BLOCKCHAIN BASED NATIONAL DONATION CHAIN PROJECT (BLOKZİNCİR TEMELLİ MİLLİ BAĞIŞ ZİNCİRİ PROJESİ)

Conference Paper · February 2021

CITATIONS
0

READS
15

4 authors:

Mustafa Takaoğlu
Istanbul Aydin University
15 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Naim Ajlouni
Istanbul Aydin University
48 PUBLICATIONS **150** CITATIONS
SEE PROFILE

Adem Ozyavas
Istanbul Aydin University
4 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Alaa Ali Hameed
Istanbul Sabahattin Zaim University
28 PUBLICATIONS **68** CITATIONS
SEE PROFILE

BLOKZİNCİR TEMELLİ MİLLİ BAĞIŞ ZİNCİRİ PROJESİ

Mustafa Takaoğlu[1], Naim Ajlouni[1], Adem Özyavaş[1], Alaa Ali Hameed[2]

[1]*İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, İstanbul, TURKEY*
[2]*İstanbul Sabahattin Zaim Üniversitesi, Mühendislik Fakültesi, İstanbul, TURKEY*

mustafatakaoglu@aydin.edu.tr
ORCID: 0000-0002-1634-2705

ÖZET

Yürütmekte olduğumuz Milli Bağış Zinciri projesi tamamen blokzincir teknolojisi ve bilgisayar bilimleri kullanılarak geliştirilmiş bir yardımlaşma sistemidir. Türkiye ve uygulanabilecek tüm dünya ülkelerinin dijitalleşmesine katkı sağlayacak, şeffaf ve güvenilir bir sistemdir. Gerek hâlihazırdaki kurum ve kuruluşların iş yükünün azaltılması gerekse de özellikle vakıflar üzerinde oluşan güven sorunlarının aşılması açısından önemli bir çözüm önerisidir. Önermekte olduğumuz bu çalışma, insanların hayatlarını doğrudan etkileyecek olması ve oluşturacağı yeni ekosistemin doğuracağı sonuçlar dikkate alındığında çok disiplinli bir çalışma konusu olarak karşımıza çıkmaktadır. Kısaca önermekte olduğumuz fikir, ihtiyaç sahipleri ve yardımseverleri bir platformda buluşturup birbirlerinden habersiz bir şekilde yardımlaşmanın amaçlandığı blokzincir temelli bir çalışmadır. İhtiyaç sahiplerinin bilgilerine oluşturulacak bir web sitesi üzerinden ulaşılacak olup, ihtiyaç sahibinin kripto cüzdanına yardımseverlerin yapmak istediği miktarda kripto para göndermesi ile gerçekleşen mühendislik temelli bir sosyal yardımlaşma projesidir. Temelinde blokzincir teknolojisi yatmaktadır. Kullanılacak kripto paranın milli olması ve sabit kura sahip olması büyük önem taşımaktadır çünkü günümüz kripto para kurlarında karşılaşılan yüksek değer sıçramaları göze alınabilecek bir durum değildir. Bu nedenle projemizde sabit kurlu kripto para kullanımı planlanmaktadır. Milli Bağış Zinciri Projesi, yüz yıllar öncesine dayanan yardımlaşma kültürümüze uygun, gizliliğin yüksek, şeffaflığın tam olduğu, yardım maliyetinin yok denecek kadar az olduğu yeni bir çözüm önerisi olması amacıyla geliştirilmiştir.

Anahtar Kelimeler: *Blokzincir Teknolojisi, Milli Bağış Zinciri, Kripto Paralar, Kripto Cüzdanlar, biLira.*

BLOCKCHAIN BASED NATIONAL DONATION CHAIN PROJECT

ABSTRACT

The National Donation Chain project that we are conducting is a donation system developed using blockchain technology and computer science. For Turkey and all countries in the world which can be applied will contribute to the digitalization, it is a transparent and reliable system. It is an important solution proposal both for reducing the workload of existing institutions and organizations, and especially for overcoming the trust problems on foundations. This study, which we propose, directly affects people's lives, and when it comes to the results of the new ecosystem it creates, it is a multidisciplinary study subject. The idea that we propose briefly is a blockchain-based study that brings together poor and benefactor people on a platform and helps them to be unaware of each other when they are supporting each other. It is an engineering-based social assistance project that is realized by sending the amount of crypto money that benefactors want to make charity to the crypto wallet of the poor people through a website to be created. At its core lies blockchain technology. It is very important that the crypto money to be used is national and has a fixed value. Because the high value jumps encountered in today's crypto currency exchange rates are not something that can be taken into risk. For this reason, fixed exchange rate crypto money is used in our project. The National Donation Chain Project was developed with the aim of being a new solution proposal in accordance with our culture of charity dating back hundreds of years, with high confidentiality, full transparency, and scarcely any aid costs.

Keywords: *Blockchain Technology, National Donation Chain, Crypto Currencies, Crypto Wallets, biLira.*

1. GİRİŞ

Yardımlaşmak temel insani bir faaliyettir. İnsanın sahip olduğu merhamet ve duygudaşlık olgusu, zor durumda bulunan kişilere, bir gün kendilerinin de aynı durumda olabileceği bilinciyle yardımcı olmak ve bunu karşısındakinin onurunu kırmadan, belirli bir hassasiyet çerçevesinde yapılmaya çalışılan bir süreçtir. Sadece kendi kültürümüzle sınırlı olmayan yardımlaşma, birçok farklı millet ve kültürlerde gerçekleştirilen, sürecin merkezinde bir numaralı aktör olarak insanın bulunması sebebiyle de çokça aksiliklerin yaşandığı bir süreçtir. Bu sebeple günümüzde yardımlaşma vaadiyle insanların iyi niyetlerini suistimal eden kişilerin önüne geçilebilmesi için, 2860 sayılı Yardım Toplama Kanunu'nda ve Yardım Toplama Esas ve Usulleri Hakkında Yönetmelikte hukuken yardımlaşma faaliyeti gösterebilecek kurum ve kuruluşlar belirlenmiş ve yetkileri tanımlanmıştır. Ancak %100 şeffaflığın olmadığı, kamunun arzu etmesi durumunda, kimseden izin almadan, yapılan yardım bütçelerini incelemesi çok kolay olmadığı için birçok suçlayıcı iddia ve yolsuzluk söylentileri oluşmaktadır. Günümüzde çokça karşılaştığımız, dezenformasyon çalışmalarının da yapıldığı gerçeği unutulmadan, düzgün işleyen mekanizmaların güvenilebilirliğinin daha da arttırılacağı, sorunlu yardım mekanizmaların da ortadan kaldırılacağı, şeffaf ve yenilikçi sistemlere ihtiyaç olduğu görülmektedir [19]. Bu sebeple uygulama alanlarının genişlediği blokzincir teknolojisi gibi yenilikçi çözümlerin, hâlihazırdaki yardımlaşma süreçlerinde daha güvenilir ve şeffaf çözümler önerilmesinin sağlanmasında kullanılması düşünülmelidir. Çalışmamızın ortaya çıkmasının sebebi de tam olarak budur. 2008 yılında Satoshi Nakamoto mahlaslı yazarın paylaşmış olduğu Bitcoin: "A Peer to Peer Electronic Cash System" isimli makale ile hayatlarımıza yeni bir finansal çözüm önerisi olarak girmiştir [1].

