Kullanıcılar sözleşme adresine işlemleri ve veriyi göndererek sözleşmeyi çağırırlar, Şekil 2.13'deki paranın, bu durumda bir işlem yoluyla her türlü (kripto) para birimi anlamına gelebileceği unutulmamalıdır. Madenciler, sözleşme işlemlerini normal işlemlerle aynı şekilde ele almaktadır. Sözleşme kodunda, hesap, kodunu etkinleştiren bir ileti aldığında, dahili depolamaya okuma ve yazma ve başka mesajlar gönderme veya sırayla sözleşme oluşturma olanağı sağlayan bir mesaj alır. Sözleşmeler yerine getirilecek bir şey olarak görülmemeli, daha sonra bir mesaj alırken daima kendi kendine bir dengeyi ve kalıcı değişkenleri takip etmek için anahtar / değer deposunu takip ederek her zaman belirli bir kod parçasını uygulayan otonom aracılar olarak görülmelidir.



Şekil 2.13. Blokzincir üzerinde Akıllı sözleşmelerin farklı bir gösterimi (Boogaard, 2018)

Genellikle kişilerin kullandığı cihaz ya da kaynaklar büyük ölçüde kısıtlı olduklarından, blokzincirinin bir kopyasını sistemlerinde saklama kabiliyetine sahip değillerdir, dolayısıyla blokzincir ağına kendileri katılamamaktadırlar. Bunun yerine, yönetici olarak adlandırılan, ağa bağlı bir yönetici düğüm vardır. İstemciler adı verilen ikinci oyuncu grubu, belirli bir aygıtı yönetme haklarına sahip olmayan ancak

durumlarını sorgulamak isteyen düğümlerdir. Şekil 2.14, sisteme katılan oyuncuların oynadığı rolleri gösteren rol bazlı diyagramı sunmaktadır.



Şekil 2.14. Aktörler için genel olarak rol bazlı diyagram (Bagchi, 2017)

Blokzincir teknolojisi, Ethereum teknolojisi itibariyle varlık transferi kapasitesinin yanında programlanabilir bir yapıya sahip oldu. Ethereum dünyasında blokzincir ağı üzerinde yazılan programların çalıştırılabilmesi için akıllı sözleşme kavramı devreye girmektedir.

2.3.3 Ethereum Teknolojisinde Akıllı Sözleşmeler

Ethereum blok mimarisi Bitcoin ile benzer yapıdadır ve işlemler (transaction) aynı mantıkla blok içinde tutulmaktadır. Blok içinde işlemlerin nasıl tutulduğunu ve işlemlerin özet (hash) değerinin alınarak bir merkle ağacı içerisinde saklanması ile ilgili bazı detaylar 2.2 bölümünde verilmiştir. Aynı şekilde Ethereum da benzer yolu kullanmaktadır. Bitcoin kripto-para transfer işleminde, transferi yapan hesap bu işlemin

girdi kısmında dijital olarak işlemi imzalar ve bu şekilde hem transfer işlemi veri bütünlüğü sağlanmış olur hem de göndericinin imzası taklit edilemeyeceğinden gönderici doğrulaması sağlanmış olur. Ethereum'da da işlem özel anahtar ile imzalanır, yani mantık aynıdır. Madencilik ile ilgili ise Ethereum yine Bitcoin'de olduğu gibi "İşin İspatı", yani PoW (Proof of Work) algoritmasını kullanarak madenciliğin gerçekleşmesini sağlar. Bitcoin'den farkı, Ethereum'un "ethash" isminde sha3 tabanlı özet algoritmasını kullanmasıdır (Buterin, 2013).

Ethereum blokzincir ağı üzerinde yüksek işlem gücü veya performans elde etmek mümkün değildir. Çünkü bu yapı paralel programlama veya dağıtık hesaplama gibi mantıkla kurgulanmadığından amacı bu değildir. Buradaki asıl amaç çalıştırılan programın hiç bir zaman çökmemesinin garanti edilmesi, programa müdahalenin mümkün olmaması, hata toleransının sağlanması, programa sağlanan verinin blokzincir üzerinde tutulması nedeniyle verinin değiştirilemez olmasının garantisidir. Bu sistemin teknik olarak yaptığı iş şu şekilde tanımlanabilir: IFTT (If This Than That) yani bir işlem gerekli kuralı sağladığında sıradaki işlemin gerçekleştirilmesidir. Ethereum blokzincir ağı üzerine gönderilen programların çalıştırılmasını üstlenen altyapı ise Ethereum Sanal Makinesi diye tabir edilen "Ethereum Virtual Machine" kelimelerinin kısaltmasıdır, yani: EVM. Genelde akıllı sözleşme kavramı ile ilgili yanlış algılar oluşmasına neden olan şey ise isimlendirilmesidir. Aslında temel olarak bilinmesi gereken tanım, Ethereum'a bağlı bilgisayarlarda madencilik işlemi sırasında çalışan programlardır. İstenirse karşılıklı hukuki bir sözleşme olarak da geliştirilebilir veya istenirse döviz kuru bilgisini otomatik olarak finans kurumlarından alıp kaydeden bir program olarak da yayınlanabilir (Ethereum, 2019).

Örneğin Hasan ve Ahmet aralarında bir kurban pazarlığına giriştiler. Ahmet'in iddiasına göre kurbanlık fiyatı bayramdan birkaç gün öncesinde canlı hayvan kilogram fiyatı 24 TL'ye inecektir. Doğal olarak kurban satıcısı olan Hasan'a göre ise asgari 26

TL civarında kalacaktır. Pazarlıktaki iddialarına göre “Et ve Süt Kurumu” nun belirlediği son fiyat hangisinin iddia ettiği fiyata yakın olursa o fiyat geçerli olacaktır. Elbette ikisi de birbirine para mevzunda güvenmemektedirler. Bunun yerine, aralarında kolayca akıllı sözleşme geliştirerek arefe gününü beklemeye karar verirler. Buna göre süreç şöyle ilerleyebilir: Akıllı sözleşme, kurban müşterisi Ahmet’ten kilogramı 26 TL’den kurban parasını alır. Arefe günü Et ve Süt Kurumu et fiyatı kesinleşince, fiyat 25-26 TL arası olursa, para aynı şekilde Hasan’a transfer edilir. Fiyat 24-25 TL veya 24 TL’den de az olursa, kilogram başı 2 TL kesinti Ahmet’e iade edilir, kalan tutar da 24 TL üzerinden kaç kilogram ediyorsa hesaplanarak Hasan’a gönderilir.

Akıllı sözleşme geliştirme süreci Solidity programlama dili ile yapılabilmektedir. Solidty, C++ ve Java dillerinin yazım yapısına benzeyen bir programlama dilidir. Solidity ile akıllı sözleşme yazılım süreci gerçekleştirildikten sonra Solidity derleyebilen bir derleyici ile derlenir ve blokzincire işlem (transaction) olarak iletilir.

Örnek bir akıllı sözleşme kodu:

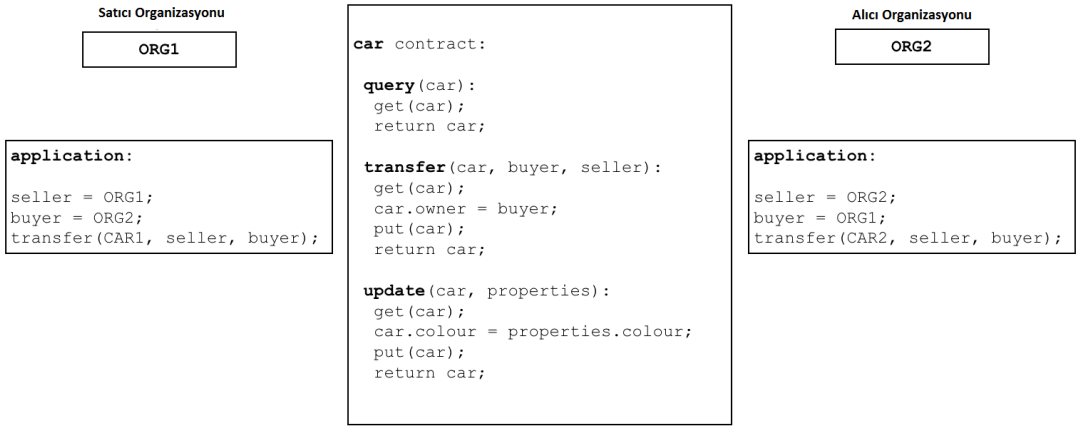
```
pragma  solidity ^0.4.0;
contract  Simple.Storage  {
   uint  stored.Data;
   function  set( uint x )  public {
      stored.Data = x;
   }
   function  get( )  public constant returns ( uint )  {
      return  stored.Data;
   }
}
```

Akıllı sözleşmelerin ve diğer işlemlerin gerçekleştirilebilmesi için bir ücretlendirme sistemi mevcuttur. Bunun için "*gas*" adı verilen birim kullanılır. İşlem veya akıllı sözleşme kodunun sürdürülmesi için gereken gas miktarı ve kullanabileceği azami gas miktarı tespit edilir. Aynı şekilde, Bitcoin ağındaki "*transaction fee*" yani işlem ücreti ile aynı mantıktadır. Akıllı sözleşme için ise kullanılan işlem hesaplama sarfı, veri bağlantısı, kullanılan kaynak durumuna göre ihtiyaç duyulan gas miktarı artacaktır. Akıllı kontratı çalıştırabilen gas harcaması, hesapta bulunan "*ether*" sayesinde temin edilebilir. Yeterli ether bulunmadığında, programı çalıştıracak gas gereksinimi karşılanamaz, bu durumda işlem iptal olur ve işlem öncesi duruma dönülmüş olur. Gas, Ethereum içindeki karmaşık hesaplamaları, ağ üzerinde çalışmada "güvenli" hale getiren hassas bir mekanizmadır; çünkü kontrolden çıkmış programlar ancak akıtılan para kadar sürecektir. Para akmazsa, madenciler bu işlem üzerinde çalışmayı durdururlar. Bu şekilde ücretsiz program çalıştırma olmaması sistem güvenliği için koruyucu bir mekanizma sağlar (Wood, 2014).

2.3.4 Hyperledger Platformunda Akıllı Sözleşmeler

Kayıt defteri ile birlikte akıllı sözleşme, Hyperledger Fabric blokzincir sisteminin kalbini oluşturmaktadır. Bir defter, bir dizi iş nesnesinin şu anki ve tarihi durumu hakkındaki gerçeklere sahip olmasına rağmen, akıllı sözleşme, deftere eklenen yeni gerçekleri oluşturan uygulanabilir mantığı tanımlar. Genellikle bir zincir-kod (chaincode) dağıtımı, ilgili akıllı sözleşmeleri gruplandırmak için yöneticiler tarafından kullanılır, ancak Fabric platformu düşük seviyeli sistem programlaması için de kullanılabilir.

İşletmeler birbirleriyle işlem yapmadan önce, ortak terimler, veriler, kurallar, kavram tanımları ve süreçleri kapsayan ortak bir sözleşme seti tanımlamalıdırlar. Birlikte ele alındığında, bu sözleşmeler, işlem yapan taraflar arasındaki tüm etkileşimleri yöneten iş modelini ortaya koymaktadır.

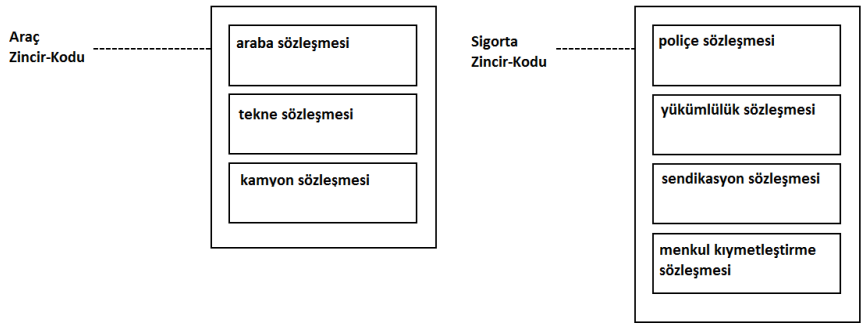


Şekil 2.15. Farklı organizasyonlar arasında kuralları yürüten zincir-kodu (Hyperledger Fabric Github Repository, 2019)

Bir blokzincir ağı kullanarak, bu sözleşmeleri, sektörde akıllı sözleşmeler olarak bilinen, çok çeşitli yeni olasılıklar açmak için yürütülebilir programlara dönüştürebiliriz. Bunun nedeni, akıllı bir sözleşmenin her tür iş nesnesi için yönetişim kurallarını uygulayabilmesi ve böylece akıllı sözleşme yapıldığında otomatik olarak çalışması için uygulanabilmesidir. Örneğin, akıllı bir sözleşme belirli bir zaman dilimi içinde yeni bir araba teslimatı yapılmasını veya sırasıyla mal veya sermaye akışını iyileştirerek önceden belirlenmiş şartlara göre fonların serbest bırakılmasını sağlayabilir. Ancak en önemlisi, akıllı bir sözleşmenin imzalanması, manuel bir insan iş sürecinden çok daha verimlidir.

a. Terminoloji:

Hyperledger Fabric kullanıcıları, sıklıkla akıllı sözleşme ve zincir-kodu terimlerini birbirlerinin yerine kullanırlar. Genel olarak akıllı bir sözleşme, küresel düzende bulunan bir iş nesnesinin yaşam döngüsünü kontrol eden işlem mantığını tanımlar. Daha sonra blokzincir ağına dağıtılan bir zincir-koduna paketlenir. Akıllı sözleşmeler geçerli işlemler olarak düşünülürse; zincir-kod ise akıllı sözleşmelerin dağıtım için nasıl paketlendiğini düzenler.



