Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi

Afyon Kocatepe University International Journal of Engineering Technology and Applied Sciences

AKÜ IJETAS Cilt **4(1)** (2021) Haziran(37-48 s) AKU J.Eng.App.Sci. **Vol 4(1)** (2021) June(37-48 pp)

Araştırma Makalesi / Research Article

e-ISSN 2667-4165 (https://dergipark.org.tr/akuumubd)

Blokzincir Tabanlı Donanımsal Cüzdan ve Akıllı Kartlar

Adil TANRIKULU[1], Hüseyin YÜCE[2], Ercan ÖLÇER[3]

[1] *Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Bölümü, İstanbul.*

[2] *Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Siber Güvenlik Anabilim Dalı, İstanbul.*

[3] *TÜBİTAK BİLGEM, UEKAE, E-Kimlik Uygulamaları Birimi, Kocaeli.*

e-posta: atk.ank.http@gmail.com, ORCID ID: https://orcid.org/0000-0003-1586-0321

e-posta: huseyin@marmara.edu.tr, ORCID ID: https://orcid.org/0000-0001-5525-7733

e-posta: olcerercan@gmail.com, ORCID ID: https://orcid.org/0000-0003-3786-6230

Geliş Tarihi:23.01.2021 ; Kabul Tarihi: 30.05.2021

Öz

Kripto para transferi için gönderen ve alıcıya ait ortak anahtar denilen adreslerin olması gereklidir. Göndericinin adresi, alıcının adresi ve gönderim miktarı gibi bilgilerin olduğu işlemler, birbiri ardına bağlı blokların içerisinde belli bir sisteme göre tutulur. Her adresin yani ortak anahtarın benzersiz gizli bir anahtar karşılığı bulunmaktadır. Kripto para işlemleri için bu özel anahtarlar ile atılmış imzalar kullanılır. Mahremiyet söz konusu olduğu için kripto para transferinde birden fazla adres yani anahtar çifti kullanmak önemlidir ve önerilmektedir. Bu anahtarların yönetimi ve depolanması cüzdanlar sayesinde sağlanır. Çevrimdışı cüzdanların direkt olarak internet erişimi yoktur ve daha güvenlidir. Bu makalede çevrimdışı cüzdan çeşidi olan blok zincir tabanlı kripto paraların erişimine ve harcanabilmesine olanak sağlayan anahtarların tutulduğu donanımsal akıllı kart cüzdan konusu işlenmiştir. Anahtarın üretimi ve depolanması için hiyerarşik ve deterministtik bir yöntem sunan BIP-32, BIP-39 ve BIP-44'e bu çalışmada detaylı olarak yer verilmiştir. Yerli ve milli akıllı kart işletim sistemi olan AKiS'in yeni sürümünde kimlik, pasaport, ehliyet, e-imza, bilet gibi uygulamalar tek bir kart içinde toplanabilmektedir. Bu sürümle birlikte kartın içinde olan uygulamalardan biri de cüzdan uygulamasıdır. Kripto para çeşidi olarak Bitcoin transferini yapabilecek özellikte tasarlanmıştır. AKiS cüzdan BIP-32, BIP-39 ve BIP-44 ve eliptik eğri kripto grafik işlemlerini yapabilecek şekilde geliştirilmektedir.

Anahtar kelimeler
Blokzincir; Hiyerarşik Deterministik Donanımsal Cüzdan; Akıllı Kart; AKiS

Hardware Wallets and Smart Cards for Blockchain Platforms

Abstract

The addresses which are called as public keys that belong to the sender and receiver are required for crypto currency transfer. The transactions with information such as transfer amount, recipient's and sender's addresses are kept in a particular system in which successive connected blocks. Each address, the public key, has a unique secret key equivalent. Signatures signed with these private keys are used for crypto currency transactions. Since privacy is at stake, it is important and recommended to use more than one address that is to say key pair in crypto currency transfer. The management and storage of these keys is provided by wallets. Offline wallets do not have direct internet access and are more secure. In this article, the topic of a hardware smart card wallet that holds keys that allow access and spending of block chain-based crypto currencies, which is an offline wallet type, is discussed. BIP-32, BIP-39 and BIP-44, which offer a hierarchical and deterministic method for key generation and storage, are given in a detailed way. In the new version of AKiS, the domestic and national smart card operating system, applications such as identity, passport, driver's license, e-signature and ticket can be collected in a single card. With this version, one of the applications included in the card is the wallet application. It is designed to handle Bitcoin transfer. AKiS wallet is developed to be able to perform BIP-32, BIP-39 and BIP-44 and elliptic curve cryptographic transactions.