Bitcoin önerisinin ortaya çıkış sebebi olarak; dünyanın birçok kez karşılaştığı ekonomik krizler ve bu krizlerin arkasındaki asıl suçlu olarak görülen merkezi otoritelere duyulan güvensizliğin doğurduğu bir tepki olabileceği düşünüldüğü gibi, zeki bir suçlunun para transferini gerçekleştirmek için planladığı bir çözüm önerisi olduğu da düşünülmektedir. Sebebi ne olursa olsun Bitcoin kripto parasının arkasındaki yaratıcı güç olan blokzincir teknolojisi üzerinde durulması gereken ve günümüzde de çalışmaların bu konuda yapıldığı bir araştırma alanıdır [14]. Öncelikle blokzincir teknolojisi 2008 yılında ortaya atılmış bir öneri değildir. Esasen bir kriptoloji bilimi çalışma konusu olan ve 1950'li yıllarda tanıtılan özütleme (Hash) algoritmaları ile temellerinin atıldığını söyleyebileceğimiz blokzincir teknolojisi, Ralph C. Merkle'ın 1970'li yıllarda tanıttığı Merkle ağaçlarından faydalanan ve ilk blokzincir temelli kripto para uygulaması olarak da eCash isimli çalışmanın gösterilebileceği eski bir çalışma konusudur [2]. Günümüzde bilgisayar teknolojilerinin çalışma konularının çok geniş olması ve bilgisayar biliminin de özünde kriptolojik bir çalışma konusu olduğu düşünüldüğünde, blokzincir teknolojisi %100 bilgisayar bilimleri ve kriptoloji çalışma konusudur denilmektedir [15].

Mühendislik kavramı, kelime anlamına da paralel olacak şekilde, günümüzde sorun çözen kişi olarak algılanmaktadır. Mühendislerin ve tabii ki akademide çalışmalarına devam eden farklı

disiplinlerdeki bilim insanlarının, karşılaşılan teknolojik yeniliklerin anlaşılması ve potansiyelin doğru analiz edilmesi açısından sorumluluk sahibi olduğu unutulmamalıdır. Çalışmamız bu anlayışla ortaya çıkmış ve hali hazırda yeniliklere ihtiyaç duyulan bir alanda blokzincir teknolojisinin uyarlanması amaçlanmıştır. Günümüzde yardım faaliyetleri yıllardır süregelen ekonomik araçlar vasıtasıyla devam ettirilmektedir. İhtiyaç sahiplerine gıda, giyim, eğitim ve nakdi yardımlar bakanlık, belediyeler ve vakıflar vasıtasıyla geliştirilen mekanizmalarla gerçekleştirilmektedir. Tüm bu yardımların yapılmasında kullanılan ana araç çok genel bir tabirle paradır. Yardım amacıyla toplanan ve kullanılan meblağın tümünün kayıt altında olması ve hesap verilebilir olması gerekmektedir. Ancak hesap verilebilirlik aşamasında şeffaflığın yeteri kadar yüksek olmaması sebebiyle toplum tarafından hoş görülmeyecek adımlar gerçekleşiyor olabilir. Önermekte olduğumuz Milli Bağış Zinciri, MBZ ile yapılacak tüm nakdi yardımların kayıt altına alınması ve tüm paydaşlarca görüntülenmesine imkân tanınması amaçlanmaktadır. Günümüzde yardımlaşmak isteyen insanlar haberdar oldukları ihtiyaç sahiplerine yaptıkları yardımlar dışında genellikle güvendikleri vakıflar vasıtasıyla yardımlaşma süreçlerine dâhil olurlar [23]. Milli Bağış Zinciri sisteminde aynı Bitcoin blokzincir sisteminde olduğu gibi arada bir aracı olmadan, yardımsever insanlarla ihtiyaç sahibi kişileri, tarafları birbirlerinden habersiz olarak buluşturan bir platform sunulmaktadır. Ancak ihtiyaç sahibi olan kişilerin sisteme kaydedilmesi anlaşılacak resmi kurumlardan gönderilen listeler dikkate alınarak yapılması düşünülmüştür. Bu sebeple projemizin öncelikli amacı bir kamu kuruluşuyla çalışılması ve ihtiyaç sahibi olan kişilerin şaibesiz bir şekilde sisteme dâhil edilmesidir.

Milli Bağış Zinciri teoride gerçekleştirilmesi çok basit bir projedir. Hali hazırda oluşturulmuş blokzincir temelli sabit kurlu bir kripto para sisteminde, tüm paydaşların kullanılan sistemin kripto parasıyla uyumlu birer kripto cüzdanı sahibi olmasıyla blokzincir sürecinin tamamlandığı bir projedir. Öncelikli amacın Türkiye Cumhuriyet Merkezi Bankası'nın geliştireceğini duyurduğu milli kripto para ile yahut tanıtımı yapılmış ve kullanıma açık olan biLira stabil kripto parası gibi kripto paraların kullanılmasının olduğu bir sistemdir. Burada kullanılan kripto paranın günümüzde kullanılan ve sabit değeri olmayan kripto paralardan seçilmemesi çok büyük önem taşımaktadır. Çünkü günümüzde işlem gören Bitcoin ve tüm altcoinlerin değerinde karşılaşılan dalgalanmalar göze alınabilecek bir risk değildir. Bu sebeple kullanılan kripto paranın değerinin o ülkenin milli parasının değerine sabitlenmiş olması gerekmektedir. Seçilen kripto paranın yardımseverin kripto cüzdanından ihtiyaç sahibinin kripto cüzdanına transfer edilmesiyle yardımlaşma süreci tamamlanacaktır. Kullanılan kripto paranın değer olarak Türk Lirası ile aynı değerde olması sayesinde, hiçbir zorluk yaşanmadan, gönderilen ücretler anlaşmalı platform ve bankalar üzerinden kullanılabilecektir.