Şekil 2.16. Bir zincir-kodunda tanımlanan akıllı bir sözleşme (Hyperledger Fabric repository, 2019)

b. Kayıt Defteri:

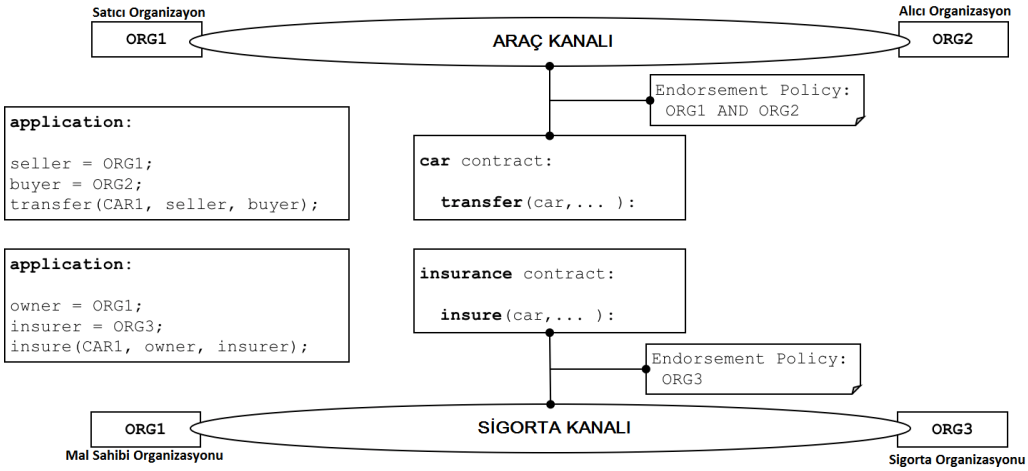
En basit seviyede bir blokzincir, durumları bir defterde güncelleyen işlemleri kesin olarak kaydeder. Akıllı sözleşme, defterin iki ayrı parçasına programlı olarak erişir. Akıllı sözleşmeler öncelikli olarak durumları ortaya koyar, alır ve siler ve aynı zamanda işlemlerin değişmez blokzincir kaydını sorgulayabilir.

- 'Get' komutu, bir iş nesnesinin o andaki durumu hakkında bilgi almak için bir sorguyu temsil eder.
- 'Put' komutu, yeni bir iş nesnesi yaratır veya muhasebe dünyasında var olanı değiştirir.

- 'Delete' komutu, bir iş nesnesinin, defterin o andaki durumundan kaldırılmasını, ancak tarihinin silinmemesini temsil eder.

c. Kanallar:

Hyperledger Fabric, bir kuruluşun aynı anda birden fazla ayrı blokzincir ağına kanallar üzerinden katılmasını sağlar. Kanallar, veri ve iletişim gizliliğini korurken, altyapının verimli bir şekilde paylaşılmasını sağlar. Kuruluşların iş trafiğini farklı taraflarla ayırmalarına yardımcı olacak kadar bağımsızdır, ancak gerektiğinde bağımsız faaliyetleri koordine etmelerini sağlayacak kadar entegredirler.



Şekil 2.17. Organizasyonlar arası Kanal Mekanizması (Hyperledger Fabric repository, 2019)

Yönetici, bir kanalda başlatıldığında zincir-kodu için bir onay politikası tanımlar ve zincir-kodu yükseltildiğinde değiştirebilir. Onay politikası, bir kanala dağıtılan aynı zincir-kodunda tanımlanan tüm akıllı sözleşmelere eşit olarak uygulanır. Ayrıca, tek bir akıllı sözleşmenin farklı onay politikalarıyla farklı kanallara konuşlandırılabileceği anlamına gelir.

Bir zincir-kodunda tanımlanan akıllı sözleşmeler, bir dizi blokzincir organizasyonu arasında kararlaştırılan iş süreci için etki alanına bağlı kuralları kodlar. Bununla birlikte, bir zincir-kodu iş süreçleri için bu akıllı sözleşmelerle ilgili olmayan, alan bağımsız sistem etkileşimlerine karşılık gelen düşük seviyeli program kodunu da tanımlayabilir.

Blokzincirde akıllı sözleşmelerin kullanılması, çok sınırlı bir betik dili sunan Bitcoin ile başladı. Bu komut dosyası dilinin, belirli işlemler gerçekleştirilirken bile güvenlik açıkları keşfedilince kullanımı kısıtlandı (Watanabe ve ark., 2015). Ek olarak, Bitcoin blokzincir "durumsuz" bir tasarıma sahiptir. İşlemler, hangi girdilerin tüketildiği ve yeni harcanmış çıktıların yaratıldığı konusunda başarılı ya da başarısız da olabilir (Kaptchuk ve ark., 2019). Bu akıllı sözleşmelerin birden fazla duruma sahip olması veya herhangi bir iç durumu sürdürmesi mümkün değildir. Bu model güvenlik ve ölçeklenebilirlik avantajları sağlarken, defterin kullanımı basit varlık alışverişleriyle sınırlanabilir (Croman ve ark., 2016).

Ethereum, özel olarak oluşturulmuş bir sanal makinede işlemleri işleyerek akıllı sözleşmeler kavramını ilerletmiştir. Akıllı sözleşmeler, daha sonra EVM bytecode'a derlenen, genellikle Solidity olan, daha yüksek bir dilde yazılmıştır. Akıllı sözleşme, sözleşme kodunu yayınlayarak ağa dinamik olarak dağıtılabilir (Bhargavan ve ark., 2016). Bu sözleşme kodu, ağ katılımcıları tarafından daha sonra sözleşme adresine gönderilen işlemleri doğrulamak için kullanılacaktır. Bir işlem gerçekleştiğinde, akıllı sözleşmenin iç durumu dağıtılmış bir veri deposuna yazılır (Bashir, 2018).

Hyperledger Fabric dışında Sawtooth framework'ü, akıllı sözleşmeyi bir durum makinesi veya "işlem işlemcisi" şeklinde görerek akıllı sözleşmeler kavramını

genişletir. Dağıtık logdan geçtikten sonra, işlemler uygun işlem işlemcisine yönlendirilir. Bu işlem işlemcileri, işlemi işlemeden önce işlemin yükünü ve ilgili durumları almaktan daha iyidir. Sawtooth hem durumsuz (UTXO) hem de durum bilgisi olan (Ethereum tarzı) modelleri destekleyebilir (Olson ve ark., 2018).

2.4 Tahmin Piyasaları ve Kolektif Tahmin

Tahmin piyasaları kavramı, tez fikrinin gelişiminde ilk zamanlar değerlendirilmiş, fakat daha sonraları rekolte tahmin süreçleri ile ilgili yeterli bilgi toplandıktan sonra biraz daha arka planda kalmıştır. Ancak fikrin teorik zemininde rekolte tahmini öncesinde taahhüt alınarak bir piyasanın oluşması ve bu piyasaya bağlı kalarak pozisyon alınması nedeniyle benzerlikleri gözden kaçmamaktadır. Bu yüzden kısaca incelenecek ve aynı zamanda son günlerde bu konunun BZT ile birlikte de ele alındığından bahsedilecektir.

Tahmin piyasaları, bilgi devriminin başlangıcından beri sermaye piyasalarında ve veri biliminde yenilikçi bir yaklaşım göstermiştir. Tahmin Piyasaları, bireylerin veya bir grup teşekkülün gelecekteki olayların sonuçlarını tahmin etmelerini ve sonuçlardan teşvik edilmelerini sağlar. Tüm tarafların katıldığı bir etkinliğin sonuçlarının gerçekleşmesi üzerine teşvikler yeniden dağıtılır. Tahminde başarılı olabilmek için katılımcılar agresif bir şekilde bilgi toplar ve öngörme şansını doğru bir şekilde en üst düzeye çıkarmak için matematiksel modelleme uygular. İstatistiksel olarak, her sonuçla ilişkili fiyat, yüksek pozitif korelasyona sahiptir. Bu arada, tahminin doğruluğu büyük ölçüde katılımcı sayısına göre belirlenmektedir. Bilgi teknolojilerinin hızla ilerlediği son yıllarda, insanlar tahmin etkinliğine katılmanın önündeki engelleri en aza indirgemek için çevrimiçi tahminde bulunmaya yönelmiştir (Peterson ve Krug, 2015).

Tahmin piyasaları, herhangi bir soruyu sormak veya herhangi bir olayın sonucunu tahmin etmek için herhangi bir şahsın veya kuruluşun "kalabalığın bilgeliğine" dokunabileceği bir takas görevi görür. Geleneksel tahmin piyasaları, tahmin sonuçlarının önüne geçen ve adaletli ve büyük miktarda para alan merkezi bir *"Bilge" '*ye büyük ölçüde bağlı kalmıştır. Bu Bilge'nin rolü, kalabalıkların tahmin piyasalarına geniş çapta katılımları ve öngörülen olayların tipleri arasında tezat bir durum söz konusudur. Öngörülen olaylar çeşitlidir; seçim sonuçları, spor, eğlence, finansal araçlar ve hatta hava durumu gibi akla gelebilecek herhangi bir konuyu temel alabilir. Bir borcun gelecekteki tahmini kazancına bir fiyat veren finansal piyasalara benzer şekilde, tahmin piyasaları geleceğe ilişkin bir inanca ticari bir fiyat tahsis eder. Piyasa fiyatı, genel olarak kalabalığın bir olayın sonucunun olasılığını nasıl gördüğünü belirtmek için de kullanılabilir. Başka bir deyişle toplumun ne düşündüğünü, hatta araştırma ya da anket şirketlerinin yaptığı tahminlerin çok ötesinde insanların ne tahmin ettiğini kestirebilmektir, yani toplulukların nabzını tutabilme imkanı sağlar: Bu kavrama da kısaca "Kolektif Tahmin" olarak isim verilebilir (Peterson ve ark., 2015).

Tahmin piyasaları, aşırı düzenleme ve mevcut merkezi uygulamaların kırılganlığı nedeniyle henüz kitlesel yatırımcı gruplarına nüfuz etmeyen yıkıcı bir ekonomik araçtır. Ethereum ve Bitcoin gibi güçlü, eşler arası merkeziyetsiz ve dağıtık teknolojilerinin ortaya çıkışıyla, piyasaya dayalı tahminin bilimsel araştırılması, potansiyeli kestirilemeden ilerlemektedir. Blokzincir teknolojilerinin çıkardığı sinerji, toplumda adil ve gayri merkezi olan açık blokzinciri bilge kehaneti olarak gören güveni ortaya çıkarmıştır (Fröberg ve ark., 2018). BZT, bilgi şeffaflığı ve veri değişmezliği gibi özelliklerinden dolayı tahmin piyasasının yapı taşını oluşturmak için mükemmel bir adaydır. Programlanabilir ve dinamik bir karar verme kabiliyetine sahip blokzincirin adilliği, tahmin piyasasının düşük maliyete yani idari maliyetle çalışmasını sağlayabilir.

3. BULGULAR

Katılımcılar arasında bir güven mekanizması sağlayan BZT'yi kullanan ilk uygulamalar, ilk başlarda tabiatı itibariyle finans alanında önerilmiştir. Ardından sağlıktan tedarik zinciri yönetimine kadar birçok alanda uygulanabileceği anlaşıldı. Farklı iş hedefleri nedeniyle farklı tedarik zinciri oyuncuları merkezi bir sisteme güvenmeyebilir. BZT'nin temel amacı, dağıtık ve merkezi olmayan bir veritabanı sağlayarak veri tutarlılığı ve bütünlüğünü temin etmektir. Bu teknoloji, şirketlerin iş modellerinde değişiklik için büyük bir potansiyele sahiptir.

Rekolte tahmin yöntemleri ile ilgili yapılan yeni yayın ve çalışmalara bakıldığında "Hassas Tarım" perspektifi açısından yeni nesil teknolojilerin uygulanabilir olduğuna rastlanılmaktadır. Bilhassa makine öğrenmesi, nesnelerin interneti (IoT), uydu haberleşmesi ve sayısal görüntü işleme teknolojileri ile uyumlu çalışmalar ortaya koyulmaktadır. Bununla birlikte, son yıllarda popüler hale gelen BZT, tarım sektöründe bekleyen birçok problem ve ihtiyaç için çözüm olabileceği hususunda çeşitli insiyatifler gelişmektedir. Özellikle, tarladan direkt sofraya gıda tedarik zinciri, temiz ve organik gıda, çevre ve iklime daha duyarlı iyi tarım uygulamaları, tarımda demokratik katılımlı kooperatif gibi konuların BZT ile çözülebileceğine dair yeni fikirlerin emareleri görünür olmuştur. Ancak, uzun bir süre yapılan literatür araştırmasında, rekolte tahmin yöntemlerine BZT ile çözüm sunmayı hedefleyen yaklaşımlar bulunamamıştır. Bu açıdan dikkat edildiğinde getirilen çözüm yaklaşımı ilk olmaya adaydır. Modelin inşası ve tasarım mimarisi için gereken teorik bilgi de bu bağlamda geniş ve kapsamlı tutulmuştur. Bu yüzden literatür çalışmasına iki kısım olarak değinilecek, akabinde güncel rekolte verilerine dair bulgular ele alınarak kıyaslanacaktır. İlkinde, rekolte tahmin ile yeni teknolojilerin ilişkisi; diğerinde ise, tarım ve BZT ile bağlantılı olan çalışmalar olacaktır. Son kısımda, elde edilen güncel rekolte verilerindeki bulgular sayesinde platformun gereksinimine yönelik basit bir şekilde geliştirilen ihtiyaç analizi sunulacaktır.

3.1 Rekolte Tahmin Problemini İleri Teknolojiler ile Araştıran Çalışmalar

Modern rekolte tahmin yöntemleri daha önceki bölümlerde değinildiği gibi, bilgi ve iletişim teknolojilerinin yaygınlaşması sayesinde, son on yıldır geleneksel yöntemlerden daha çok kullanılır oldu. Hassas tarım içerisin yer alan bu kavram, halihazırda yeni teknolojileri tarım sektöründeki ihtiyaçlara hızlı bir şekilde adapte etmeyi amaçlamaktadır. Bunun yanında, son günlerde yıkıcı teknolojiler (Disruptive Technologies) diye isimlendirilen yeni teknolojileri de dikkate alarak, rekolte tahmin yöntemlerine yeni yaklaşımlar getirilmesi mümkündür.