Keywords
Blockchain; Hierarchical Deterministic Hardware Wallet; Smart Card; AKiS

1. Giriş

İnsanoğlunun toplum düzenine geçmesiyle mal ve mülk edinme ihtiyacı doğmuştur. Bu da mal veya hizmet satın almak için belli bir değeri olan nesnelerin yani paranın icadını sağlamıştır. Akıllı kartlar ve blokzincir tabanlı cüzdana giriş yapmadan önce paranın tanımını ve tarihsel gelişimini bilmek gerekir. Para, genellikle mal ve hizmetlerin ödenmesi ve vergiler gibi borçların belirli bir ülkede veya sosyoekonomik bağlamda geri ödenmesi olarak kabul edilen herhangi bir kalem veya doğrulanabilir kayıttır (Mishkin 2007, Smithin 2000).

Aslında paranın birçok tanımı yapılabilir. Fakat bir şeye para denmesi onun fonksiyonuna bağlıdır. Değiştirilebilir olması, belli bir birime sahip olması, kendi değerini koruması vb. özellikler parayı niteler. Bu işlevleri yerine getiren herhangi bir madde veya doğrulanabilir kayıt para olarak kabul edilebilir. Eskiden taşınılabilir olması, sert ve dayanıklı olması birimler halinde bölünebilmesi, değerinin her yerde aynı olması, güvenilir olup taklit edilemeyecek olması gibi özellikleri aranan paranın teknoloji ile birlikte belirgin özellikleri de biçimsel olarak evirilmiştir. Para yıllar içinde biçim değiştirse de insanlık tarihi boyunca değerli varlık olarak yerini korumaktadır. Lidyalılardan günümüze kadar uzanan taş paraların, gümüş ve altınların, kâğıt banknotların ve kripto paraların tümünün amacı değeri niteliğinde mal ve hizmetlerin değiş tokuşu için ödeme aracı olarak kullanılmasıdır (Usta 2018). Son yüzyılda da hızla değişen teknoloji değerli varlık olan paranın biçimini de radikal olarak dijitalleşmeye doğru itmiştir. Akçe, kâğıt gibi fiziksel özelliklerin yerini dijital para sistemleri almıştır. 1946'da John Biggins tarafından kredi kartının icat edilmesiyle paranın serüvenine yeni bir dönem eklenmiştir. 1950'lerden sonra teknolojideki büyük gelişmeler para sistemini de etkilemiştir. Dünyada ilk defa bankalarda paranın elektronik olarak transferi yani EFT kullanımı yapılmıştır (Karayew 2012). Son 30 yıldır tarih sahnesine çıkan dijital paranın önemi akıllı kartlar yoluyla benzin alınması, esnafların pos cihazlarıyla kullanılmaya başlanması, otomatik para çekme makineleri olan ATM'lerin üretilmesiyle daha da artırmıştır. Alışveriş ve ticaret başta olmak üzere çoğu alanda kredi kartlarının kullanımı fiziksel ortamın sınırlılığını ortadan kaldırarak istenilen saatte daha çok mal ve hizmete ulaşma imkânı sağlamıştır. Bunun en büyük getirileri arasında zamandan tasarruf sağlaması ve mekâna olan bağımlılığın azalması sayılabilir.