Projemiz iki aşamadan oluşmaktadır. İlk aşaması şu anda sürdürmekte olduğumuz gereksinimlerin belirlenmesi aşamasıdır. İkinci aşama ise kısaca Milli Bağış Zinciri projesinin uygulanmasıdır. İkinci aşama iki bölümden oluşmaktadır. Birincisi kullanılacak kripto para birimine göze sistemin ve cüzdanların oluşturulması, ikinci aşaması ise tarafların buluşturulacağı ve yardımlaşma

işleminin geçekleşeceği platformun oluşturulmasıdır. Ancak geliştirilmesi sürdürülen bu projeden beklentinin gerçekçi olması gerekmektedir. Önermekte olduğumuz projenin geleceği, ilerleyen bölümlerde açıklandığı üzere, blokzincir teknolojisinin gelişimine ve aynı kredi kartlarında olduğu gibi kullanımının yaygınlaşmasına bağlıdır. Bugünden yapılacak yatırım ve çalışmalar, gelecekte yaşanacak değişimlere çok daha hızlı ve düşük maliyetlerle uyum sağlanmasına yarayacaktır. Araştırma ve geliştirmenin amacı da esasen budur. Projemizin uygulanmasına imkân sağlayacak teknolojik altyapının yaygınlaşması durumunda, hayatlarımıza girecek Milli Bağış Zinciri ile şeffaflığın tam olduğu, güvenilir ve herkesi kapsayan bir yardımlaşma sisteminin oluşturulmasını amaçlanmaktadır.

Çalışmamızın ikinci bölümünde genel olarak blokzincir teknolojisi hakkında bilgiler paylaşılmış ve blokzincir mimarisinin incelendiği kısımda şu alt başlıklar hakkında bilgiler verilmiştir: İşlem, Yaratılış Bloku ve Blok Yapısı, Özüt Algoritmaları ve Özüt İşaretçisi, Merkle Ağacı, Uzlaşma Algoritmaları, Kripto Paralar ve Kripto Cüzdanlar. Üçüncü bölümde Milli Bağış Zinciri Platformu yani çalışmamızın ne olduğu ve nasıl çalışacağı hakkında gerekli bilgiler paylaşılmıştır. Dördüncü bölüm olan Sonuç ve Tartışma'da projemizin geliştirilme aşamasında elde edilen sonuçlar ve bunlar üzerine görüşlerimiz paylaşılmıştır.

2. BLOKZİNCİR TEKNOLOJİSİ

Blokzincir teknolojisi en kısa tanımı ile dağıtık bir veri merkezidir [5]. Eşler arası (P2P) ağ üzerine kurulmuş, arada üçüncü bir otoritenin bulunmadığı yani âdemi merkeziyetçi bir yapıdadır [13]. Blokzincir sistemi oluşturulurken belirlenmiş uzlaşma algoritmasına göre onaylanan ve gerçekleştirilen işlemlerin kayıtlarının bloklar halinde saklandığı bu sistem; tek yönlü veri kaydı ve üzerinde değişiklik yapılmasına müsaade etmemesi sebebiyle oldukça güvenli ve erişim hakkı olan kullanıcılar için şeffaf bir yapıdadır [6]. Örneğin 2009 yılında kullanılmaya başlanılan Bitcoin kripto parası, günümüze kadar kesintisiz bir şekilde kullanılmaya devam etmiş ve geçen bu süreç içerisinde gerçekleşen tüm işlemlerin kayıtları ağ üzerinde bloklar halinde saklanmış olup, arzu edilmesi durumunda tüm işlem kayıtları kullanıcılar tarafından görülebilmektedir. 2008 yılında yayınlanan Bitcoin makalesi incelendiğinde, yapılmak istenen işin dijital varlıkların dağıtık veri merkezlerinde (defterlerinde) sahipliklerinin takip edilmesi olduğu görülmektedir [3]. Bu doğrultuda blokzincir teknolojisi uygulama alanlarının sadece finans sektörü ile sınırlanamayacak durumda olduğu fark edilmiş ve günümüzde neredeyse her sektörde uyarlama çalışmalarının yapıldığı görülmektedir.

Blokzincir teknolojisinin Bitcoin ile finansal bir çözüm önerisi olarak ortaya atılmasına (Literatürde Bitcoin 1.0'da denilmektedir.) Blokzincir 1.0 denilmektedir. Karşılaşılan belirli durumlarda sürekli aynı işi yapan kodlara verilen isim olan Akıllı Sözleşmelerin blokzincir sistemlerine dinamizm getirmesinin anlaşılması ve uygulamalarının yapılması sonrasında geçilen sürece Blokzincir 2.0 denilmiştir. Blokzincir teknolojisinin finans dışı alanlarda uygulamalarının araştırılması ve

denemelerinin yapılmasına da Blokzincir 3.0 denilmiştir. Günümüzde yapay zeka ve makine öğrenmesi konularının blokzincirle birlikte kullanılması çalışmalarının Blokzincir 4.0 olarak adlandırılabileceği üzerinde durulmaktadır [21].

Blokzincir sistemlerine erişim hakkı olan kullanıcılar (düğümler) için işlem kayıtlarının incelenmesi %100 şeffaf bir şekilde gerçekleştirilebilmektedir [24]. Ancak her blokzincir sisteminde işlem kayıtlarına erişmek mümkün değildir. Erişim hakkı dahi olan sistemlerde işlem kayıtlarına ulaşım sınırlandırılabilir. Blokzincir sistemine erişim hakkı kurulan sistemin özelliğine göre değişmektedir. Örneğin açık (izinsiz) bir blokzincirde isteyen herkes kullanıcı olarak sisteme kayıt olabilir ve bu sistemde özgürce işlem yapabilirler [11]. Blokzincire erişimin bir izne tabii olduğu durumlarda özel (izinli) blokzincir kavramı karşımıza çıkar [9]. Şeffaflığın çok yüksek olmaması gereken örneğin şirket içi uygulamalarında kullanılmaktadır. Konsorsiyum blokzincirlerinde ise açık ve özel blokzincir sistemlerinin özelliklerinin bir arada bulunduğu bir yapıdır. Sistemde seçilmiş ve otorite olarak belirlenmiş kullanıcılar (düğümler) yönetici durumundadır.

2.1. Blokzincir Mimarisi

Genel blokzincir mimarisini anlamak için bazı kavramlar hakkında bilgi sahibi olunması gerekmektedir. Bunlar sırasıyla işlem, yaratılış bloku ve blok yapısı, özüt algoritmaları ve özüt işaretçisi, Merkle ağacı ve uzlaşma algoritmaları, kripto paralar ve kripto cüzdanlarıdır.