Rekolte tahmininde en doğru tahminlere yaklaşmak için Makine Öğrenmesi (ML) yöntemlerini değerlendiren birçok çalışma bulunmaktadır. Bunlardan birisi de, rekolte tahmini ve aynı zamanda optimize edilmiş azot yönetimini başarabilmek adına ML yöntemlerini bir arada kullanan bir araştırmadır (Chlingaryan ve ark., 2018). Bu yayın, son 15 yılda, doğru ürün rekolte tahmini ve azot durumu tahmini için makine öğrenmesi temelli teknikler üzerine yapılan araştırma gelişmelerini tartışmaktadır. Raporda ayrıca, uzman bilgilerinin toparlanması, ML ve sinyal işleme tekniklerini birleştiren hibrit sistemlerin geliştirilmesi gibi olguların da yakın gelecekte hassas tarımın bir parçası olması değerlendirilmektedir. Benzer şekilde, kısmen de olsa yapay zeka ile geliştirilen çalışmalara da rastlamak mümkündür. Örneğin, *"Ürün Rekolte Tahmini için Major Yapay Zeka Modelleri Arasında Bir Karşılaştırma: Birleşik Devletler Midwestern Vaka Çalışması, 2006 – 2015"* isimli yayında, Amerika Birleşik Devletleri (ABD) Midwestern için en iyi ürün rekolte tahmin modelini geliştirmek için farklı yapay zeka (AI) modellerini karşılaştırılmaktadır (Kim ve ark., 2019). Bu araştırmada, ürün rekolte tahmini için altı farklı AI modeli test edildikten sonra, AI modelleri arasında kapsamlı ve objektif bir karşılaştırma yapılmaktadır. Bunların yanı sıra, nesnelerin interneti (IoT), artırılmış gerçeklik (AR) ya da VR gibi teknolojiler ile melezlenen projelere de denk gelmek mümkündür.

3.2 Tarım Sektöründe Blokzincir Teknolojisi Kullanımını İrdeleyen Çalışmalar

Tarım ve gıda sektöründe, blokzincir uygulamaları gıda tedarik zinciri, gıda güvenliği ve bütünlüğü, tarımsal ticarette şeffaflık ve izleme, mahsul kalite güvencesi takibi, tarımsal gıda tedarik yönetimi gibi birçok şekilde kullanılabilir. Bermeo-Almeida (Bermeo, 2018), tarımda blokzincir teknolojilerine dayalı bilimsel makalelerin %60'ının gıda tedarik zinciri yönetimi üzerine odaklandığını göstermiştir. Çin akademik çevrelerinden bir makale, bunu gıda tedarik zincirinin bilgi güvenliğine entegre etmek ve geleneksel tedarik zinciri sistemi ile karşılaştırmak için blokzincir teknolojisi kavramını değerlendirmektedir. Bu makale, blokzincir teknolojisini uygulayarak üretim işleyicileri, brokerler ve tüketiciler için bir tedarik zincir sistemi platformu oluşturmayı önermektedir (Tse ve ark., 2017). Benzer şekilde, bir başka örnek tarımsal işletmelerde blokzincir teknolojisinin şeffaflık ve tarımsal ticarette izlenmesi olarak kullanılmasına odaklanmaktadır (Papa, 2017). Brezilya Tahıl İhracatçıları İş Ağı (GEBN), Hyperledger platformuna dayalı tahıl kalite güvencesi takibi ile ilgili bir vaka çalışması sunmaktadır (Lucena ve ark., 2018). IoT (Nesnelerin İnterneti) cihazlarının da bu süreçte entegre edilmesini araştıran bazı çalışmalar, güvenilir gıda için blokzincir platformu olarak geliştirilmesini dikkate almaktadır. Örneğin, AGRIBLOCKIOT sistem mimarisi, BZT ve IoT ikisini bir arada içermektedir (Caro ve ark., 2018). Gıda tedarik zinciri şeffaf takip sistemi için RFID ve BZT kullanılmasının olumlu ve olumsuz yanlarını analiz etmek hususunda yaklaşımı olan Çin orjinli çalışma (Tian, 2016); RFID (Radyo Frekansı ID) kullanımını değerlendirmektedir.

Ek olarak, hassas tarımda blokzincirin avantajını araştıran çalışmalar vardır. Seralarda kullanılan IoT cihazları uzaktan izlenmeli ve kontrol edilmelidir. Ancak, verileri cihazlardan ana sunuculara aktarırken her zaman güvenlik ve gizlilik endişesi mümkündür, bu yüzden (Patil ve ark., 2018) işlemlerin saklandığı dağıtılmış bir defter mekanizması önermiştir. Çiftlik yönetim bilgi sistemini daha etkin kullanmak için dağıtık çevresel ölçüm değerlerini saklamak ve mantar üretim sürecini kontrol etmek için IoT ve BZT kullanan bir çözüm de önerilmiştir (Branco ve ark., 2019). Robotik sürü sistemleri, hassas tarımda otonomluk, güvenlik, esneklik ve karlılık konularında

da kritik bir rol oynayabilirler. Ayrıca burada iki farklı teknolojinin kombinasyonundan kaynaklanabilecek sınırlamalar ve olası sorunlar tartışılmıştır (Ge ve ark., 2017).

3.3 Rekolte Taahhüt ve Tahmin İzleme Platformu İhtiyaç Analizi

Bu bölümde, BZT ile kurgulanacak platforma olan ihtiyaç, son yıllarda rekolte problemine dair bulguları ortaya koyarak belirli çizelge dahilinde geniş pencereden gösterilmeye çalışılacaktır.

Polatlı Ziraat Odası'nın sağladığı bilgilere göre (TZOB, 2019), geçtiğimiz yıllarda 80.000 dekarlık soğan ekilmiş ve 2018 yılında 20.000 dekarlık alan daralmıştır. Açıkçası, soğanın temel gıda ürünleri arasında yer alması nedeniyle, fiyat dalgalanmaları sık sık gündemdedir ve bunun temel sebeplerinden biri de yavaş yavaş tarım alanlarının küçülmesidir. 2000 yılında Türkiye, soğan için 100.000 hektarlık bir ekim alanına sahipti, sonra bu alan 2017 yılında yaklaşık 60.000 hektara kadar düşmüştür. Üreticiler ve bazı kuruluşların temsilcileri, Polatlı'da 2017 yılında 523.000 ton soğan üretimine karşılık, 2018 yılında 150.000 ton hasatla ciddi bir ürün rekolte kaybının yaşandığını belirtmişlerdir (ZMO, 2018).

Çizelge 3.1. Polatlı'da soğanın durumu (TÜİK ve ZMO, 2018):

Yıllar	Ekim Alanı (dekar)	Üretim (ton)
2017	80.000	523.000
2018	60.000	150.000

Elbette 20.000 dekarlık ekim kaybına karşılık rekoltenin 523.000 tondan 150.000 tona gerilemesi, ayrıca planlama eksikliğinin de göstergesidir. Eğer soğan ile

ilgili üreticiler arasında güvenli bir mutabakata dayanan rekolte tahmin mekanizması bulunmuş olsaydı, problemin ortaya çıkışına daha iyi bir hazırlık yapılabilirdi. Polatlı'da soğan rekoltesinin aşırı düşüşü ortaya çıkmadan önce, rekolte tahmin izleme platformu üzerinde mutabakat ortamı hazır hale getirilmiş olsaydı, Polatlı'ya yakın olan Ankara, Eskişehir, Konya gibi bölgelerdeki üreticiler, buğday, arpa, nohut, mercimek gibi ürünlere odaklanmanın yanında soğana da bir kısım arazisini tahsis edebilirlerdi.

Eğer Tarımsal Üreticiler arasında BZT kullanan Rekolte Tahmin İzleme Platformu var olsaydı:

- Aracılar ve/veya tek başına otorite yok
- Herhangi biri sistemi ve piyasayı manipüle edemez
- Yaklaşık tahmini değer belirlenebilir
- Piyasa oyuncuları arasında açık işbirliği

Çizelge 3.2. Konya'da Kuru fasulyenin durumu (TÜİK ve ZMO, 2019):

Yıllar	Ekim Alanı (dekar)	Üretim (ton)
2017	191.438	70.242
2018*	195.000	73.000

Çizelge 3.3. Ankara'da nohutun durumu (TÜİK ve ZMO, 2019):

Yıllar	Ekim Alanı (dekar)	Üretim (ton)
2017	395.300	47.000
2018*	450.000	54.000

**2018 dönemi için rekolte verileri rapor ve istatistiklere bakılarak saha gözlemleri ile kıyaslanarak yaklaşık olarak bulunmuştur.*

Çizelge 3.4. Eskişehir'de mercimeğin durumu (TÜİK ve ZMO, 2019):

Yıllar	Ekim Alanı (dekar)	Üretim (ton)
2017	41.000	6.500
2018*	47.000	7.400

Yukarıdaki çizelgelerle ortaya çıkan bulgular, üretim sezonu başlamadan üreticilerin katılımıyla uzlaşılan bir mekanizmaya aktarılsaydı, daha farklı bir tabloyla karşılaşmak mümkün olabilirdi. 2018 yılında, Polatlı'da kuru soğan için bir önceki yıla göre, 373.000 tonluk rekolte kaybının yaklaşık 100.000 tonunu telafi edebilmek için basitçe bir simülasyon hesabı sayesinde aşağıdaki artış imkan dahilindeydi:

Çizelge 3.5. Üreticiler arasında ürün geçişlerinin soğana yansıması (TÜİK ve ZMO, 2019) :

2018 Ürün Rekolte İzleme Simülasyonu	Soğan Mevcut Durum (Ton)	Soğan Güncellenmiş Durum (Ton)
Polatlı	150.000	160.000
Ankara	249.000*	290.000
Eskişehir	100.000*	135.000
Konya	25.000*	38.000
Toplam:	524.000	623.000

Yukarıda çizelgede yer alan verilerin anlaşılması için, önceki çizelgelerde yer alan bulgulara dikkat edilmesi gerekir. Yani 2018 üretim sezonu başında rekolte tahmin izleme platformuna bahsi geçen bölgedeki üreticiler dahil olmuş olsalardı, kuru soğan rekoltesinde 373.000 tonluk kayıp için diğer ürün üreticilerinin yeterli bir kısmı soğana geçiş yaparak yaklaşık 100 bin ton civarında kısmı tazmin edilebilirdi. Böylece rekolte kaybı biraz daha azaltma şansı mümkün olabilirdi.

4. TARTIŞMA

Bu bölümde, üreticilerin tarımsal planlarını piyasanın diğer oyuncularıyla paylaşmalarını sağlayan ve üreticilerin gelecek hasat mevsimi için paylaştığı bilgilere dayanarak pozisyon almalarını sağlayan modelin inşa edilme inisiyatifi tartışılacaktır. Başka bir deyişle, platform ve ilgili oyuncular arasında en uygun mutabakata dayanan modelin inşası ve sistemin mimarisi değerlendirilecektir.

Belirtildiği gibi, sistem bir blokzincir ağının üzerine kurulacaktır. Genel olarak, blokzincir ağları iki tür altında sınıflandırılabilir: izinsiz ve izinli (Miller, 2019). İzinsiz bir blokzincir, herkesin ağa katılmasına ve bloklar oluşturmasına izin verir (Androulaki ve ark., 2017). Öte yandan, izinli bir blokzincirde, blokların yaratılması ve defterlerin bakımının yapılmasında yalnızca yetkili bir grup kümeye izin verilir. İzinli blokzincir ağları, paralel hesaplama ve daha iyi ölçeklendirme kullanımına izin vermesi nedeniyle izinsiz blokzincire göre birçok avantaja sahiptir. Sistemdeki tüzel kişilikler orijinal kimlikleriyle ortaya çıktığından, izinli blokzincir protokollerini (Vukolic, 2017) kurgulanan platforma etkin bir şekilde entegre etmek yeterli olacaktır.

4.1 Sistemdeki Tüzel Kişilikler

Sistemdeki her katılımcı, oluşturduğu mesajların bütünlüğünü ve doğruluğunu sağlamak için kullanılacak olan bir sayısal imza planında açık anahtar çiftini (*sk, pk*) tutar ve onun açık anahtarının özeti ile tanımlanır, yani *h(pk)* olarak belirtilir. Bununla birlikte, doğrudan *h(pk)* kullanmak yerine, açık anahtarların özetini ifade etmek için harfler kullanılmaktadır, yani farklı rolleri tanımlamak için farklı harfler kullanılır.

Protokole dahil olan iki tüzel kişilik olacaktır: çiftçiler ve idareciler. Çiftçiler, bir tarlaya sahip olan ve tarlasındaki potansiyel bitkileri yetiştiren gerçek veya tüzel kişilerdir. Çiftçiler sistemde iki rolü desteklemektedir; üretici ve denetçi, yani düzenli olarak topraklarında üretici olarak yetiştirilebilecek olan ürünler için rekolte taahhüdü beyan ederler ve başka bir taahhüt için gözlem ve raporlama yapan denetçi olarak ilgili taahhüde atanabilir, ve dolayısıyla gözlemini sayısal bir rakam ile rapor ederler. Bu, üreticinin taahhüdünü hangi oranda yerine getirdiğini gösterir. Platformun tescili ve rekolte taahhüdünün beyan edilmesi için çiftçilerin bölgelerindeki tarım otoritesinden yani platformdaki ismiyle idarecilerden sertifika almaları gerektiği unutulmamalıdır.

İdareciler, farklı bölgelerin tarım otoritelerini temsil eden memurlardır. Sistemde iki rol üstlenirler; Platform devamlılığı ve kayıt otoritesidir, yani çiftçilere sertifika sağlamak ve platformun korunmasından sorumludurlar. Ayrıca, akıllı sözleşmeleri dağıtabilir ve doğrulayabilirler. İdareciler, kayıt için çiftçilere sertifika sağladıkları ve platformu korudukları için, güvenli bir rekolte taahhüt sistemi elde etmek için yerleşik bir kimliğe sahip olmaları çok önemlidir. Bu nedenle, idarecilerin sisteme kabul sürecini tasarlamaya daha fazla özen gösterilmelidir.

Platformun altyapısına iyi tanımlanmış kimlikleri olan ilk idareci kümesi ile başlanmalıdır. Sistemin, ilk kümenin üyesi olmayan yeni bir idarecinin yeni bir tarımsal birimin bölge otoritesi olarak kayıt yapmasına izin verdiğine dikkat edilmelidir. Bir çiftçi için de, kayıt işlemi daha basit bir şekilde gerçekleştirilmelidir. Bir çiftçi sisteme katılmak istediğinde, önce kendi bölgesinin tarım otoritesinden bir sertifika ister. Gerekli şartları yerine getirmesi durumunda, ilgili otorite çiftçinin kimliğini imzalayarak sertifika belgesini oluşturur ve ona sertifikasını verir. Sertifika belgesi, çiftçinin ilgili bölgede talep ettiği çiftlikte arazinin sahibi olduğunu kanıtlar. Çiftçinin sertifika talebi için idarecilerden birine kayıt talebi sunması yeterlidir.