Nakamoto (2008)'nun ara katmanlara ihtiyaç duymayan uçtan uca elektronik ödeme sistemi hakkında yayınladığı makale ve 2009 yılında ilk Bitcoin yazılımıyla her geçen gün popülerliği daha da artan blokzincir tabanlı kripto paralar, birçok platformda ödeme aracı olarak kullanılmaya başlamıştır. Kripto paralara örnek olarak Bitcoin ve Etherium verilebilir. Kripto kelimesi gizli ve şifreli olduğu anlamına gelir. Kripto para ise finansal işlemlerin kriptolojik algoritmalarla desteklendiği alternatif değiş tokuş aracı olan dijital bir değerdir. Kripto paralar merkezi banka sistemlerinin tersine blokzincir denilen merkezi olmayan bir sistem üzerinde çalışır. Sanal olması ve belli bir merkezi yapısının olmaması sebebiyle kripto paraların kontrolü herkesin erişimine açık kayıt defteriyle sağlanır. Tüm işlemler bu dağıtık kayıt defterinde birbiri ardına bağlanmış bloklar şeklinde tutulur ve isteyen herkesin erişimine açıktır. Bitcoin için sağlanan Açık Blokzincir platformundan sonra Hyperledger ve akıllı kontratlar gibi çeşitli uygulamalar için Açık ve İzinli Blokzincir, Gizli ve İzinli Blokzincir platform türleri de türetilmiştir (Dursun 2020).

Kripto para transferi için gönderen ve gönderilene ait açık anahtar denilen adreslerin olması gereklidir. Temelinde bütün blokzincir yapısı açık anahtar kriptografisine dayanır. Bu adreslerin birbirine transfer ettiği kripto para miktar bilgilerinin olduğu işlemler, birbiri ardına belli bir sisteme göre kayıt defterinde tutulur. Her adresin yani açık anahtarın benzersiz gizli bir anahtar karşılığı bulunmaktadır. Kripto para işlemleri için bu özel anahtarlar ile atılmış imzalar kullanılır. Mahremiyet söz konusu olduğu için kripto para transferinde birden fazla adres yani anahtar çifti kullanmak önemlidir ve önerilmektedir. Bu anahtarların yönetimi ve depolanması cüzdanlar sayesinde sağlanır. Temelde

cüzdanlar çevrimiçi ve çevrimdışı olmak üzere ikiye ayrılmaktadır. Çevrimiçi cüzdanların internet erişimi bulunur. Çevrimdışı cüzdanların ise direkt olarak internet erişimi yoktur ve daha güvenlidir. Bu çalışmada çevrimdışı cüzdan çeşidi olan blokzincir tabanlı kripto paraların erişimine ve harcanabilmesine olanak sağlayan anahtarların tutulduğu donanımsal akıllı kart cüzdan konusu işlenecektir.

1.1 İlgili Çalışmalar

Dünya genelinde GoldmanSachs, Morgan Stanley, Citibank, HSBC, Accenture, Microsoft, IBM, Cisco, Tencent, Alibaba, Samsung, LG ve diğer küresel ünlü finansal kurumlar, danışmanlık firmaları, BT satıcıları ve internet devleri blokzincir teknolojisinde laboratuvar araştırmalarını ve sermaye düzenini hızlandırmaktadır. Ayrıca IBM ve Apache vakfı tarafından desteklenen Hyperledger projesi, Ethereum, FileCoin gibi çeşitli girişimler, blokzincir araştırma ve geliştirme için açık kaynak havuzları ve platformları sağlamaktadır (Buterin 2013, IntKyn. 1).

Literatürde son beş yıl içinde blokzincirle alakalı çalışma raporları da dâhil binlerce makale yayınlanmıştır.

Bamert vd. (2014) BlueWallet ismindeki donanımsal cüzdanın temelini atmış ve tanıtmışlardır.

2014'ün Ocak ayında Trezor adlı donanımsal cüzdan açık kaynak olarak ilk kez piyasaya sürülmüştür (IntKyn. 2).

2015'in Eylül ayında Ledger adlı donanımsal cüzdanın java kart versiyonu açık kaynak olarak sürülmüştür. Şu an LedgerNanoS, LedgerNanoX isimlerinde ürünleri mevcuttur. Ürünün Github sayfasında farklı dilde yazılmış versiyonları ve mobil ile bilgisayar bağlantısı için de farklı sürücüleri ve servisleri mevcuttur (IntKyn. 3). Bu cüzdan akıllı karta yüklenen 25 farklı özel anahtarı saklayabilme kapasitesine sahiptir. Kartın ilklendirilmesi sırasında kurtarma ya da onarma durumları için bir kısım kelimelerin saklanması gerekmektedir. İşlemlerin imzalanması sırasında mobil ve bilgisayar ara bağlantısına ihtiyaç duymaktadır. Donanımsal cüzdanlar arasında en bilinenler arasındadır.