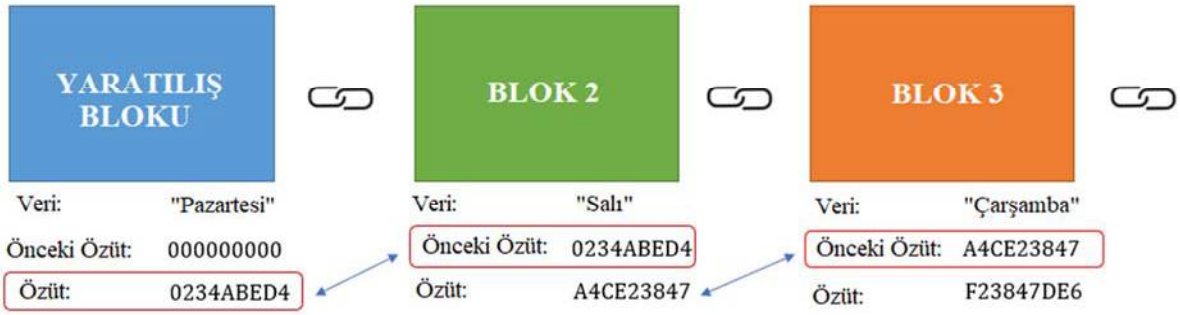
2.1.1. İşlem

Blokzincir sisteminde kaydı tutulan, değişimi gerçekleşen değerin verilerinin bulunduğu yapılardır. İşlemler blokzincir sisteminde kabul edilen protokol doğrultusunda gerçekleşirler. Bir işlem gerçekleşeceği zaman, kullanılan uzlaşma algoritmasına da bağlı olacak şekilde, blokzincir sistemine erişimi olan tüm düğümlerce işlem onaylandıktan sonra bloklarda kaydedilir. Gerçekleşen bir işlemin silinmesi yahut değiştirilmesi mümkün değildir [18].

2.1.2. Yaratılış Bloku ve Blok Yapısı

İlk oluşturulan ve zincirin nasıl devam edeceğinin bilgilerinin tutulduğu bloka yaratılış bloku denir [8]. Gerçekleşen işlemler bu blok yapılarında kaydedilir ve belirli bir boyutta işlem kaydı tuttuğu için blok dolduğu zaman yeni blok oluşturulur. Bloklar birbirlerine kriptolojik özütleme fonksiyonlarıyla bağlanır ve aynı bir zincir gibi bu yapılar oluşturulmaya devam eder. Her bir blokta blok başlığı ve kaydedilmiş veriler bulunmaktadır. Blok başlığında özütleme işaretçisi ve Merkle ağacı veri yapısı bulunmaktadır. Sadece yaratılış blokunda özütleme işaretçisi bulunmaz. Ayrıca bloklarda zaman pulu bulunmaktadır [10]. Zaman pulu blok eklenme tarihini tutar ve zincir güvenliği açısından önemlidir. Zaman pulu sayesinde blok oluşturulma zamanları kayıt altında olduğu için yeni oluşturulan

blokların eski oluşturulanlardan önce kaydedilmesinin ve zincirin manipüle edilmesinin önüne geçilir. Blokzincir yapısı Şekil 1'de paylaşılmıştır.



Şekil 1. Blokzincir Yapısı

2.1.3. Özüt Algoritmaları ve Özüt İşaretçisi

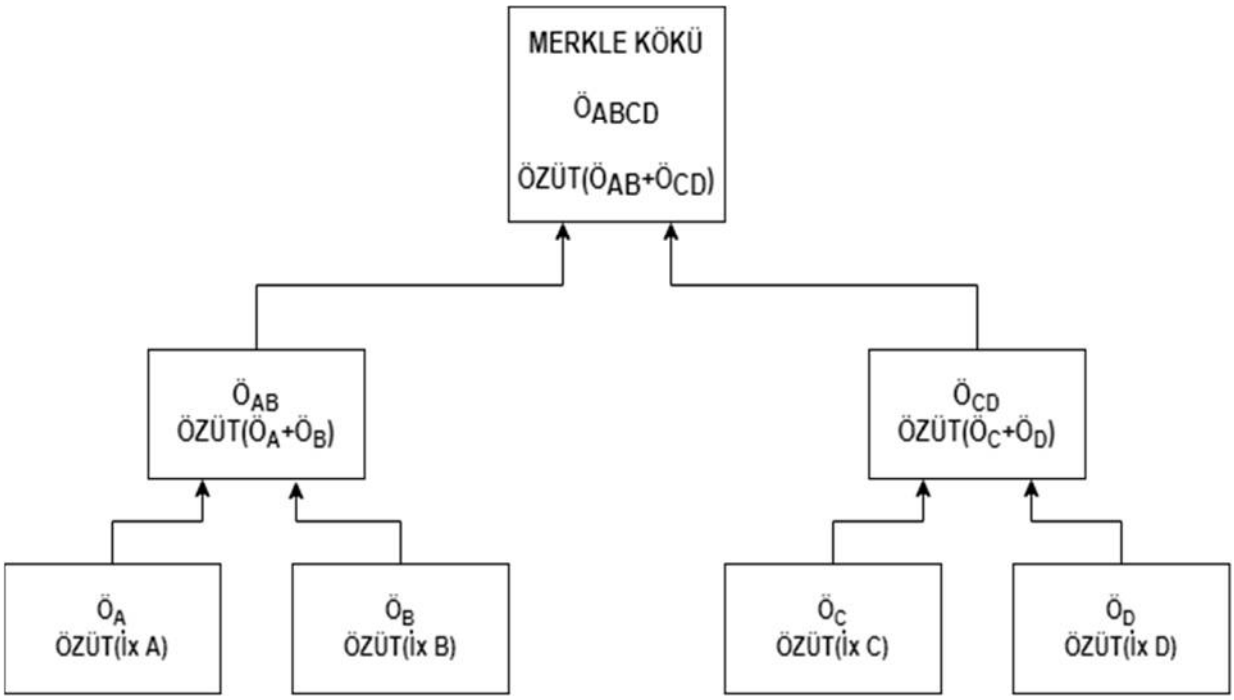
Blokzincir sistemlerinde çokça kullanılan kavramlardır. Özüt (Hash) algoritmaları matematiksel işlemler olup, farklı boyutlardaki girdileri sabit uzunlukta çıktılara çeviren algoritmalardır. Girilen verideki en ufak bir değişimde oluşacak özüt değeri değişecektir. Özüt algoritmaları her veri için farklı bir çıktı üretmektedir. Farklı değerler için aynı çıktıların oluşması durumunda o algoritmanın kullanımı bırakılır ve daha karmaşık yapıdaki bir özütleme algoritmasına geçilir. Birçok özüt algoritması bulunmaktadır. Bunlardan; MD5 128, MD6 256, SHA1 160 ve SHA256 256 bitlik sabit uzunlukta çıkış verir.