Sistemde yer alan tüzel kişiliğe sahip varlıkların aşağıdaki gibi protokol olarak sunulması mümkündür:

Protokol 1: İdareci Tüzel Kişiliği

Girdi: İlk kümedeki idarecilerin (A_{i1},.., A_{im}) tanımlayıcıları B_0 geniş bloğunda belirtilecektir. Yeni bir A* adayı sisteme kaydolmak için başvuruda bulunursa, mevcut idarecilerden biri başvuruyu onaylamak için mevcut tüm idareciler arasında oy kullanmak için akıllı sözleşme olan S* başlatır.

İşlem (Tx): Akıllı sözleşme S* şu şekilde çalışır: Her idareci A_i, reyini S* akıllı sözleşmesine gönderir, yani;

Çıktı: Kabulü onaylarsa '1' gönderir; Aksi takdirde, '0' gönderir. Onay sayısı tüm oylar arasında çoğunluktaysa, akıllı sözleşme S* yeni A adayını ağa yeni bir idareci olarak bildirmek için bir mesaj oluşturur.

Protokol 2: Çiftçi Tüzel Kişiliği

İşlem (Tx): İdareci (A_i), ilk önce tekil sertifikanın ($cert_u$) geçerli bir özgün çiftçi (F_u) imzası olup olmadığını doğrulayarak sertifikanın geçerliliğini kontrol eder. Sertifika $cert_u$ onaylandıktan sonra idareci (A_i), çiftçiyi (F_u) ağa yeni bir oyuncu olarak duyurmak için bir kayıt işlemi oluşturur.

4.2 Sistemdeki İşlemler

Sistemde tanımlanmış dört işlem türü vardır: kayıt, repütasyonun güncellenmesi, iptal ve raporlama. İlk üçü idareciler, sonuncusu da denetçiler tarafından meydana getirilir. Her işlem, bunu yapan tarafından imzalanır ve idareciler tarafından blokzincire eklenir.

4.2.1 Kayıt

Bir çiftçiyi platform ağına meşru bir oyuncu olarak duyurmak için bir idareci tarafından bir kayıt işlemi meydana getirilir. Aşağıdaki forma sahiptir:

$$(kayıt , F_u , Cert_u , R_u , n_u , sig_i , pk_i)$$

Çizelge 4.1. Kayıt işlemlerindeki değerler:

• F_u	kayıt edilecek çiftçinin benzersiz tanımlayıcısıdır.
• $cert_u$	çiftçi F_u'ya kayıt otoritesi tarafından verilen sertifikadır.
• R_u	çiftçi F_u için başlangıç repütasyonu olan itibardır.
• n_u	çiftçi F_u'ya atanan pozitif bir tamsayıdır.
• sig_i	açık anahtar pk_i altında ⟨ kayıt, F_u, $cert_u$, R_u ⟩ imzasıdır.
• pk_i	idareci A_i ortak anahtarıdır.

İlk repütasyon değeri R_u, her çiftçi F_u için 1/2 olarak belirlenecek ve çiftçinin performansına dayalı olarak her bir taahhütte güncellenecektir. Sertifika $cert_u$, çiftçi F_u için hazırlanmış geçerli bir sertifika ise, ve sig_i, pk_i açık anahtarı altında geçerli bir imza ise, o zaman geçerli bir kayıt işlemi olarak kabul edilir. Çiftçilerin zincirde kaydedilmiş geçerli kayıt işlemi varsa, sadece rekolte taahhütleri oluşturmalarına izin verildiğini hatırlatmak gerekir.

İdarecilerin, pozitif tamsayıları 1, 2,... kayıt sırasına göre çiftçilere sayısal değerler olarak atadığını, yani sistemde kayıtlı olan ilk çiftçiye 1 atandığına dikkat edilmelidir. Bu tür sayısal değerleri çiftçilere atamak, sistemde kayıtlı toplam çiftçi

sayısını saymaya olanak sağlar, ancak daha önemlisi taahhütler için çiftçiler arasından rastgele denetçiler seçmeyi daha verimli hale getirir.

4.2.2 Repütasyon Güncelleme

Bir repütasyon güncelleme işlemi, bir çiftçi tarafından oluşturulan ayrıca taahhütlerden birine atanan denetçiler tarafından sağlanan rapora göre ilgili çiftçinin itibarını güncellemek için bir idareci tarafından tetiklenir. Aşağıdaki forma sahiptir:

$$(güncelleme, F_u, c, R_u, sig_i, pk_i)$$

Çizelge 4.2. Repütasyon güncelleme için değerler:

• F_u	kayıt edilecek çiftçinin benzersiz tanımlayıcısıdır.
• c_j	çiftçi F_u'nun itibarının belirli bir T eşiğinin altında kaldığı ardışık taahhütlerin sayısını gösteren sayaçtır.
• R_u	çiftçi F_u için başlangıç repütasyonu olan itibardır.
• sig_i	açık anahtar pk_i altında ⟨ güncelleme, F_u, c_j, R_u ⟩ imzasıdır.
• pk_i	idareci A_i ortak anahtarıdır.

İşlemi oluşturmadan önce idareci A_i ilk önce zincirdeki çiftçi F_u için hazırlanan son repütasyon güncelleme işlemine bakar. Böyle bir işlem varsa, A_i yeni repütasyon R_u'nun T'den az olup olmadığını kontrol eder. Bu durumda c_j sayacını 1 arttırır; aksi takdirde sayacı 0 olarak ayarlar. Böyle bir işlem yoksa, A_i R_u itibarının T'nin altına düşüp düşmediğini kontrol eder. Bu durumda A_i, c_j'yi 1 olarak ayarlar; aksi takdirde c_j sayacını 0 olarak ayarlar.

4.2.3 Feshetme

Son taahhütlerinde iyi performans göstermemiş olan çiftçiyi iptal etmek için bir idareci tarafından iptal işlemi yaratılır. Aşağıdaki forma sahiptir:

$$(feshetme, F_u, sig_i, pk_i)$$

Çizelge 4.3. Feshetme işlemi için değerler:

• F_u	kayıt edilecek çiftçinin benzersiz tanımlayıcısıdır.
• sig_i	açık anahtar pk_i altında ⟨ güncelleme, F_u, c_j, R_u ⟩ imzasıdır.
• pk_i	idareci A_i ortak anahtarıdır.

Çiftçi F_u'nun iptal işlemi, F_u'nun son itibar yükseltme işlemindeki sayaç, t eşiğine eşitse ve F_u sonlandırılmayan son taahhütte başarısız olursa sadece o durumda meydana getirilir.

4.2.4 Raporlama

Denetçi tarafından, kendisine verilen taahhüt hakkındaki gözlemine ilişkin oranı bildirmek için bir raporlama işlemi yaratılır. Aşağıdaki forma sahiptir:

$$(raporlama , O_{j,k} , p_{j,k} , C_j , sig_k , pk_d)$$

Çizelge 4.4. Raporlama işlemi için değerler.

• $O_{j,k}$	ilgili C_j taahhüdüne atanan denetçinin tanımlayıcısıdır.
• $p_{j,k}$	$O_{j,k}$ tarafından C_j taahhüdüne verilen oran değeridir.
• C_j	taahhüdün tanımlayıcısıdır.
• sig_k	açık anahtar pk_d altında ⟨raporlama, $O_{j,k}$, $p_{j,k}$, C_j ⟩ mesajının imzasıdır.
• pk_d	denetçi $O_{j,k}$'nın açık anahtarıdır.

Akıllı sözleşme başlatıldığı vakit, çiftçilerin taahhütlerini beyan ettiği unutulmamalıdır. Her akıllı sözleşme, benzersiz bir adresle ilişkilendirilir. Sistemde bu adres, taahhüdün tanımlayıcısı olarak kabul edilecektir.

4.3 Rekolte Taahhüt Mekanizması

Rekolte taahhüdü mekanizması modelinde dört rol vardır: üreticiler, denetçiler, platform ve idareci kayıt makamlarıdır. *F* ile tanımlanan bir üretici, sistem üyelerine artırdığı ürünler için rekolte taahhütlerini periyodik olarak ilan eder. Kayıtlı bir çiftçi, *C* tarafından belirtilen rekolte taahhüdünü beyan ettiğinde, " *x* ürününün, gelecek sezon için çiftçiye ait *L* arazisinin *y* miktarında ekileceği " taahhüdünü yerine getirmesi beklenir. Bir denetçi, atandığı taahhüt için bir gözlem yapar ve gözlemini, çiftçinin taahhüdünü hangi oranda yerine getirdiğini belirten *R* sayısı ile bildirir. Bu modeldeki platform, hem çiftçilerin beyanlarını hem de denetçilerin raporlarını izleyen ve bir veritabanına kaydeden bir ortam olarak görülebilir. Platform, ya tek bir otorite ya da bir oyuncular ağı tarafından yönetilmektedir. Kayıt yetkilisi, koşulları yerine getirmesi durumunda her bir işletmeye benzersiz bir kimlik belgesi atayarak çiftçilerin ve denetçilerin kayıt sürecini yönetir.

Bu çalışma, bir dizi ağ oyuncusu tarafından yönetilen platformu dikkate almaktadır. Sebebi şu senaryo ile daha iyi açıklanabilir: platformu yöneten merkezi bir otorite olduğunu ve karlarını en üst düzeye çıkarmak için piyasayı manipüle etmeye çalışan bazı kötü niyetli çiftçiler olduğunu varsayalım. Kötü niyetli çiftçiler, piyasa oyuncularını yanlış yönlendirmek için yerine getiremeyecekleri yanlış taahhütler verebilir, yani belirli bir *X* ürünü için planladıklarından daha fazla rekolte taahhüdünde bulunabilirler. Bu durumda, *X* ürününün üretilen miktarı bir sonraki hasat mevsimi için beklenenden düşük olacaktır. Bu nedenle, ürünün birim fiyatı artacaktır ve kötü niyetli çiftçiler olması gerekenden çok daha fazla kazanacaktır. İdeal bir sistemde, bu davranışın kolayca tespit edilmesi beklenir. Ancak, kötü niyetli çiftçilerin merkezi otoriteyi kontrol etmek için yeterli güce sahip olmaları durumunda, bu eylem tespit edilmeden devam ettirebilir ve piyasayı istedikleri gibi tasarlayabilirler. Bu yüzden, böyle bir senaryonun gerçekleşmesini önlemek veya genel olarak, tek bir başarısızlık noktasını (*single point of failure*) önlemek için, kontrolü birtakım ağ oyuncuları grubu arasında dağıtmak daha iyi olacaktır.

Rekolte taahhüt sisteminde, sisteme kaydolmak için yerleşik bir kimliğe ihtiyaç duyulmaması durumunda, kötü niyetli bir oyuncu birden fazla kimlik oluşturabilir ve sistemin büyük bir bölümünü kontrol edebilir. Daha sonra bu gücü piyasa oyuncularını manipüle etmek ve hatta bir Sybil saldırısı yapmak için kullanabilir. Bu tür yanlış davranışları önlemek için, rekolte taahhüt sisteminin, iyi tanımlanmış kimliklere ihtiyacı vardır. Çiftçilerin kimliklerini tespit etmek için, kayıt otoritesinden kimlik doğrulama servisi aracılığıyla sağlanan kayıt sertifikası sayesinde, sisteme entegre edilmesinden sonra bu tespitin mümkün olduğunu belirtmekte fayda vardır.

4.3.1 Rekolte Taahhüdü Beyan Etmek

Sistemde, çiftçiler düzenli aralıklarla ağa yönelik bir rekolte taahhüdü bildirmek zorundadır. Bu taahhüt, çiftçinin niyetini belirleyen bir beyanat olacaktır; yani, "mahsul *X*, gelecek hasat mevsimi için *Z* tarım arazisine *Y* miktarında ekilecektir". Çiftçiler bu bildirimi akıllı bir sözleşme yaparak gerçekleştirirler. Ayrıca, verilerin doğruluğunu sağlamak için imzalarını sözleşmeye eklerler.

4.3.2 Rastgele Bir Denetçi Seçmek

Önceki bölümde vurgulandığı gibi, rekolte taahhüt sistemi, bir denetçinin üretici rolündeki çiftçi tarafından verilen taahhüdüne atanınca, taahhüdün yerine getirilip getirilmediğinin doğrulanmasını gerektirir. Bu amaçla, bir çiftçi, kendisi için başlatılan akıllı sözleşme ile denetçi olarak taahhüdüne atanabilir. Ancak akıllı sözleşme meydana getirildiğinde, bu işlemin çiftçi tarafından kolayca bozulabilecek bir denetçi seçimi şeklinde değiştirebilir. Bu nedenle, denetçinin çiftçilerin taahhüdüne görev verme müdahalesi engellenmelidir.

Sistemde, akıllı sözleşmenin bir taahhüde denetçi seçmek için kullanacağı "rastlantısallık"; çiftçi tarafından müdahale edilemeyecek bir kaynaktan alınacaktır, yani akıllı sözleşme C_j, son blok B_v'nin özetini alacaktır, $h(B_v)$, rastgele girdi olarak zincire eklenir ve bu rastlantısallığı kullanan tüm kayıtlı çiftçiler arasında bir denetçi olarak çiftçi O_j seçilir. Ancak, önceki bölümde detaylandırıldığı gibi, kötü niyetli bir denetçi, tarım alanlarının gerçek durumunu yansıtmayan yanlış bir rapor sunabilir. Bu nedenle, sadece bir denetçiye güvenmek yerine, gözlem görevini bir grup denetçi

arasında dağıtmak daha iyi olacaktır, yani sistemdeki akıllı sözleşme C_j ; $O_{j,1}$, $O_{j,2}$ ve $O_{j,3}$ olan 3 farklı çiftçiyi her bir taahhüde denetçi olarak atayacaktır.