2016'nın Şubat ayında KeepKey adlı donanımsal cüzdan Trezor cüzdanın çatalı şeklinde ilk versiyonunu duyurmuştur. Güvenlik açısından Trezor cüzdan ile özellikleri aynıdır denilebilir. Aralarındaki göze çarpan ilk fark dış tasarımıdır. Bundan farklı olarak KeepKey daha stabil çalışmaktadır ve kullanıcı dostu ara yüze sahiptir (Skála 2018).

Bulut (2019) kripto para cüzdanların güvenlik açıkları ve riskleri gibi güvenlik durumunu Ortak Kriterler çerçevesinden incelemiş ve gereksinimlere göre cüzdan tasarımı önerisinde bulunmuştur. Ayrıca çalışmasında hâlihazırda kullanılan cüzdanların karşılaştırması yapılmıştır.

2. Materyal ve Metot

Bu çalışmanın hazırlanması genelden özele doğru ilerlemiştir ve yöntemi ise kavram ispatı şeklinde yapılmıştır. Blokzincir tabanlı kripto para birimlerine erişimi sağlayacak, işlemler için imza atacak ve blokzincir ağına bağlanmayı sağlayacak örnek uygulama için akıllı kart çeşidi olarak java kart seçilmiştir.

2.1 Blokzincir

Bir blokzincir, işlevsel olarak işlem kayıtlarının tutulduğu dağıtık ve güvenli bir veri tabanıdır. Bir Bitcoin ağında, A istemcisi başka bir B istemcisine bitcoin göndermek istiyorsa, A istemcisi tarafından bir bitcoin işlemi oluşturulur. İşlem, Bitcoin ağı tarafından işlenmeden önce madenciler tarafından onaylanmalıdır. Madencilik sürecini başlatmak için işlem, ağdaki diğer tüm düğümlere dağıtılır.
İşlemleri bir blok halinde toplayacak olan madencilerin kastedildiği bu düğümler, bloktaki işlemleri doğrular ve ağdan onay almak için bir uzlaşma protokolü kullanarak bloğu ve doğrulamasını yayınlar (İş İspatı). Diğer düğümler blokta bulunan tüm işlemlerin geçerli olduğunu doğruladığında, blok artık blokzincire eklenebilir. İşlemi içeren "blok" diğer düğümler tarafından onaylandığında ve blokzincire eklendiğinde, artık A'dan B'ye bu bitcoin transferi sağlanmış ve meşru hale gelmiş olur.

2.2 Eliptik Eğri Dijital İmza Algoritması (ECDSA)

Blokzincir teknolojisinde dijital imzanın kullanım amaçlarından biri ortak anahtar ve buna karşılık gelen özel anahtarın sahibinin kanıtlanması ve bunun özel anahtarı açığa çıkarmadan yapılmasıdır (Donanımsal cüzdanda özel anahtar çevrimdışı alanda kullanılır). Başka bir deyişle dijital imza imzanın ve ortak anahtarın aynı özel anahtarla üretildiğini kanıtlamaya yaramaktadır. Böylece blokta yer alan sahibi olunan cüzdanın ortak anahtarına tanımlı harcanmamış işlemdeki kripto paraya ulaşabilir ve harcama veya gönderim gibi yeni bir işlem yapılabilir.

Aynı dijital imza ile aynı adresteki farklı harcanmamış işlemlere erişilemez çünkü her işleme özel benzersiz bir imza üretilmektedir. Dijital imza, hangi işleme erişim gerekiyorsa o işlemin kendisi de imzaya dâhil edilerek oluşturulur.

Dijital imza, imza oluşturma ve imzayı doğrulama olmak üzere iki bölümden oluşmaktadır.

2.3 Fikir Birliği ve Madencilik

Merkezi olmayan blokzincir bağlamında, yeni bir blok üretilip ağa yayınlandığında, her düğümün bu bloğu kendi blokzincir kopyalarına ekleme veya yok sayma seçeneği vardır. Fikir birliği, ağın büyük bir kısmının blokzincirin genişlemesini sağlamak ve hileli girişimleri veya kötü niyetli saldırıları önlemek için tek bir durum güncellemesi üzerinde anlaşmaya varmak için kullanılır.