Şekil 2. Özüt Algoritması Çalışma Yapısı

Özüt işaretçisi ise bir önceki blokta bulunan özüt değerini işaretleyen yapıdır. İlk oluşturulan yaratılış blokunda üretilen özüt değeri ikinci blokta bulunan özüt işaretçisi tarafından tutulur. İkinci blokta üretilen özüt değeri de üçüncü bloktaki özüt işaretçisi tarafından tutulur ve bu böyle devam eder. Bu sayede blokların özüt kayıtlarını bir birlerine bağlayarak bir zincir oluşturulmuş olur. Herhangi bir blokta kaydedilmiş işlemin değiştirilmeye çalışması durumunda özüt fonksiyonunun değeri değişeceği için bir sonraki blokta bulunan özüt işaretçisindeki değerden farklı bir değer ortaya çıkar. Bu durumda zincir bozulmuş olan bloku sistem dışına atar. Blokta yapılan değişiklik düzeltildiği durumda ise zincire geri alınır.

2.1.4. Merkle Ağacı

İkili bir ağaç yapısıdır. Kök, yaprak ve üst düğümler bulunmaktadır. Blokta kaydedilen veri parçalarının özütlenmesine ve bu özüt değerinin saklandığı yapıya yaprak denir. Yapraklarda bulunan özüt değerlerinin de özütlenerek kaydedilmesine üst düğüm denir. En üstteki üst düğüme kök denir. Blokzincir sistemlerinde Merkle ağaçlarında bu kök değeri tutularak işlem yapılır. Bu sayede çok hızlı ve az bir alan tutularak Merkle ağacı uygulanmış olur. Merkle ağacı sayesinde işlem verileri üzerinde bir değişiklik yapılması durumunda yaprak ve üst düğümlerdeki özüt değerleri değişeceği için sisteme bir müdahale yapıldığının gizlenmesi mümkün olmayacaktır ve fark edilecektir. Bu bağlamda Merkle ağacı verilerin verimli, hızlı ve güvenli doğrulanmasında kullanılır [12]. Şekil 3'de örnek bir Merkle ağacı yapısı paylaşılmıştır.



Şekil 3. Merkle Ağacı Yapısı

2.1.5. Uzlaşma Algoritmaları

Blokzincir sistemi oluşturulurken seçilmiş olan izlenecek kurallar bütünüdür. Her blokzincir sisteminde uygulanan uzlaşma algoritmaları bulunmaktadır. Kurulan sistem ve seçilen yahut sistem için özel olarak geliştirilen uzlaşma algoritmalarının özenle belirlenmesi gerekir. Yanlış kullanılan uzlaşma algoritmaları, fazla enerji tüketiminden uzun süren işlem süreçlerine varıncaya kadar birçok olumsuzluğa sebebiyet verebilir [17]. Bir başka deyişle uzlaşma algoritmaları, blokzincir sisteminde bir işlemin gerçekleşip bloklara kaydedilmesi için geçmesi gereken onay mekanizmalarıdır. Günümüzde birçok uzlaşma algoritması bulunmaktadır. Bunlardan ön plana çıkan İşin İspatı Algoritması (PoW,

Proof of Work) Bitcoin'de kullanılıyor olması sebebiyle çokça bilinen bir algoritmadır [7]. Madencilik işlemleri ve blok oluşturulmasında yüksek işlemci gücü gerektiği için yüksek elektrik tüketimine sebebiyet veren bir algoritmadır.

Blokzincir sisteminde ön plana çıkan bir başka kripto para olan Ethereum, ilk olarak uzlaşma algoritması olarak İşin İspatı algoritmasını kullanmış ancak daha sonra Türkçe karşılığı Hissenin İspatı (PoS, Proof of Stake) demenin daha doğru olacağı uzlaşma algoritmasına geçmiştir [16]. Bu algoritmada ise yeni blok oluşturma görevi düğümlerden rastgele seçilen birine verilerek yapılır. Rastgele seçim işleminde seçilen düğümün tutmuş olduğu kripto para miktarı, blok oluşturma görevini almasında öncelikli etkendir. Yani yüksek miktarlarda kripto para tutan düğümler daha çok ödül alırlar. Ancak burada zincirin belirli düğümlerce yönetilme durumu ortaya çıkabilmektedir. Buna çözüm olarak da yine Hissenin İspatı algoritması içinde kripto para yaşına göre bir seçim yapılmaktadır. Burada kripto paralarının miktarı ve kaç gündür hisse olarak sistemde tuttukları önemlidir. Çünkü bekleme gün sayısı ve tutulan kripto para çarpımı ile elde edilen değeri en yüksek olan düğümler, yeni bloku oluşturacak düğüm olarak seçilir. Bloku oluşturan düğümün bekleme gün sayısı sıfırlanır ve bu sayede sistemde yüksek kripto paralı düğümlerin sürekli işlem yapması ve ödülleri toplamasının önüne geçilmiş olur. Günümüzde Pratik Bizans Hata Toleransı (PBFT, Practical Byzantine Fault Tolerance), Kapasite Kanıtı (Proof of Capacity), Geçen Sürenin Kanıtı (Proof of Elapsed Time) ve belirmediğimiz birçok uzlaşma algoritmaları bulunmaktadır. Tablo 1'de blokzincir platformları ve kullanılan uzlaşma algoritmalarının bilgileri paylaşılmıştır [4].