C_j taahhüdüne tayin edildikten sonra, her bir denetçi $O_{j,k}$; ilgili tarlaları belirli bir zamanda ziyaret etmek ve gözlemine ilişkin bir değeri rapor etmek zorundadır. Bu değer, çiftçinin taahhüdü yerine getirme oranını belirten $p \in [0, 1]$ sayısal değeri olacaktır. Her mahsulün belirli bir ekim zamanı ve belirli bir hasat zamanı olduğunu ve çiftçilerin taahhütlerini beyan ettiklerinde bu süreleri göz önünde bulundurmaları gerektiği platformda tekraren vurgulanmalıdır. Başka bir deyişle, çiftçiler taahhüt oluşturduğunda, denetçilerin taahhütlere ilişkin raporlama oranlarını ne zaman vermeleri gerektiğini çiftçilerin belirtmeleri gerekir. Bunun yanında, blokzincir ağının dışından bir kaynak kullanmak yerine, sistemde zaman, zincire eklenen blokların sayısı ile belirlenir. Kısaca, zincire eklenen iki ardışık blok arasındaki geçen süreyi tanımlayan blok üretim aralığı tespit edilmektedir. Bu yüzden, çiftçiler belirli bir mahsulün taahhüdü için akıllı sözleşme oluşturduklarında, hasat mevsimi ile ilgili zamanı, blokların sayısı cinsinden belirtirler, daha sonra denetçilerin taahhüt için verdikleri gözlem değerlendirme oranlarını sağlayacaklarını belirtirler.

4.3.3 Denetçilerin Yerinde Kontrol Ziyaretinde Konum Garantisi

Diğer taraftan, bu sistem denetçilerin ilgili tarım alanlarını gerçekten ziyaret ettiklerini ve yeterince gözlem yaptıklarını kanıtlamalarını gerektirecek şekilde genişletilebilir. Bu durumda, denetçiler raporları için bir yer kanıtı ekleyebilirler, bu da Veriplace isimli çalışmasına göre, belirli bir zamanda ilgili tarlalardaki varlığının doğrulanması mümkündür (Luo ve Hengartner, 2010). Ayrıca, raporlama değerlerini onaylamak için bazı fotoğrafları sağlayabilirler.

4.4 Repütasyon Mekanizması

Bu bölümde, çiftçileri taahhütlerine bağlı kalmaya zorlayan "repütasyon" gibi anahtar bir kavram ortaya koyulmaktadır. Serbest piyasa koşullarının çıkardığı sorunlarda bilindiği gibi, kârlarını en üst düzeye çıkarmak isteyen çiftçiler ağın diğer oyuncularına yanlış bir taahhütte bulunarak veya planlarını gizlemek için bir taahhütte bulunmamayı tercih ederek manipüle edebilirler. Bununla birlikte, bu hareket piyasayı bozmakta ve taahhütlere dayalı yatırım yapmış diğer oyuncuların yatırımlarını kaybetmelerine neden olmaktadır. İtibar ya da sistemde tanımlı ismiyle repütasyon, bu gibi durumlardan kaçınmalarını sağlar. Ayrıca çiftçileri, taahhütlerini yerine getirme konusunda teşvik etmek için de kullanılabilir. İtibar, çiftçinin güven seviyesini belirleyen bir çiftçiye ait güven değeri olarak kabul edilebilir. Başka bir deyişle, piyasadaki diğer oyuncuların çiftçinin ne kadar güvenilir olduğunu tespit etmesini ve planlarını buna göre yapmasını sağlar.

İdarecilerin ağa yeni bir çiftçiyi üretici rolünde yasal oyuncu olarak bildirmek için bir kayıt işlemi yayınladığını tekrar dikkate almak gerekir:

❖ *Taahhüde İlişkin Repütasyon Süreci*

- Her kayıt işleminde, 1/2 olarak ayarlanan yeni çiftçi F_u için başlangıç değeri olan R_u bulunur.
- F_u'nun repütasyon değeri, çiftçi F_u'nın performansına bağlı olarak her bir taahhütte güncellenir.
- Kısaca, her çiftçi F_u bir taahhüt beyan etmek için akıllı bir sözleşme başlatır ve akıllı sözleşme C_j sözleşmesinin sahibi, sözleşmeyi sona erdiğinde performansını gösteren puanı P_j üretir. *(Aşağıya devam)*

- C_j'nin ürettiği P_j puanı [0,1] 'den gerçel bir sayı veya $\perp$ sembolü olacaktır, yani eğer hiçbir denetçi sözleşme için bir oran bildirmezse, P_j skoru $\perp$ olacaktır;
- Aksi halde puan, taahhütlerin denetçileri tarafından bildirilen $p_{j,k}$ oranlarının ortalaması olacaktır.
- Akıllı sözleşme C_j, $\perp$ sembolünü P_j olarak üretirse, idareciler bu taahhüdü gerçek bir düşünce olarak görmeyeceklerdir ve bu taahhüde dayanarak herhangi bir repütasyon-güncelleme oluşturmayacaklardır.

Diğer taraftan, eğer akıllı sözleşme C_j, P_j olarak [0,1] arasında gerçel bir sayı üretirse, idareciler P_j oranını dikkate alarak bir repütasyon-güncelleme işlemi oluşturacaklardır. Buradaki kilit soru; "idareciler işlemdeki repütasyon değerini nasıl hesaplar?" Diğer bir deyişle "ilgili çiftçinin yeni repütasyon puanı nasıl hesaplanır?" sorusudur. Sade olan yaklaşım ise, yeni repütasyon değerinin, çiftçinin yaptığı her taahhütten aldığı puanların ortalaması ve başlangıç repütasyon değerinin hesaplanmasıdır, yani çiftçinin aldığı puanların sayısı n ve çiftçi F_u'nun başlangıç repütasyon değeri R_u^* olsun, o zaman yeni repütasyon değeri;

$$(R_u^* + \Sigma P_j) / (n + 1)$$

olacaktır; burada P_j, F_u'nun C_j taahhüdünden aldığı puandır. Bununla birlikte, eğer yeni repütasyon değeri bu şekilde üretilirse, çok sayıda taahhüdü yerine getiren başarılı bir çiftçi, kendi repütasyonu az çok zarar göreceğinden, diğer oyuncuları manipüle etmek için yaptığı yeni taahhütlere göre hareket etmemeyi tercih edebilir.

Bir çiftçinin sözüne daha sadık kalabilmesi için, idareciler repütasyon değerini, çiftçinin son repütasyon değerinin ve onun yaptığı son taahhütten aldığı puanın ortalaması olarak hesaplar; çiftçi F_u'nun son repütasyon değeri R_u ve çiftçinin aldığı puan P_j olsun, öyleyse yeni repütasyon değeri;

$$(R_u + P_j) / 2$$

olacaktır. Eğer çiftçi F_u sisteme yeni kayıt olmuşsa ve henüz herhangi bir taahhütte bulunmamışsa, son repütasyon değeri R_u, ilk repütasyon değerine eşit olacaktır; Aksi halde R_u, F_u için tesis edilen son repütasyon-güncelleme işlemindeki repütasyon değeri olacaktır.

Çiftçilerin periyodik olarak yatırım planlarını paylaşma taahhütlerini beyan etmeleri gerektiğine en başından beri işaret edilmektedir. Bunu uygulamak için "repütasyon" kavramı halihazırda vurgulanmaktadır. İdareciler, çiftçilerin rekolte taahhütlerini beyan edip etmediklerini periyodik olarak kontrol eder:

❖ *Taahhüde İlişkin Raporlama Süreci*

❖ İdarecilerden biri, A_i, belirli bir zaman diliminde rekolte taahhüdü beyan etmeyen bir çiftçi F_u tespit ederse;

➢ çiftçi F_u için bir itibar-güncelleme işlemi ($güncelleme, F_u, c_{j+1}, R_u^*, sig_i, pk_i$) oluşturur.

❖ Eğer çiftçi F_u sisteme yeni kaydolduysa ve henüz herhangi bir taahhütte bulunmadıysa;

➢ A_i işlemi R_u'nun olduğu ($güncelleme, F_u, 1, R_u / 2, sig_i, pk_i$) olarak oluşturur.

➢ *(Aşağıya Devam)*

- ❖ R_u, F_u'nun ilk repütasyon değeri; yoksa, A_i F_u için oluşturulan son işlem-güncelleme;
- ➢ (*güncelleme,* F_u, c_j, R_u, sig_i, pk_i) ayıklar ve sonra yeni işlemi,
- ➢ (*güncelleme,* F_u, c_{j+1}, $R_u / 2$, sig_i, pk_i) olarak hesaplar.

Ayrıca, denetçilerin görevlerini ihmal etmemesi, verimli bir rekolte taahhüt sistemine sahip olmak için zorunludur. Repütasyon, denetçileri bu şekilde davranmaya zorlamak için de kullanılabilir:

Bu amaç doğrultusunda; eğer idarecilerden biri A_i diyelim, C_j taahhüdüne atanmış olan denetçi $O_{j,k}$'nin belirtilen süre içerisinde $p_{j,k}$ oranını sağlamadığını tespit ederse, bir repütasyon-güncelleme işlemi ihdas eder:

$$(\textit{güncelleme}, \ O_{j,k}, c_{j+1}, R_u^*, sig_i, pk_i)$$

Repütasyon ve raporlama sürecinde, repütasyon-yükseltme ve işlem-güncelleme arasındaki ayrıma dikkat edilmelidir:

$O_{j,k}$ denetçisi için şu şekilde; A_i'nin ortaya çıkarttığı son işlem-güncelleme:

$$(\textit{güncelleme}, O_{j,k}, \ c_j, \ R_u, sig_i, pk_i)$$

$O_{j,k}$ için tesis edilir ve sonra yeni işlem şu şekilde hesaplanır:

$$(\textit{güncelleme}, O_{j,k}, c_{j+1}, Ru / 2, sig_i, pk_i)$$

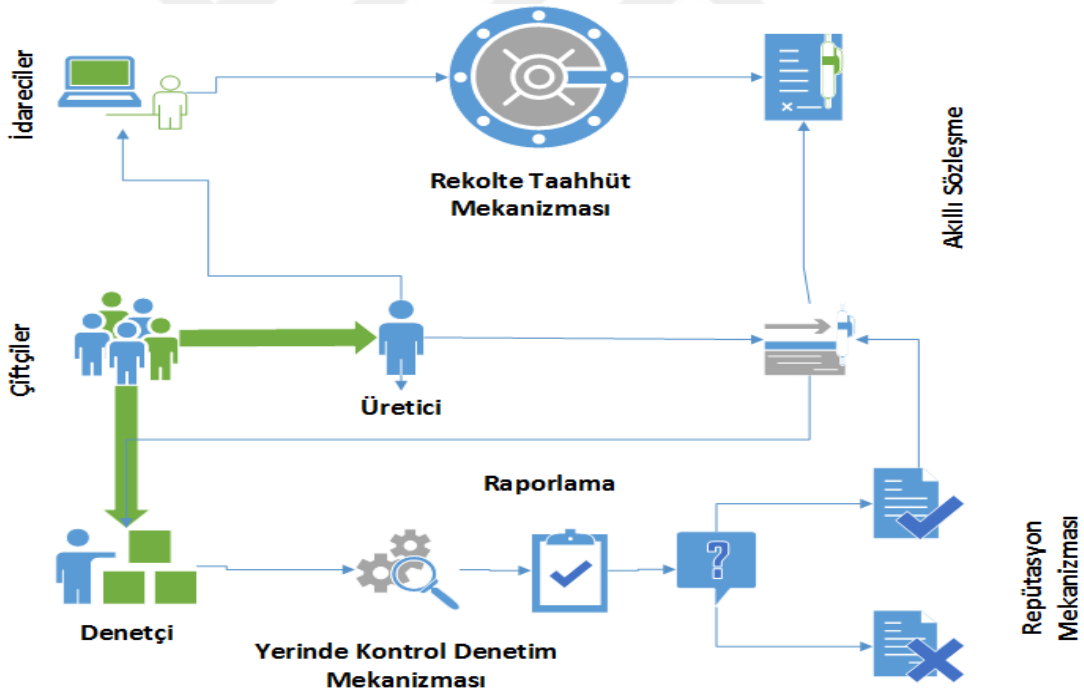
Son olarak repütasyon kavramı kapsamında, özellikle blokzincir üzerinden yapılan çalışmalara da dikkat çekmek gerekir. İlerleyen günlerde, hem protokol olarak hem konsensüs şekliyle ilgilenen projelerin ortaya çıkışı hızlanabilir. *Repucoin* (Yu ve ark., 2019) ve *Repchain* (Huang ve ark., 2019) bu açıdan ışık tutan çalışmalar olarak dikkate alınabilir.

4.5 Tasarım ve Örneklem

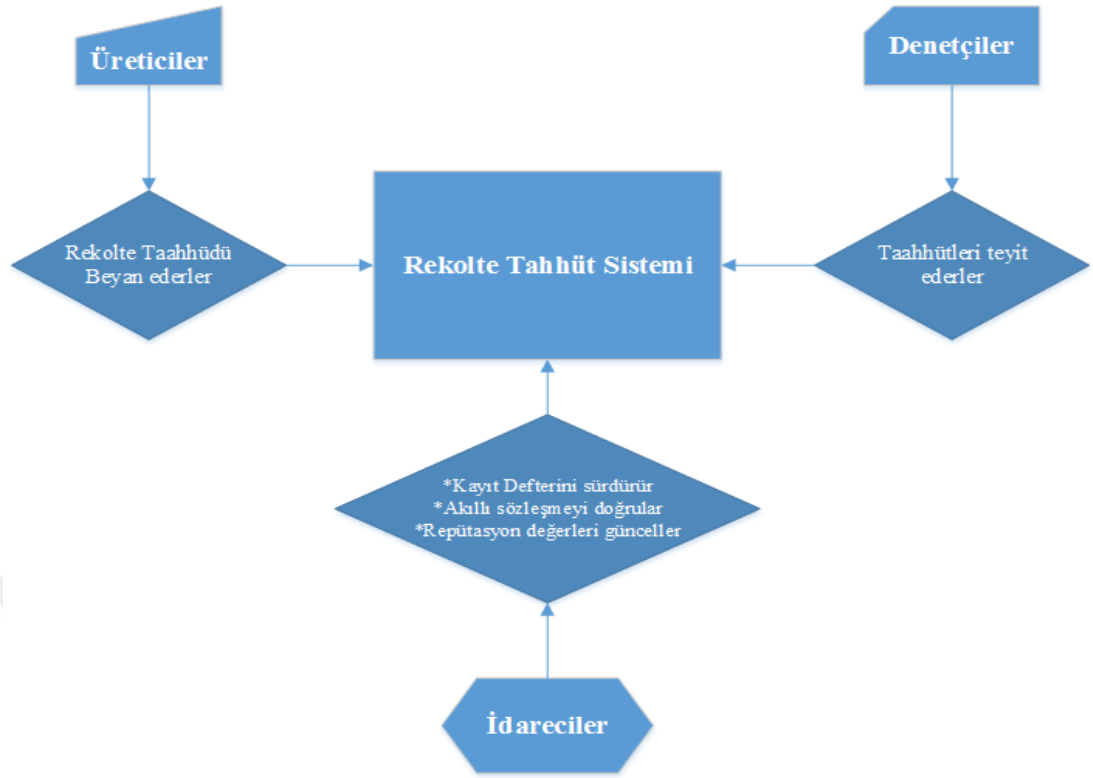
Model inşası bölümünde belirtildiği gibi, kurgulanacak platform ağı izinli türde blokzincir ağı olacaktır. Bu bölümde rekolte taahhüt sistemi tanıtılmıştır. Rekolte taahhüt sistemi, rekolte tahmin sürecini uygulamak için gereken blokzincir tabanlı kurgulanmış bir sistemdir. Sistem, üretici rolündeki çiftçilerin rekolte taahhüdü için yeni kontrat oluşturmasına imkan verir. Bu prototip dahilinde, akıllı sözleşmeye bağlı kalarak sistem sadece rekolte taahhüt, repütasyon, ve konsensüse odaklanır. Denetçiler taahhüdü doğrular ve onlara raporlama girerek repütasyon puanı ekleyebilirler. Repütasyon hesaplanması, daha sonra akıllı sözleşmeye bağlı olarak otomatik olarak yapılmaktadır.