2.4 İşlemler

Bitcoin'de işlem göndericinin adresi, gönderilen adres ve gönderim miktarı gibi bilgilerin olduğu bir bilgi grubudur. Cüzdanla bir işlem yapıldığında bu işlem blokzincir ağına gönderilir ve bloğa eklenip onaylanması beklenir.

Mevcut banka sisteminde istenilen tutar hesabınızdan alınıp gönderilir. Fakat Bitcoin sisteminde bir gönderim yapıldığında aslında gönderim miktarı hesabınızdan istenilen tutar kadar alınıp gönderme yapılmaz, bunun yerine işlemlerde girdiler ve çıktılar kullanılır. Örneğin bir gönderim işlemi için adresteki (hesaptaki) harcanmamış para girdi olarak seçilip iki çıktı oluşturulur, çıktıların biri gönderilecek miktar kadarı gönderilmek istenilen adrese, diğer çıktıda ise paranın geri kalanını para üstü olarak kendi adresinize gönderilerek oluşturulur. Bunun yanında çıktıların miktarı girdilerin miktarını aşmayacak şekilde birden fazla girdi ile tek çıktı, bir girdi ile birden fazla çıktı ve birden fazla girdi ve birden fazla çıktı halinde oluşan işlemler de geçerlidir ve yaygın olarak kullanılmaktadır. Sonuç olarak işlemler para transferine ait girdiler ve çıktılardan oluşan bilgi yığınlarıdır.

3. Blokzincir Tabanlı Cüzdanlar

2020 yılı Mart ayındaki verilere göre Etherium, Bitcoin, Litecoin, Altcoin gibi 5255 adet kripto para çeşidi bulunmaktadır (IntKyn. 4). Bu gibi kripto para hesaplarının anahtarları cüzdanlarda tutulur. Temelde internet erişimleri bakımından 2 farklı cüzdandan bahsedilebilir; çevrimiçi cüzdanlar ve çevrimdışı cüzdanlar. Çevrimiçi cüzdanların internete erişimi bulunmaktadır ve bu cüzdanlara yazılımsal cüzdanlar da denilmektedir. Çevrimiçi cüzdanlar masaüstü, mobil, web cüzdanlar olarak üçe ayrılırlar. Çevrimdışı cüzdanlar donanımsal ve kâğıt cüzdan olmak üzere ikiye ayrılmaktadır. Bu cüzdanlar da kendi içlerinde anahtarların üretilme şekline göre deterministik ve deterministik olmayan olmak üzere ikiye ayrılmaktadır.

3.1 Deterministik Cüzdan

Deterministik cüzdan Sıralı Deterministik (Sequential Deterministic: SD) ve Hiyerarşik Deterministik (Hierarchical Deterministic: HD) cüzdan olmak üzere ikiye ayrılır. SD cüzdanda özel anahtarlar SHA256 (tohum +n) fonksiyonuyla özet alınarak üretilir. Buradaki n indeks numarasıdır. 0'dan başlar ve ihtiyaç duyulan adres sayısına göre artırılır.

Şekil 1: Deterministik Cüzdanda Anahtarların Üretim Aşamaları

Hiyerarşik deterministik cüzdanın amaçları arasında şunlar sayılabilir;

- Sadece bir tane temel anahtar olacak ve bu anahtar ile cüzdana tekrar ulaşılabilecek.
- Yapılacak her ödeme için ayrı adresler kullanılacak ve bu sayede gizlilik sağlanacak.
- Size gelecek ödemeler için ödeme adresleri otomatik olarak üretilip değiştirilecek. (Seçimli)