Tablo 10. Çokça Kullanılan Blokzincir Platformları ve Uzlaşma Algoritmaları

Platform İsmi	**Uzlaşma Algoritması**
Bitcoin	İşin İspatı Algoritması
Ethereum	İşin İspatı Alg. & Hissenin İspatı Alg.
Hyperledger Fabric	Takılabilir Algoritma
EOS	Yetkilendirilmiş Hisse İspatı Algoritması
Stellar	Stellar Uzlaşma Protokolü
Quorum	Çoğunluk Oylaması
Ripple	Olasılıklı Oylama

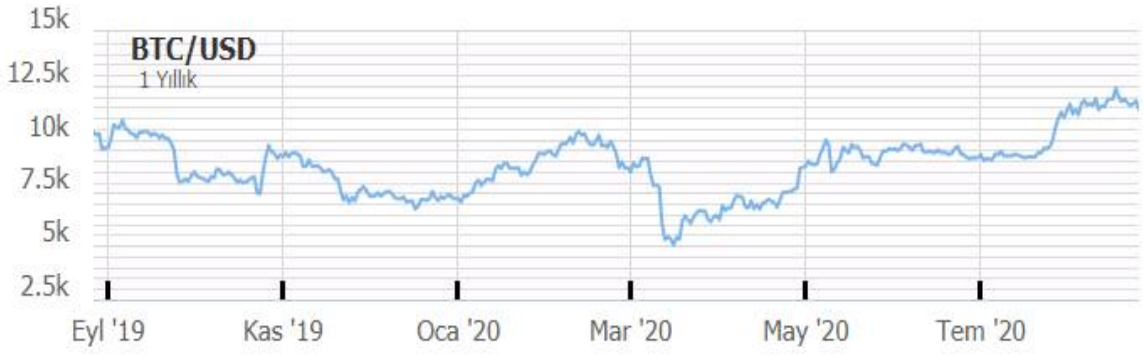
2.1.6. Kripto Paralar

Blokzincir sistemleri üzerinde üretilen Bitcoin ve altcoinlerin tamamına denilmektedir [22]. Bitcoin sonrası üretilen tüm dijital paralara altcoin denilmektedir. Günümüzde birçok blokzincir sistemi açık kaynak kodludur. Bu sayede programlama yeteneği bulunan herkes kendi kripto parasını geliştirip kullanıma sunabilir. Bu sebepten olsa gerek günümüzde 1600 farklı kripto para bulunmaktadır. Üretilen kripto para sayısının bu kadar fazla olması, birçok altcoin için, kaçınılmaz olarak değerlerinin Bitcoin ve Ethereum'da olduğu gibi yüksek meblağlara ulaşmamasıyla sonuçlanmaktadır. Kripto paranın değerinin belirlenmesinde o paranın üretilmesinde görev alan teknik ekibin özgeçmişleri de büyük önem taşımaktadır. Çünkü blokzincir sistemleri oluşturulurken her şeyin düşünülmesi ve sistemin çok iyi optimize edilmesi gerekmektedir. Blokzincir sistemlerinin kaynak kodlarında gözden kaçan çok küçük hataların dahi çok büyük sorunlara sebebiyet vereceği unutulmamalıdır. Bu sebeple çok iyi bir yazılımcı ekibi olan kripto para girişimlerinin geleceği ve değerinin ne olacağı hakkında fikir sahibi olunabilir.

Günümüzde kullanılan banknotlara itibari para denilmektedir. İtibari denilmesinin sebebi, basılan paranın karşılığında altın yahut benzeri değerli bir materyalin merkez bankalarında tutulmuyor olmasıdır. Büyük buhran öncesi merkez bankaları ons altın karşılığı banknot basımı gerçekleştirmiştir. Ancak İkinci Dünya Savaşı zamanında basılan paraların karşılığı olarak merkez bankalarında tutulması gereken ons altın miktarının yeterli seviyenin çok altında olduğu anlaşılmıştır. Bu durum sonrasında savaşın da doğurmuş olduğu olumsuzluklar sebebiyle tüm dünyayı etkileyen ekonomik kriz başlamıştır. Yaşanılan bu süreç sonrasında piyasaya sürülen banknotların karşılığı olarak ons altın tutulması durumu değişmiştir. Günümüzde itibari paraların değerini belirleyen birçok ekonomik ve siyasi etken bulunmaktadır. Banknotun basıldığı ülkenin bulunduğu coğrafi konum, sahip olduğu zenginlikler, üretim gücü, teknolojiyi geliştirme seviyesi, imzalamış olduğu uluslararası anlaşmalar ve üyesi olduğu birlikler gibi birçok değişken, ülke paralarının değerinin belirlenmesinde etkili olmaktadır.

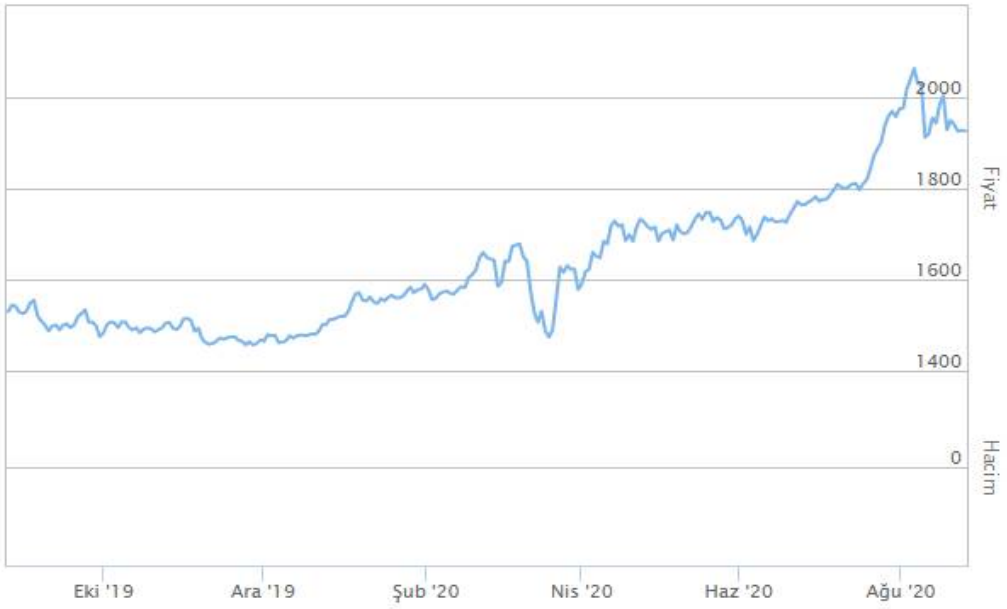
Kripto paraların değerlerinin belirlenmesinde yukarıda bahsedilenlerden farklı bir şekilde ilerlemektedir. Fiyatlarda karşılaşılan yüksek dalgalanmalar, özellikle Bitcoin örneğinde olduğu gibi ulaşılan yüksek değerler ve kripto para borsalarının kurulmuş ve kaldıraç gibi ekonomik araçlarla işlem yapılma imkanı olması sebebiyle yatırımcılar açısından ilgi çekici bir değer halini almıştır. Sabit değerli kripto paralar dışında piyasada kullanılmakta olan tüm dijital paralarda tahmin edilemez fiyat değişimleri ile karşılaşılabilir. Covid19 pandemisi sürecinde güvenli yatırım aracı olarak görülen ons altın fiyatlarında görülen yükseliş ile Bitcoin'in son bir yılı incelendiğinde önemli bir tablo ile karşılaşılmaktadır. Şekil 4'de Bitcoin Dolar karşısındaki değer değişim grafiği gözükmektedir. Son bir sene incelendiğinde günümüzde Bitcoin Eylül 2019 tarihindeki değeri üzerinde bir bedele ulaşmış gözükmektedir. Ancak grafik dikkatle incelendiğinde pandemi sürecinde Mart 2020 tarihinde 5000 dolarlık bir bedele gerileme olduğu görülmektedir. Ardından gerçekleşen değer artışı ile günümüzde