4.5.1 Sistem Tasarımı

Sistemin mimari olarak tasarımı ve kurgusunda, idareciler ve çiftçiler iki tüzel kişilik, çiftçiler de üretici ve denetçi olarak iki ayrı rol bazlı aktör olarak ortaya çıkmaktadır. Çiftçiler, idarecilerden temin edecekleri sertifika ile platforma kayıt yapabilmektedirler. Daha sonra, üretici olarak taahhüt beyan etmeleri gerekmektedir. Burada akıllı sözleşme otomatik olarak başlatılır ve süreç taahhütlerin denetçiler tarafından teyidi ve idarecilerin repütasyon değerlerini güncellemesi ile devam eder. Ayrıca bu süreçte idareciler, dağıtık kayıt defterlerini sürdürür ve akıllı sözleşmeyi doğrular.



Şekil 4.1. Kurgulanan Sistem Tasarımı



Şekil 4.2. Sistemin Çalışma Şekli

İlk başta bir çiftçi, bölgesinin tarım otoritesinden bir sertifika alır. Bu sertifika, çiftçinin ilgili bölgede talep ettiği çiftlikte arazinin kendisine ait olduğunu kanıtlar. Çiftçi daha sonra bu sertifikayı platforma kaydolma isteği olarak sunar. Sertifikanın onaylanmasından sonra, platform çiftçinin arazisi için rekolte taahhüdü oluşturulmasına yönlendirir. Bu taahhüt, çiftçinin niyetini belirleyen bir bildirimdir, yani; "gelecek sezon için onun arazisine X mahsulü Y miktarı kadar ekilecek" mealindedir.

Önerilen tasarımda, üreticilerin tarım planlarını pazarın diğer oyuncularla paylaşmalarını sağlayan ve üreticilerin gelecek hasat mevsimi için paylaştığı bilgilere dayanarak pozisyon almalarını sağlayan protokol açıklanmaya çalışılacaktır. Tasarımdaki aktörler ve roller aşağıdaki tabloda belirtilmiştir:

Çizelge 4.5. Tasarımdaki Aktörler ve Rolleri:

Aktörler	Roller
Üretici (Çiftçiler)	Bir tarlaya sahip olan ve tarla bölgesinde mümkün olan tarla bitkilerini yetiştiren gerçek veya tüzel kişilerdir. Çiftçiler periyodik olarak tarlalarında yetişebilecek ürünler için rekolte taahhüdü verdiklerini beyan eder. Platformun tescili ve rekolte taahhüdünün beyan edilmesi için çiftçilerin bölgelerinin tarım otoritesinden sertifika almaları gerekmektedir.
İdareci	Farklı bölgelerin tarım otoritelerini temsil eden memurlardır. Çiftçilere sertifika sağlamak ve platformun korunmasından sorumludurlar. Ayrıca, akıllı sözleşmeleri dağıtabilir ve doğrulayabilirler.
Denetçi (Çiftçiler)	Çiftçilerin taahhütlerini doğrulayanlardır. Bölgenin yakınlığına bağlı olarak çiftçiler arasından rastgele seçilirler. Gözlemle ilgili olarak, çiftçilerin taahhütlerini değerlendirir.

Platformda, çiftçi bir taahhüt ilan etmek için akıllı bir sözleşme başlatır. Ayrıca, verilerin doğruluğunu sağlamak için sözleşmeye olan taahhüdün imzasını da ekler. Akıllı sözleşme, çiftçinin taahhüdüne rastgele olarak bir denetçi atar. Belirlenen süre geçtiğinde, bu akıllı sözleşme denetçiyi çiftçinin taahhüdüne ilişkin gözlemine dayanarak $p \in [0,1]$ oran değerini girmesi için tetikler. Buradaki oran değeri, taahhüdün yüzde kaçının yerine getirildiğine bağlı olarak belirlenir. Son olarak, idareciler akıllı sözleşmeyi çiftçi ve denetçi tarafından sağlanan girdilere göre doğrularlar.

İşlemler, kısıtlanmış işlemin başka bir tüzel kişilikte belirli kontratlara erişimi olup olmadığını sorgulayabilir. Blokzincir ağına bağlı herhangi bir düğüm, bu bilgilere salt okunur bir şekilde erişebilir. Bu işlem yalnızca erişim bilgilerini sorgulamak içindir ve bir istemci her sorguladığında işlem göndermez. İşlem talebi, akıllı bir sözleşmedeki bir işlevi çağırır ve bir iade değeri alır. Bu nedenle bu işlem, madenciliğe ihtiyaç duymaması nedeniyle herhangi bir işlem ücreti gerektirmez.

Bölüm 4.4'de "Repütasyon Mekanizması" içerisinde geçen modele ayrıca ışık tutması açısından, repütasyon ve blokzincirin birlikte değerlendirildiği çalışmalar giderek artmaktadır. Hatta mutabakat protokolü olarak değerlendirildiğinde, "*Blokzincir Konsorsiyumu için Repütasyon-Bazlı Bizans Hata Toleransı*" başlıklı çalışma (Lei ve ark., 2018) bünyesinde geçen algoritma, protokol ve modüller bu kısımda geçen problemin çözümü için daha hızlı neticeler verebilir. Böylece ilerleyen süreçte buna benzer çalışmalar için de daha basit bir entegrasyon için imkan sağlanabilir.

4.5.2 Örneklem için Güvenlik Analizi

Bu bölümde, önerilen protokolle ilgili güvenlik sorunları tartışılmaktadır. Daha önce de belirtildiği gibi, platformda herhangi bir işlem veya herhangi bir akıllı sözleşme, içeriğini, imzalayanın açık anahtarı altında imza ile birlikte ağa yayınlar. Altta yatan imza düzeninin unutulmazlığı, bir oyuncunun başka bir oyuncu adına bir işlem veya akıllı sözleşme oluşturamamasını sağlar ve sistemdeki hiç kimse sisteme dağıtıldıktan sonra akıllı kontrat işleminin içeriğini değiştiremez.

Sistemde, idareciler zincirdeki son bloğun özet değerini yenisine ekleyerek deftere yeni bir blok eklerler. Temel özet fonksiyonunun çarpışmaya dayanıklı özelliğinden dolayı, idarecilerin deftere eklenen blokların içeriğini değiştirmesi hesaplama açısından mümkün olmayacaktır.

4.5.2.1 Taahhütlerin Yerine Getirilmemesi

Rekolte taahhüdü sisteminde, çiftçiler, diğer çiftçilerin önümüzdeki hasat mevsimi için paylaştığı bilgilere dayanarak üretim politikalarını gözden geçirir. Çiftçiler daha sonra, yetiştirdikleri ürünün rekoltesi için en uygun oranı belirler ve bu oranı ağdaki bir taahhüt yoluyla paylaşır. Dahası, optimum bir kâr elde etmek için taahhütlere bağlı kalmaktadırlar. Ancak, kötü niyetli bir üretici kârını en üst düzeye çıkarmak için taahhütlerini yerine getirmeden veya bir taahhütte bulunmadan piyasaya müdahale edebilir ve platformun diğer oyuncularının yatırımlarını kaybetmesine neden olabilir.

Bu gibi durumlardan kaçınmak için, platformdaki her bir çiftçiyle ilişkilendirilen [0,1] den gerçel bir sayı olan 'repütasyon' anahtar kavramı ortaya koyuldu. Repütasyon değeri R_u başlangıçta her çiftçi F_u için kayıt işlemi ile 1/2 olarak belirlenir ve her bir taahhütte çiftçilerin performansına dayalı olarak birincil idareciler tarafından güncellenir. İtibar değeri, çiftçilerin güvenilirliğini gösteren bir gösterge olarak görülebilir. Başka bir deyişle, platformdaki taraflar, gelecek hasat mevsimi için yatırım planlarını yaparken itibar değerlerine bakarak belirli bir çiftçinin taahhütlerini dikkate almaları gerekip gerekmediğini belirlerler. Daha önce açıklandığı gibi, diğer çiftçilerin yatırım planlarına taahhütleri dahil edildiğinde, çiftçiler karlarını en üst düzeye çıkaracaktır. Bunu yapmak için çiftçiler repütasyon puanlarını yüksek tutmaya çalışırlar. Bu nedenle, repütasyon değeri çiftçileri dürüst davranmaya ve taahhütlerine bağlı kalmaya zorlar.

4.5.2.2 İhmal Edilen Denetimler

Sistemde, çiftçiler düzenli aralıklarla akıllı sözleşme yaparak her hasat mevsimi için ağa rekolte taahhüdünü beyan eder. Etkin bir rekolte taahhüdü sistemi, taahhüdün yerine getirilip getirilmediğini doğrulamak için, "denetçi" olarak adlandırılan tarafsız bir üçüncü taraf gerektirir. Platform, başlatılan akıllı bir sözleşme ile her bir taahhüt için çiftçiler arasından denetçileri seçer. Bir rekolte taahhüdüne atandıktan sonra, her denetçi taahhüt için bir gözlem yapar ve gözlemini ağa rapor eder.

Ancak, kötü niyetli bir denetçi üreticinin itibarını zedelemek için yanlış bir oran rapor edebilir veya ilgili tarım alanını ziyaret etmeden bir oran rapor edebilir ya

da sadece görevini ihmal edebilir ve taahhüt hakkında hiçbir şey bilmeyebilir. Her şeyden önce, sadece bir denetçiye güvenmek yerine, sistemde bunun için oluşturulan akıllı sözleşme ile her bir taahhüt için üç denetçi görevlendirir. Ayrıca, denetçilerin raporlarına konum ispatı eklemelerini gerektirir, bu da belirlenen zaman diliminde karşılık gelen tarım alanlarını gerçekten ziyaret ettiklerini gösterir. Ayrıca, birincil idareci bir denetçinin, ilişkili zaman diliminde kendisine verilen taahhüt için oranını yayınlamadığını tespit ederse, birincil idareci, itibar-güncelleme işlemi yoluyla denetçinin itibarını düşürür. Ayrıca, her bir zaman dilimi için, birincil idareci, denetçilerden birini rastgele seçer ve ilgili tarım alanını ziyaret ederek gerçek bir rapor hazırlayıp hazırlamadığını kontrol eder. Birincil idareci, denetçinin yanlış bir oran sağladığını fark ederse, denetçinin itibarını düşürür.

Öte yandan, kötü niyetli bir üretici, üreticinin bildiği denetçileri seçecek şekilde akıllı sözleşmeler yapabilir. Ardından, denetçilerin taahhütleri yerine getirmese bile daha yüksek bir oran bildirmelerini sağlayabilir. Böyle bir durumdan kaçınmak için, her akıllı sözleşme defterdeki son bloğun özet değerini alır ve bu özet değeri, sistemde kayıtlı tüm çiftçiler arasından denetçiler seçmek için rastgele olarak kullanır. Burada rastgelelik kaynağı olarak görülen bloklar idareciler tarafından oluşturulduğundan, üreticiler denetçi seçim sürecine müdahale edemezler.

4.5.2.3 Temelsiz Oranlarla Repütasyon Güncelleme

Sistemde zaman, zaman dilimleri olarak adlandırılan ve her zaman dilimini round-robin tarzında bir idareci ile ilişkilendiren ayrık birimler dizisi olarak kabul edilmektedir. $(N+1)$ ve N, sistemde kayıtlı olan son idareciye atanan tam sayı değeridir. Her bir zaman dilimi için, birincil olarak adlandırılan ilgili yönetici, B_k bloğunu, ilgili zaman diliminde aldığı tüm akıllı sözleşmeler ve işlemler ile önceki

blok *h*'nin ($B_k - 1$) özetiyle birlikte oluşturur. Geçerli zaman damgası olarak karşılık gelen zaman dilimi, blok indeksi *k* ve tüm bu kayıtların bir imzası (Castro ve Liskov, 1999) 'de sunulan üç fazlı protokol kullanılarak blok deftere eklenir.

Buradaki kötü niyetli biri, ilgili zaman diliminde oluşturulan rekolte taahhüdünü veya denetçinin raporunu fiili olandan farklı olarak oluşturduğu bloğa yazabilir. Ayrıca, bloğa belirli bir taahhüt veya belirli bir rapor yazmamayı tercih edebilir ve görmezden gelebilir. İdareciler ağa yayılan tüm işlemleri görebildiklerinden, bu tür davranışlar kolayca algılanabilir.