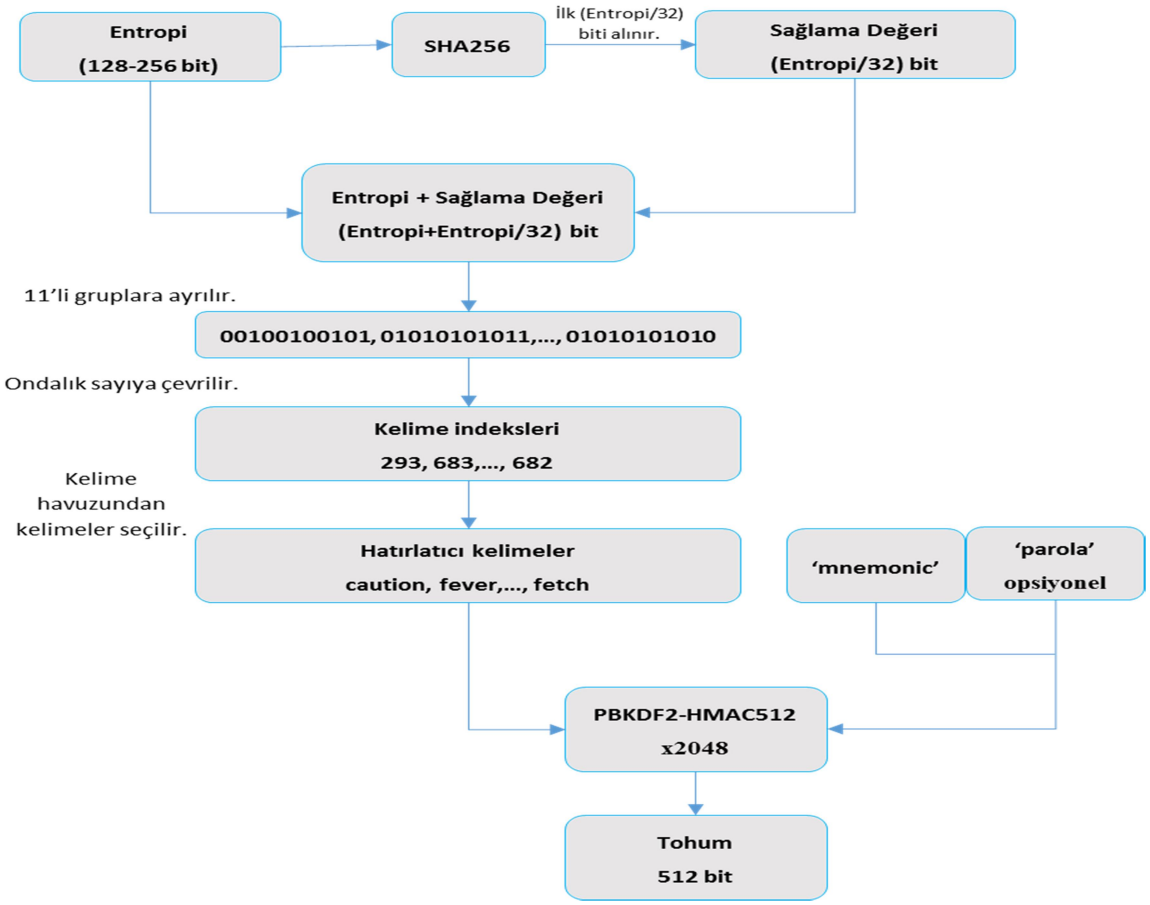
Bu amaçları sağladığı için en çok kullanılan ve tavsiye edilen cüzdan çeşididir.

3.2 *Blokzincir Tabanlı Donanımsal HD Cüzdanın Çalışma Mekanizması*

Hiyerarşik cüzdan için ilk olarak 512 bitlik bir tohum gereklidir. Bu 512 bitin nasıl olması gerektiğini BIP-39 belirler. 512 bit tohum seçildikten sonra temel anahtar ve alt anahtarların üretilmesi aşamasına geçilir. Bu anahtarların nasıl üretilmesi gerektiği ise BIP-32 önerisinde sunulmuştur. BIP-32 anahtarlarının hangi amaçla kullanılacağını tarif eden BIP-44 önerisiyle belirlenir.

BIP-39

BIP-39, BIP-32'de kullanılacak 512 bitlik tohumun oluşturulması için bir takım aşamalar önermektedir. Bu önermenin amacı kullanıcının hatırlamakta fayda sağlayacağı kelime grupları oluşturarak cüzdanına ait tüm anahtarları geri getirebilmesini sağlamaktır. Uzun anahtarlar saklamak yerine kullanıcı dostu bu kelimeler tercih edilebilir. Sonrasında bu kelimelerden BIP-32'de veya benzeri sistemlerde kullanılacak tohum ve anahtarlar oluşturulabilir.