11000 dolar civarında bir değere sahiptir. Ortalama fiyat dalgalanması bu süreçte 5000 dolar gibi çok yüksek bir rakam olarak kayıtlara geçmiştir.



Şekil 4. Bitcoin Bir Yıllık Değer Değişim Grafiği

Şekil 5'de paylaşılan ons altının bir yıllık değer değişim grafiği incelendiğinde, grafiksel olarak Bitcoin grafiğinden çok daha agresif ve sürekli bir yükseliş varmış gibi gözükse de ortalama 600 dolarlık bir değer yükselişi gerçekleşmiştir. Mart 2020 tarihinde Bitcoin'de olduğu gibi bir değer kaybı görülmüş ancak bu fiyat değişimi 200 dolarlık bir aralıkta kalmıştır. Karşılaşılan pandemi süreci, devam eden ticaret savaşları ve bozulan dünya ekonomisi düşünüldüğünde, tüm bu olumsuzluklara rağmen, ons altında karşılaşılan bu yükseliş Bitcoin'le kıyaslandığında önemsiz bir rakammış gibi görünmektedir.



Şekil 5. Ons Altın Bir Yıllık Değer Değişim Grafiği

Kripto para fiyatlarında karşılaşılan bu yüksek değer değişimleri çok ciddi bir sorundur. Ancak bu denli yüksek değerlere ulaşmasının sebebinin Bitcoin yahut diğer tüm altcoinlere duyulan güven olduğu unutulmamalıdır. Burada güven, kripto paranın yaratılış blokunda belirlenmiş ve değiştirilemez olan kurallarına, değiştirilemez olan işlem kayıtlarına, ademi merkeziyetçi yapısına ve düşük işlem

maliyetlerine duyulmaktadır. Blokzincir teknolojisinin finans alanında kat ettiği gelişim düşünüldüğünde, kripto paraların ilerleyen süreçte çok daha yaygınlaşacağı ve kullanımının kolaylaşacağı söylenebilir. Ancak sabit değerli olmayan tüm kripto paraların değerlerinin yukarıda bahsedilen güven kaynaklarında bir şaibe meydana gelmesi durumunda sıfırlanacağı unutulmamalıdır.

Kuantum hesaplama gücü güvenlik noktasında önemli bir etken olarak dikkate alınmalıdır. Kripto para ve blokzincir sistemleri bilgisayar bilimleri ve kriptoloji bilimi çalışma konusudur. Kullanılan algoritmaların kırılması veya yeni algoritmaların kuantum bilgisayarlarıyla geliştirilmemesi durumunda ciddi sistemsel güvenlik sorunlarının karşılaşılacağı unutulmamalıdır. Bu sebeple kripto paraların geleceği ile ilgili olumlu beklenti devam ederken akademinin de blokzincir teknolojisini yeni gelişmelerle destekleyici çalışmaları sürdürmesi büyük önem taşımaktadır. Projemizde Türkiye Cumhuriyet Merkez Bankası'nın geliştireceğini duyurduğu kripto para yahut biLira gibi sabit değerli kripto paraların kullanılmasına önem verilmesinin sebebi yukarıda belirtilen olumsuzluklardan yardımlaşma sürecine dahil olan tüm paydaşları koruma altına almaktır.

2.1.7. Kripto Cüzdanlar

Günümüzde tedavülde bulunan Bitcoin ve Ethereum baştan olmak üzere tüm kripto paraları, altcoinleri, kullanabilmek için kripto cüzdana ihtiyaç duyulmaktadır. Kripto cüzdanlarda özel ve genel anahtarlar ve kripto para adresi tutulmaktadır [20]. Bu bilgiler sayesinde kripto cüzdanlar arasında transfer işlemi gerçekleştirilebilir. Sanal cüzdan olarak da adlandırılan kripto cüzdanlar internet erişimi durumuna göre sıcak ve soğuk olarak ikiye ayrılırlar. Soğuk cüzdanlar internet erişiminin olabildiğince çevrimdışı tutulduğu cüzdanlardır. Sıcak cüzdanlarda ise çevrimiçi internet erişimi bulunup, işlemler süratle gerçekleşmektedir. İntemet erişiminin bulunduğu durumlarda siber saldırılara maruz kalma durumu söz konusu olabileceği için sıcak ve soğuk cüzdan çözümleri ortaya atılmıştır. Günümüzde her iki cüzdan türünde de güvenlik seviyesi yüksek olup her geçen gün yeni çözüm önerileri geliştirilmekte ve güvenlik arttırılmaktadır. Kripto cüzdanlar beş farklı sınıfta incelenebilir. Bunlar: Mobil Cüzdanlar, Masaüstü Cüzdanlar, Çevrimiçi (Web) Cüzdanlar, Kâğıt Cüzdanlar, Donanım Cüzdanlardır. Tüm cüzdan çeşitlerinde kripto paranın kendisi tutulmamaktadır. Kripto cüzdanlarda tutulan kripto paranın varlığını ispatlayan verileri depolanmaktadır. Aynı zamanda tüm kripto cüzdanların aynı IBAN numarası gibi bir cüzdan adresi bulunmaktadır. Bu adrese genel anahtar denilmektedir. Cüzdan adresinin bilinmesi durumunda başka bir bilgiye gerek duyulmadan ve geri dönüşümü yapılmaksızın para transferi gerçekleştirilebilir. Kripto cüzdanlara erişim özel anahtar ile mümkündür. Özel anahtarın unutulması yahut başka birinin eline geçmesi durumunda geri dönüşümü olmayan para transferlerine yahut cüzdana erişimin şifre hatırlanıncaya kadar durmasına sebebiyet verilebilir. Bu sebeple cüzdanınızı oluşturduktan sonra sahip olacağınız anahtar ve şifrenizi kaybetmeyeceğiniz ve güvenli bir yerde yazarak saklayınız [25].