5. SONUÇ VE ÖNERİLER

Rekolte tahmini, piyasa oyuncuları tarafından etkin bir yatırım planı hazırlamak için kullanılan en önemli araçlardan biridir. Mevcut rekolte tahmini yöntemleri, yalnızca ekim zamanından sonra veri sağladığından, ekim mevsiminden önce zamanında ve doğru sonuçlar vermez. Dolayısıyla ekim zamanından önce rekolte tahminine olanak veren bir mekanizma tasarlamak, tarımsal üretimdeki oyuncuların etkili ve kalıcı üretim politikaları geliştirmelerini sağlar. Ayrıca bu oyuncular, gıda pazarındaki koşullar hakkında önceden bilgilendirilecek ve piyasada oluşabilecek oynaklık için etkili önlemler alınacaktır. Bu amaç doğrultusunda, çiftçilerin gelecek hasat mevsimi için tarımsal üretim planlarını, pazarın diğer oyuncularıyla paylaşmalarını sağlayan etkin bir rekolte taahhüt sistemi önerilmiştir. Platform, aynı zamanda çiftçilerin başkalarının planlarını gözlemlemelerine ve yatırımlarını gözden geçirmelerine ve gelecek sezon için gerekli adımları atmalarına olanak tanımaktadır. Blokzincir teknolojisi ise, sansüre dayanıklı, kurcalamaya karşı korumalı ve zamana bağlı işlemlerin güçlü şekilde değişmez olduğu dağıtık kayıt defteri sağlayan platformu tasarlamak için tercih edilmiştir.

Bu tez çalışması daha önce Uluslararası bir konferansta bildirisi de yapılan makalenin (Doğantuna ve ark., 2018) özellikle teorik zemin, ihtiyaç metodolojisi, model ve tasarım kurgusu üzerinden geliştirilerek şekillenen geniş bir çalışma olarak karşımıza çıkmaktadır. Model ve tasarım üzerinden uygulama (implementation) yerine, bu süreçte örnekleme (instantiation) fırsatı bulunabilmiştir. Hem zaman hem de kaynak (donanım, yazılım lisansı) olarak daha fazla imkan bulunduğu takdirde, bu çalışma fikrinin daha ileriye götürülmesi mümkün olacaktır. Diğer taraftan konunun farklı disiplinleri bir araya getirmesi nedeniyle, bu çalışmanın sahada uygulanabilir etkili bir pratiğe dönüşmesi için ziraat mühendisi, tarım ekonomisti, blokzincir yazılım geliştiricisi, front-end/backend geliştiricisi, yazılım mimarı ve ilgili disiplinlerin uzmanlarından bir ekibi bir araya getirmeye ihtiyaç olacaktır.

Tez çalışmasını ve sonuçlarını, Adli Bilişim ve Adli Bilimler perspektifi açısından da ayrıca değerlendirmek özgün bir bakış açısı için gerekli görülmektedir. Adli Bilişim, hem hukuki terminolojiyi hem de bilişim kavramlarını bir araya getirmesi nedeniyle "Disiplinlerarası Adli Bilimler Anabilim Dalı" olarak değerlendirilmektedir. Adli Bilişim çalışmalarının; "Disiplinlerarası Adli Bilimler Anabilim Dalı" içerisindeki etkinliği hem akademik hem de pratik açısından daha fazla öne çıkmıştır. Adli Bilişimin sadece bilişim suçları ve siber güvenlik bakış açısıyla değil, aynı zamanda bilişim teknolojilerinin hukuki açıdan toplumda temas ettiği sosyal, ekonomik ve teknik birçok mevzunun da dikkatle ele alınması faydalı olacaktır. Bu noktada, tarım, gıda, hayvancılık ve kırsal kalkınma gibi sektörlerin; ayrıca toplumun, ülkenin ve hatta bütün insanlığın yaşam standartlarını etkilemesi hasebiyle, Adli Bilişim ve Adli Bilimler ile bağlantılı şekilde problemlerin analiz edilmesi de gelecekte incelenecek akademik çalışmalar olarak fikir verebilir.

Tarım ve gıda sektöründe bahsi geçen birçok probleme sadece teknolojik olarak bir çözüm bulmak değil, ayrıca ortaya çıkan sosyal ve hukuki yansımalarının da düzgünce ele alınarak adli süreçlerle ilgili toplumsal ve kurumsal hafızanın gelişimine katkı sunabilir. Bunun birlikte, tarımsal ürünlerin rekolte tahmini ile ilgili ortaya çıkabilecek sorunlar da, adli vakalara sebebiyet verebilir. Özellikle son birkaç yıl içinde, üretici ile tüketici, devlet ile vatandaş arasında, gıda fiyatlarındaki tutarsızlıklardan dolayı maalesef güven sorunu oluşmuştur. Ayrıca bu güven sorununun, hem kitle medyasında hem de sosyal medyada daha görünür olmasının, toplumu daha fazla rahatsız ettiği gerçeği göz önünde durmaktadır. Bu yüzden, blokzincir teknolojisinin sunduğu dağıtık mimari ve mutabakat algoritmaları ile akıllı sözleşmelerin imkan sağladığı otonom çalışma kabiliyeti bu tarz problemlerin çözümünde büyük bir potansiyel vaat etmektedir. Dolayısıyla yakın gelecekte, adli bilişim ile ilgili akademik çalışmalarda ister teorik ister pratik olsun blokzincirin ve akıllı sözleşmelerin göz ardı edilmemesi gereken teknolojiler olarak yerini aldığını görebiliriz.

Gelecekteki çalışmalara ışık tutması açısından bu çalışmada, rekolte tahmin sürecindeki aksaklıklara blokzincir ve akıllı sözleşmeler perspektifinden yeni bir yaklaşım getirilmiştir. Fakat rekolte tahmin yöntemleri, özellikle uzaktan algılama tekniklerinin sunduğu modern metotlar ile geniş bir çalışma alanı sunmaktadır. Bu sebeple, blokzincir ile sunulan bu çözüm modeline ileride nesnelerin interneti, derin öğrenme, yapay zeka ve hatta kuantum bilgisayım gibi yeni teknikler/teknolojiler eklenerek daha verimli ve başarılı çözümlerin ortaya çıkarılması mümkün olabilir.

ÖZET

Blokzincir Teknolojisi ile Rekolte Tahmin Platformu Tasarlamak

Tarımsal üretim sürecindeki belirsizlikler nedeniyle, gelişmekte olan ülkeler gıda fiyatlarının dengelenmesinde sorunlar yaşamaktadır. Tarımsal ürünlerde pazarın aktörlerini olumsuz etkileyen fiyat artışı, birçok faktörün etkisinde ciddi bir konudur. Ürünlerin rekolte tahminindeki belirsizlik, bu faktörlerden biri olarak sayılabilir. Doğru rekolte tahminini hesaplamayı amaçlayan geleneksel ve uzaktan algılama yöntemleri vardır. Ancak, bu yöntemler yalnızca ürünlerin ekim ve hasadından sonra çıktılar üretmektedir. Bu durumda, karar vericiler ellerinde fiyat istikrarı sağlamak için yeterli araçlara sahip değillerdir. Genel olarak, mevcut rekolte tahmin sistemleri merkezi bir ortamda tasarlanmıştır. Bununla birlikte, veri akışındaki sorunlar nedeniyle etkili takip yapılamayabilir. Önerilen model, piyasa koşulları hakkında önceden bilgi sağlayacak, böylece piyasa oyuncuları yatırımlarını planlamak ve önemli önlemler almak için yeterli zamana ve bilgiye sahip olacaklardır. Bu çözüm modeli ayrıca, ayrı organizasyonları bir platformda bir araya getirecek ve aralarındaki işbirliğini artıracaktır. Çözüm yeni bir teknoloji olan blokzincir üzerinde kurgulanmıştır. Her ne kadar bu teknoloji, özellikle finans sektöründe birçok alanda uygulama olanağına sahip olsa da, rekolte tahmini için ilk kez önerilmiştir. Bu çalışmada, öncelikle etkin bir rekolte taahhüt sistemi önerildi. Sistem, çiftçilerin gelecek hasat mevsimi için tarım planlarını pazarın diğer oyuncularıyla paylaşmalarını sağlayan bir platform olarak görülebilir. Ayrıca çiftçilerin başkalarının planlarını gözlemlemelerine ve yatırımlarını revize etmelerine ve gelecek sezon için gerekli adımları atmalarına olanak tanımaktadır. Dolayısıyla platform, tarımla ilgilenen tüm katılımcıları bir araya getiriyor ve erken rekolte tahmini üretiyor. Bu nedenle, tarımsal mahsul üretiminde doğabilecek aşırı dengesizlikler için gerekli önlemler önceden planlanacaktır. Blokzincir teknolojisi kullanılarak, sansüre dayanıklı, kurcalamaya karşı korumalı ve zamanla işlem görmeyen güçlü bir şekilde açık kaynak defteri sağlayan platform tasarımı önerilmiştir.

Anahtar Sözcükler: Akıllı Sözleşmeler, Blokzincir, Rekolte tahmin

SUMMARY

Designing Yield Estimation Platform by Blockchain Technology

Due to the uncertainties in the agricultural production process, developing countries have problems in balancing food prices. The price increase in agricultural products, which adversely affects the market actors, is a serious issue under the influence of many factors. Uncertainty in yield estimation of crops can be considered as one of these factors. There are traditional and remote sensing methods that aim to calculate the correct yield estimation. However, these methods only produce output after the planting season. In this case, decision-makers do not have sufficient means to ensure price stability. In general, existing yield estimation systems are designed in a centralized environment. However, effective monitoring may not be possible due to problems in the data flow. The proposed model will provide advance information on market conditions so that market players will have sufficient time and information to plan their investments and take important measures. This solution model will also bring together separate organizations on a platform and increase the cooperation between them. The solution is based on a new technology, so, the blockchain. Although this technology can be applied in many areas, especially in the financial sector, it was proposed for the initial term for yield estimation. In this study, an effective yield commitment system was first proposed. The system can be seen as a platform that allows farmers to share their agricultural plans with other players of the market for the next harvest season. It also allows farmers to observe others' plans and revise their investments and take the necessary steps for the next season. Therefore, the platform brings together all participants interested in agriculture and produces an early yield estimate. So, necessary measures for excessive imbalances in agricultural crop production will be planned in advance. Using blockchain technology, it is proposed to design platform that provides a censorship resistant, tamper-proof, and strongly immutable public ledger of time-stamped transactions.

Keywords: Blockchain, Smart contracts, Yield estimation

KAYNAKLAR

ABARES (2019). Publications, Data and News. Erişim Adresi: [www.agriculture.abares.gov.au]. Erişim Tarihi: 9/2/2019

ABUZALATA, M., MOMANİ, M., FAYYAD, S., & ABU-EİN, S. (2012). A practical design of anti-theft car protection system based on microcontroller. *American Journal of Applied Sciences, 9*(5), 709.

ANDROULAKI, E., CACHIN, C., DE CARO, A., SORNIOTTI, A., & VUKOLIC, M. (2017). Permissioned blockchains and hyperledger fabric. *ERCIM NEWS*, (110), 9-10.

BAGCHI, R. (2017). Using Blockchain Technology and Smart Contracts for Access Management in IoT devices.

BALIGA, A., SUBHOD, I., KAMAT, P., & CHATTERJEE, S. (2018). Performance evaluation of the quorum blockchain platform. *arXiv preprint arXiv:1809.03421*.

BALLANTYNE, P. G., & CHAVEZ-TAFUR, J. (2019). *Enhancing next-generation ACP agribusiness through digitalisation*. CTA.

BARNABY, G. A., & RUSSELL, L. A. (2016). Crop insurance will be at the center of the 2019 Farm Bill Debate. *Choices*, *31*(316-2016-7834).

BASHIR, I. (2018). *Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing Ltd.

BERMEO-ALMEİDA, O., CARDENAS-RODRİGUEZ, M., SAMANİEGO-COBO, T., FERRUZOLA-GÓMEZ, E., CABEZAS-CABEZAS, R., & BAZÁN-VERA, W. (2018, November). Blockchain in agriculture: a systematic literature review. In *International Conference on Technologies and Innovation* (pp. 44-56). Springer, Cham.

BESSANI, A. J. a. SOUSA, and EEP Alchieri,"State machine replication for the masses with bft-smart,". In *Proceedings of the 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN'14,(Washington* (pp. 355-362).

BHARGAVAN, K., DELIGNAT-LAVAUD, A., FOURNET, C., GOLLAMUDI, A., GONTHIER, G., KOBEISSI, N., ... & ZANELLA-BEGUELIN, S. (2016, October). Formal verification of smart contracts: Short paper. In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security* (pp. 91-96). ACM.

BITCOIN WIKI. (2018). Smart Property. Erişim Adresi: [https://en.bitcoin.it/wiki/Smart_Property]. Erişim Tarihi: 14/5/2019.

BOOGAARD, K. (2018). *A model-driven approach to smart contract development* (Master's thesis).

BRANCO, F., MOREİRA, F., MARTİNS, J., AU-YONG-OLİVEİRA, M., & GONÇALVES, R. (2019, April). Conceptual Approach for an Extension to a Mushroom Farm Distributed Process Control System: IoT and Blockchain. In *World Conference on Information Systems and Technologies* (pp. 738-747). Springer, Cham.

GE, L., BREWSTER, C., SPEK, J., SMEENK, A., TOP, J., VAN DİEPEN, F., ... & DE WİLDT, M. D. R. (2017). *Blockchain for agriculture and food: Findings from the pilot study* (No. 2017-112). Wageningen Economic Research.

BUTERIN, V. (2013). Ethereum white paper. *GitHub repository*, 22-23.

CARO, M. P., ALİ, M. S., VECCHİO, M., & GİAFFREDA, R. (2018, May). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)* (pp. 1-4). IEEE.

CASTRO, M., & LISKOV, B. (1999, February). Practical Byzantine fault tolerance. In *OSDI* (Vol. 99, No. 1999, pp. 173-186).

CHAFFIN, B. (2009). *Crop yield and revenue insurance: choosing between policies that trigger on farm vs. County indexes* (No. 1097-2016-88612).

CHLİNGARYAN, A., SUKKARİEH, S., & WHELAN, B. (2018). Machine learning approaches for crop yield prediction and nitrogen status estimation in precision agriculture: A review. *Computers and electronics in agriculture*, *151*, 61-69.

CROMAN, K., DECKER, C., EYAL, I., GENCER, A. E., JUELS, A., KOSBA, A., ... & SONG, D. (2016, February). On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security* (pp. 106-125). Springer, Berlin, Heidelberg.

DEFRA (2019). Crop Yields and Production Estimates. Erişim Adresi: [https://www.gov.uk/defra]. Erişim Tarihi: 11/2/2019.