Şekil 2: BIP39'a göre tohum oluşturma adımları (IntKyn. 5)

Aslında BIP-39, entropi değerini verilen kelime havuzuna göre haritalandırmaktadır. Güvenlik için 24 kelimeden oluşan entropi seçilmesi tavsiye edilir. 128 bit entropi için 12 kelime, 256 bit entropi için 24 kelimedir seçilir.

Entropi	Kelime sayısı	Varyasyon	Varyasyon
128	12	2^{12}	~$3{,}4x10^{38}$
160	15	2^{15}	~$1{,}46x10^{48}$

192	18	2^{18}	~6,28x10^{57}
224	21	2^{21}	~2,70x10^{67}
256	24	2^{24}	~1,16x10^{77}

Şekil 3: Entropi-Kombinasyon Tablosu

BIP-32

BIP-32 genel bir hiyerarşik cüzdanın nasıl olması gerektiğini tarif etmektedir. BIP-39 tohumundan Temel Özel Anahtar (Master Private Key) ve Zincir Kodu (Master Chain Code) üretilir (IntKyn. 6).

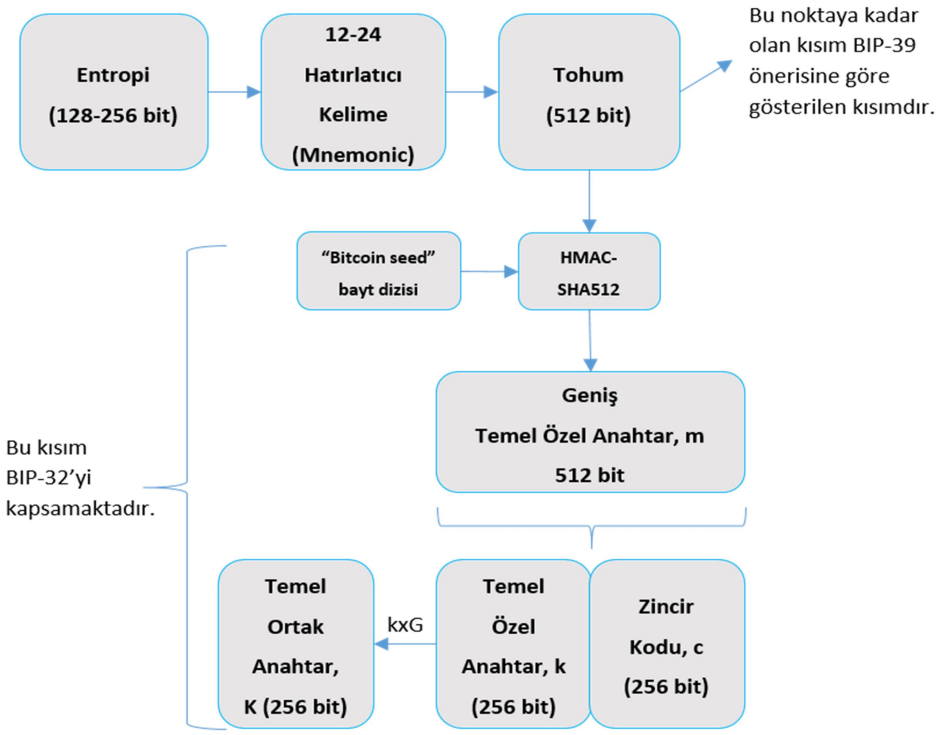
BIP-32 ağaç yapısına benzetilmektedir. En başta kök ya da temel anahtar diye tabir edilen anahtar ve bundan türetilen üst ve alt anahtar çeşitleri bulunmaktadır. Üst anahtarlardan alt anahtarlar üretilir, alt anahtarlardan onların da altı olan daha derine doğru alt anahtarlar üretilir ve bu şekilde devam edip dallanır. Fakat alt anahtarlardan üst anahtarlar tekrar geri getirilemez, sistem sadece üstten alta tek yönlü anahtar üretme şeklinde çalışır. Bunun sebebi üst anahtarlardan alt anahtarlar üretilirken üst anahtarların tek yönlü fonksiyon olan HMAC-SHA512 özet algoritmasından geçirilmesidir.