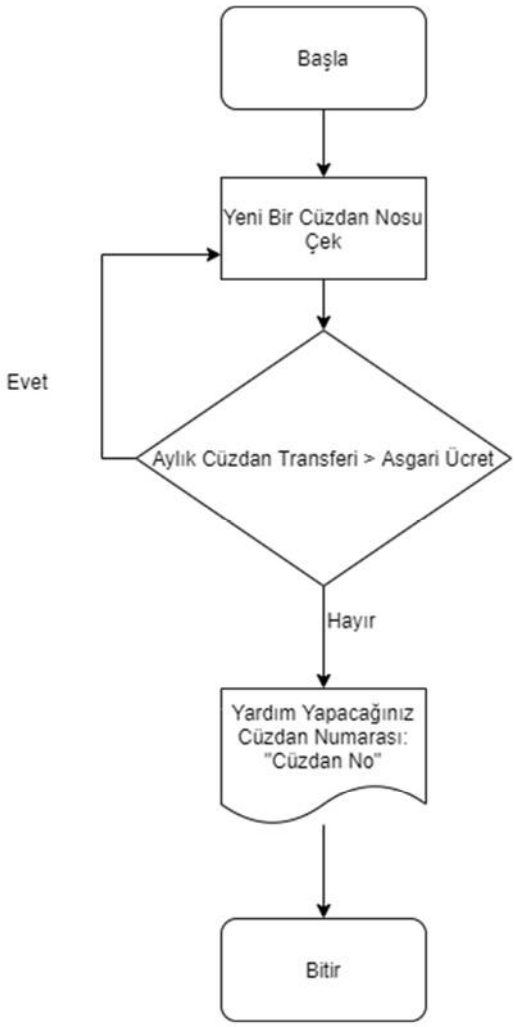
3. MİLLİ BAĞIŞ ZİNCİRİ PLATFORMU

Milli Bağış Zinciri Projesi, yardımlaşma sürecine katılan tüm paydaşların birer kripto cüzdan sahibi olduğu, gerek kurumsal hesapların gerekse de gerçek kişilerin gerçekleştirmiş oldukları tüm ödemeleri kayıt altında tutulduğu, ihtiyaç sahiplerinin şeffaf ve adil bir şekilde yardıma eriştiği bir sosyal sorumluluk projesidir. İlgili kurum dışında yardım yapılacak kişilerin bilgisi kimsede bulunmamaktadır. Bu sebeple yardımlaşma sürecinde kör eşleşme sistemi bulunmaktadır. Yardım yapan ve alan taraflar birbirlerinden habersizdir.

MBZ projesinin ilk aşaması kullanılacak Türk parasına sabitlenmiş kripto paranın belirlenmesi ve kullanılacak kripto cüzdanların paydaşlarca edinilmesinin sağlanmasıdır. MBZ projesi için özel olarak üretilmiş Türk parasına sabitlenmiş stabil bir kripto para üretmek aslen çok zor bir süreç olmamakla birlikte gereksiz bir enerji kaybına sebebiyet vermemek için hali hazırda geliştirilen ve MBZ projesinin amacına uygun kripto paraların kullanılmasına karar verilmiştir. MBZ projesinin bulunduğu aşama itibariyle yapısal değişimlere müsait olması ve ilerde yapılacak olası bir kripto para değişikliğinin de sisteme kolayca uyarlanabileceği için resmi bir kurumla anlaşılma sürecinde alınacak kararlar doğrultusunda kullanılacak kripto paranın nihai halini almasına karar verilmiştir. Çalışmamızın tanıtılması aşamasında biLira stabil kripto parası ile devam edilecekmiş gibi düşünülerek hareket edilmiştir. Bu doğrultuda biLira kripto parasının ERC-20 standardına uygun tüm cüzdanlarla uyumlu olması ve sebebiyle uygulama ara yüzü kolay olan MyEtherWallet (MEW) uygulamasının kullanılmasına karar verilmiştir. MEW uygulaması App Store ve Google Play'dan kolaylıkla indirilebilecek ve ücretsiz bir uygulamadır. MBZ platformunda yeni üyeler ve daha önce kripto para transferi yapmamış kişiler için kripto cüzdan oluşturulmasının ve kripto cüzdanlarına para yüklenmesinin nasıl yapılacağını açıklayan tanıtım görselleri ve videoları hazırlanmakta olup sistem kullanıma açıldığında kullanıma hazır bulunacaktır.

Milli Bağış Zinciri projesinin ikinci aşaması olan MBZ platformu ise en basit tabirle kripto cüzdan bilgisi paylaşan web tabanlı bir hizmettir. MBZ için geliştirilecek olan web sitesinin kullanımın çok basit ve açıklayıcı bilgilerinin çokça bulunduğu bir platform olmasına karar verilmiştir. Temel bilgisayar kullanımı yetisine sahip herkes için kolayca kullanılabilecek bir yapıda olup kullanıcılara adım adım gerekli tüm süreçlerde nasıl bir yol izleneceğinin bilgisi verilecektir.

Şekil 6'da MBZ platformu için geliştirdiğimiz algoritmanın akış şeması özet bir şekilde paylaşılmıştır.



Şekil 6. Milli Bağış Zinciri Cüzdan Belirleme Algoritması Akış Şeması

MBZ platformunda paylaşılacak olan kripto cüzdan adreslerinin belirlenmesi konusunda şu adımlar takip edilecektir:

1- Yardım yapılacak kişilerin ilgili kurumca belirlenmesi

2- ERC-20 standardında kripto cüzdanı olmayanlar için yeni kripto cüzdanların oluşturulması

3- Yeni oluşturulan cüzdan bilgilerinin sahiplerine iletilmesi

4- Tüm cüzdan bilgilerinin bir veri tabanında toplanması

5- Belirli aralıklarla ilgili kurumun belirleyeceği şekilde yardım listesindeki kişilerin eklenip çıkartılması

MBZ platformunda cüzdan bilgileri paylaşılacak kişilerin belirlenmesinde resmi kurumlarla birlikte çalışılması zorunludur. Sisteme eklenen kişilerin muhtaçlık durumu şüphe götürmemeli, ihtiyacı olmayan kişiler kesinlikle sisteme dâhil edilmemelidir. MBZ platformu ve veri tabanının tasarımı, güvenliği maksimum seviyede tutacak şekilde tasarlanmış olup her türlü siber saldırılara karşı dayanıklı