DELÉCOLLE, R., MAAS, S. J., GUÉRİF, M., & BARET, F. (1992). Remote sensing and crop production models: present trends. *ISPRS Journal of Photogrammetry and Remote Sensing*, *47*(2-3), 145-161.

DOGANTUNA T., CERAN A. A., TUGRUL B., DEMİR S., OSMANOGLU M., and BOSTANCİ G. E., “Designing yield estimation mechanism using blockchain

technology," in 2018 International Conference on Theoretical and Applied Computer Science and Engineering (ICTACSE), 2018, pp. 82–85

DOKTAR (2019). Ürünler, Medya. Erişim Adresi: [http://doktar.com]. Erişim Tarihi: 2/6/2019.

EŞTÜRK, Ö., & ALBAYRAK, N. Tarım Ürünleri-Gıda Fiyat Artışları ve Enflasyon Arasındaki İlişkinin İncelenmesi. *Uluslararası İktisadi ve İdari İncelemeler Dergisi*, 147-158.

ETHEREUM Solidity, (2019). Introduction to Smart Contract. Erişim Adresi: [https://solidity.readthedocs.io/en/v0.5.3]. Erişim Tarihi: 21/3/2019

EUROSTAT, EC., (2019). Annual Crop Statistics Handbook. Erişim Adresi: [https://ec.europa.eu/eurostat/cache/metadata]. Erişim Tarihi: 10/2/2019.

FARRELL, G., TSELONİ, A., & TİLLEY, N. (2011). The effectiveness of vehicle security devices and their role in the crime drop. *Criminology & Criminal Justice*, *11*(1), 21-35.

FRÖBERG, E., INGRE, G., & KNUDSEN, S. (2018). Blockchain and prediction markets: An analysis of three organizations implementing prediction markets using blockchain technology, and the future of blockchain prediction market.

GULED, P. M. (2007). *Crop coverage and yield estimation studies in sugarcane through use of remote sensing techniques*(Doctoral dissertation, UNIVERSITY OF AGRICULTURAL SCIENCES, DHARWAD).

HABER, S., & STORNETTA, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.

HUANG, C., WANG, Z., CHEN, H., HU, Q., ZHANG, Q., WANG, W., & GUAN, X. (2019). Repchain: A reputation based secure, fast and high incentive blockchain system via sharding. *arXiv preprint arXiv:1901.05741*.

HYPERLEDGER-FABRIC, (2019). Smart Contracts and Chaincode. Erişim Adresi:[https://hyperledger-fabric.readthedocs.io/en/smartcontract.html]. Erişim Tarihi: 18/6/2019.

JØRGENSEN, S. E. (1994). Models as instruments for combination of ecological theory and environmental practice. *Ecological Modelling*, *75*, 5-20.

KAPTCHUK, G., GREEN, M., & MİERS, I. (2019). Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers. In *NDSS*.

KIYMAZ, T. (2008). *Dünya tarım piyasalarında serbestleşmenin Türk tarımına fiyat ve gelir yönünden yansıması*. DPT.

KIM, N., HA, K. J., PARK, N. W., CHO, J., HONG, S., & LEE, Y. W. (2019). A Comparison Between Major Artificial Intelligence Models for Crop Yield Prediction: Case Study of the Midwestern United States, 2006–2015. *ISPRS International Journal of Geo-Information*, *8*(5), 240.

LAMPORT, L. (2001). Paxos made simple. *ACM Sigact News*, *32*(4), 18-25.

LEI, K., ZHANG, Q., XU, L., & QI, Z. (2018, December). Reputation-based Byzantine Fault-Tolerance for Consortium Blockchain. In *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)* (pp. 604-611). IEEE.

LISK ACADEMY (2019). Blockchain Basics. Erişim Adresi: [https://lisk.io/academy]. Erişim Tarihi: 3/7/2019.

LUCENA, P., BİNOTTO, A. P., MOMO, F. D. S., & KİM, H. (2018). A case study for grain quality assurance tracking based on a Blockchain business network. *arXiv preprint arXiv:1803.07877*.

LUO, W., & HENGARTNER, U. (2010, November). Veriplace: a privacy-aware location proof architecture. In *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems* (pp. 23-32). ACM.

MAAS, S. J. (1988). Use of remotely-sensed information in agricultural crop growth models. *Ecological modelling*, *41*(3-4), 247-268.

MANGO RESEARCH (2019). Blockchain vs. DLT. Erişim Adresi: [https://mangoresearch.co]. Erişim Tarihi: 3/6/2019.

MARMARABİRLİK (2015). Kurumsal, Mevzuat ve Bülten. Erişim Adresi: [www.marmarabirlik.com.tr]. Erişim Tarihi: 12/2/2019.

MİLLER, A. (2019). Permissioned and Permissionless Blockchains. *Blockchain for Distributed Systems Security*, 193-204.

MO, X., LİU, S., LİN, Z., XU, Y., XİANG, Y., & MCVİCAR, T. R. (2005). Prediction of crop yield, water consumption and water use efficiency with a SVAT-crop growth model using remotely sensed data on the North China Plain. *Ecological Modelling*, *183*(2-3), 301-322.

MONTEİTH, J. L. (1972). Solar radiation and productivity in tropical ecosystems. *Journal of applied ecology*, *9*(3), 747-766.

NASS, USDA (2019). Newsroom, Publications and Surveys. Erişim Adresi: [https:/www.nass.usda.gov]. Erişim Tarihi: 8/2/2019.

NAKAMOTO, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

NGUYEN, G. T., & KİM, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information processing systems, 14*(1).

OLSON, K., BOWMAN, M., MİTCHELL, J., AMUNDSON, S., MİDDLETON, D., & MONTGOMERY, C. (2018). Sawtooth: An Introduction. *The Linux Foundation, Jan*.

ONGARO, D., & OUSTERHOUT, J. (2014). In search of an understandable consensus algorithm. In *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14)* (pp. 305-319).

ÖĞÜT H., (2015). Tarımın İleri Teknoloji İle Buluşma Noktası: Hassas Tarım. Erişim Adresi: [www.turktob.org.tr/upload/dergi/14/38-41.pdf], Erişim Tarihi: 2/7/2019.

PAHLAJANI, S., KSHIRSAGAR, A., & PACHGHARE, V. (2019, April). Survey on Private Blockchain Consensus Algorithms. In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)* (pp. 1-6). IEEE.

PAPA, S. F. (2017, June). Use of Blockchain technology in agribusiness: transparency and monitoring in agricultural trade. In *2017 International Conference on Management Science and Management Innovation (MSMI 2017)*. Atlantis Press.

PATİL, A. S., TAMA, B. A., PARK, Y., & RHEE, K. H. (2017). A framework for blockchain based secure smart green house farming. In *Advances in Computer Science and Ubiquitous Computing* (pp. 1162-1167). Springer, Singapore.

PERRIN, R. K. (1968). Analysis and prediction of crop yields for agricultural policy purposes.

PETERSON, J., & KRUG, J. (2015). Augur: a decentralized, open-source platform for prediction markets. *arXiv preprint arXiv:1501.01042*.

PETERSON, J., KRUG, J., ZOLTU, M., WILLIAMS, A. K., & ALEXANDER, S. (2015). Augur: a decentralized oracle and prediction market platform. *arXiv preprint arXiv:1501.01042*.

PRASAD, A. K., CHAİ, L., SİNGH, R. P., & KAFATOS, M. (2006). Crop yield estimation model for Iowa using remote sensing and surface parameters. *International Journal of Applied Earth Observation and Geoinformation*, *8*(1), 26-33.

REYNOLDS, C. A., YİTAYEW, M., SLACK, D. C., HUTCHİNSON, C. F., HUETE, A., & PETERSEN, M. S. (2000). Estimating crop yields and production by integrating the

FAO Crop Specific Water Balance model with real-time satellite data and ground-based ancillary data. *International Journal of Remote Sensing*, *21*(18), 3487-3508.

RUSSELL, G., JARVIS, P. G., & MONTEITH, J. L. (1989). Absorption of radiation by canopies and stand growth. *Plant canopies: their growth, form and function*, *31*, 21-39.

QUORUM, Raft-based consensus for Ethereum/Quorum (2019). [Online]. Erişim Adresi: [https://github.com/jpmorganchase/quorum/blob/master/raft/doc.md] Erişim Tarihi: 6/7/2019

SAWASAWA, H. L. (2003). Crop yield estimation: Integrating RS, GIS, and management factors. *International Institute for Geo-information Science and Earth Observation, Enschede The Netherlands*.

SCHULER, R. T. (2002, July). Remote sensing experiences in production fields. In *Proceedings of the... Wisconsin Fertilizer, Aglime and Pest Management Conference* (Vol. 41). Cooperative Extension, University of Wisconsin--Extension; College of Agricultural and Life Sciences, University of Wisconsin--Madison.

SHAFİAN, S., & VALADANZOUJ, M. (2009). Assessment crop yield estimation methods by using stellite imagery. *Geospatial World*, 1-2.

SUKHWANİ, H., MARTÍNEZ, J. M., CHANG, X., TRİVEDİ, K. S., & RİNDOS, A. (2017, September). Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). In *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)* (pp. 253-255). IEEE.

SZABO, N. (1994). Smart contracts. *Unpublished manuscript*.

TARBİL (2019). Gerçek Zamanlı Gözlem ve Rekolte İzleme Sistemi. Erişim Adresi: [https://tbs.tarbil.gov.tr]. Erişim Tarihi: 13/2/2019.

TARIM VE ORMAN BAK. (2019). Bilgi Merkezi, Erişim Adresi: [www.tarimorman.gov.tr] Erişi Tarihi: 17/4/2019.

TEKNOCHAIN (2019). Teknik Detayları ile Blockchain, Erişim Adresi: [https://teknochain.com] Erişim Tarihi: 10/06/2019.

THENKABAIL, P. S., LYON, J. G., & HUETE, A. (2018). *Advanced Applications in Remote Sensing of Agricultural Crops and Natural Vegetation*. CRC Press.

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

TRIPOLI, M., & SCHMIDHUBER, J. (2018). Emerging Opportunities for the Application of Blockchain in the Agri-food Industry. *FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA*, *3*.

TSE, D., ZHANG, B., YANG, Y., CHENG, C., & MU, H. (2017, December). Blockchain application in food supply information security. In *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 1357-1361),IEEE.

TÜBİTAK BİLGEM (2018). Blokzincir Teknolojileri, Erişim Adresi: [http://blockchain.bilgem.tubitak.gov.tr/bz-calistay/blok-zincir.html] Erişim Tarihi: 18/06/2019.

TÜRKİYE CUMHURİYET MERKEZ BANKASI (TCMB). (2018). TCMB Enflasyon Raporu 2018-III, Erişim Adresi: [https://www.tcmb.gov.tr/wps/wcm] Erişim Tarihi: 20.01.2019.

TÜRKİYE İSTATİSTİK KURUMU (TÜİK). (2019). Veritabanları, Resmi İstatistik Portalı, Erişim Adresi: [www.tuik.gov.tr] Erişim Tarihi: 16/4/2019.

TÜRKİYE ZİRAAT ODALARI BİRLİĞİ (TZOB). (2019). Mevzuat, Yayınlar, Erişim Adresi: [www.tzob.org.tr] Erişim Tarihi: 1/4/2019.

USTA, A., & DOĞANTEKİN, S. (2017). Blockchain 101. *Kapital Medya Hizmetleri A. fi.*

VUKOLIĆ, M. (2017, April). Rethinking permissioned blockchains. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 3-7). ACM.

WATANABE, H., FUJIMURA, S., NAKADAIRA, A., MIYAZAKI, Y., AKUTSU, A., & KISHIGAMI, J. J. (2015, October). Blockchain contract: A complete consensus using blockchain. In *2015 IEEE 4th global conference on consumer electronics (GCCE)* (pp. 577-578). IEEE.

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

YU, J., KOZHAYA, D., DECOUCHANT, J., & VERİSSİMO, P. (2019). RepuCoin: Your reputation is your power. *IEEE Transactions on Computers*.

ZİRAAT MÜHENDİSLER ODASI (ZMO), (2019). E-Kütüphane, Yayınlar, Erişim Adresi: [www.zmo.org.tr] Erişim Tarihi: 12/2/2019.

ÖZGEÇMİŞ

I-Bireysel Bilgiler

Tuncay DOĞANTUNA
Eskişehir
16.08.1987
Türk
Evli
Turan Güneş Bulvarı No:68 Çankaya/ANKARA
+90 541 470 64 87

II- Eğitim

Ankara Üniversitesi, Adli Bilişim II. Öğretim Tezli Yüksek Lisans, Ankara, (2016 – Halen)

Anadolu Üniversitesi, Uluslararası İlişkiler AÖF Lisans Programı, Eskişehir, (2009 – 2016)

Süleyman Demirel Üniversitesi, Elektronik Haberleşme Mühendisliği Lisans Programı, Isparta, (2004 – 2011)

Eskişehir Atatürk Lisesi (2001 – 2004)

III- Ünvanlar

Yerinde Kontrol Uzmanı (2012 – 2014)
Destek Hizmetleri Uzmanı (2014 – 2015)
Bilgi Sistemleri Uzmanı (2015 – 2016)
Ağ ve Güvenlik Uzmanı (2015 – Halen)

IV- Mesleki Deneyim

Yerinde Kontrol Uzmanı, TKDK Ağrı İl Koordinatörlüğü, Ağrı, (2012 – 2014)

Destek Hizmetleri Uzmanı, TKDK Ağrı İl Koordinatörlüğü, Ağrı, (2014 – 2015)

Bilgi Sistemleri Uzmanı, TKDK Bilgi Sistemleri Koordinatörlüğü, Ankara, (2015 – 2016)

Ağ ve Güvenlik Uzmanı, TKDK Bilgi Sistemleri Koordinatörlüğü, Ankara, (2015 – Halen)

V- Üye Olduğu Bilimsel Kuruluşlar

IEEE

VI- Bilimsel İlgi Alanları

ICTACSE Güz 2018 Makale Bildirimi

Siber Güvenlik, Blokzincir ve Kriptoloji literatür takibi

VII- Bilimsel Etkinlikleri

Tübitak ve Elginkan Vakfı Sponsorluğunda Ege Üniversitesi EBİLTEM Proje Pazarı 2009; Ödül: En İyi Fikir Ödülü, Proje Adı: TiDi.Sec VoIP-Cryptor