Cüzdana ait anahtarların üretilirken ilk temel anahtar oluşturulduktan sonra üst anahtardan alt anahtarları türetmekte kullanılan dört metot bulunmaktadır. Bu metotlar:

- Normal Alt- Geniş Özel Anahtar Hesaplama
- Zorlaştırılmış Alt- Geniş Özel Anahtar Hesaplama
- Normal Alt- Geniş Açık Anahtar Hesaplama
- Zorlaştırılmış Alt-Geniş Ortak Anahtar Hesaplama

Normal ve zorlaştırılmış kavramları kullanılan indeks numarasının aralığı ile ilgilidir. İndeks numarası 0 ile2147483647 (2^{31}-1) arasında olanlara normal, 2147483647 (2^{31}-1) ile 4294967295 (2^{32}-1) arasında olanlara zorlaştırılmış (hardened) anahtar denilmektedir.

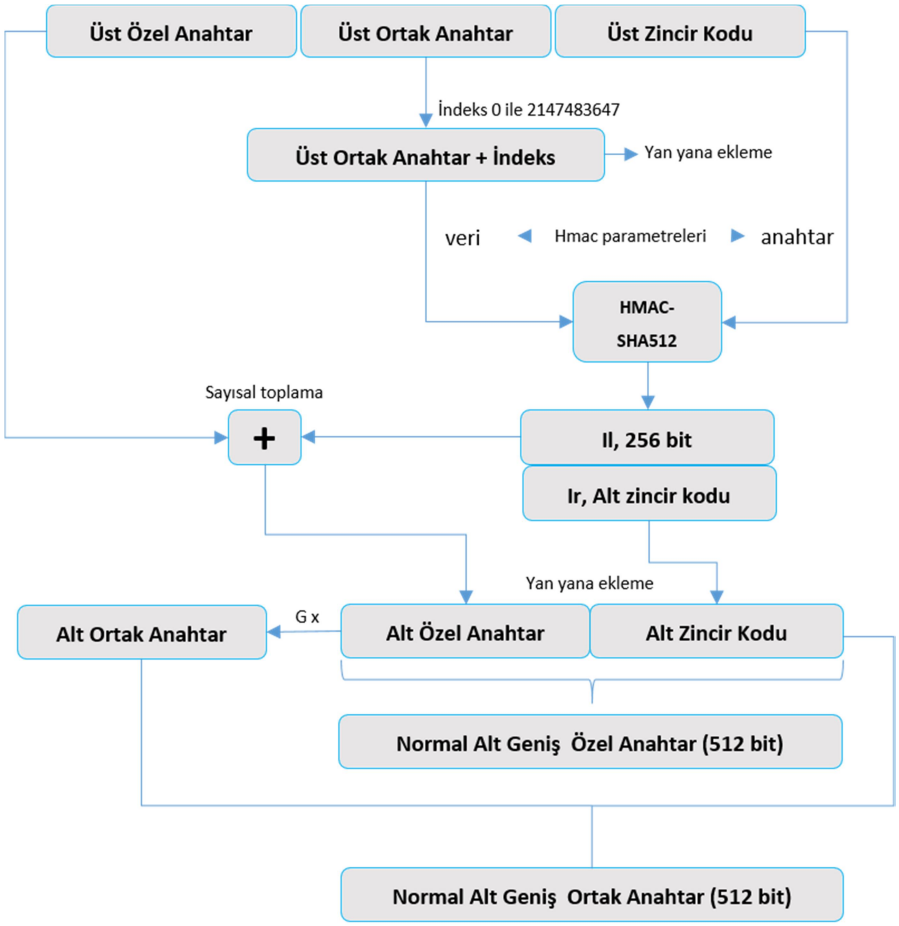
Anahtarlardaki “Geniş” ya da “genişletilmiş” ibaresi, anahtarın sonuna ilgili zincir kodunun eklenmiş olduğunu gösterir. Geniş anahtar hiyerarşik deterministik cüzdanda yeni anahtarlar türetmeyi sağlayan özel veya ortak anahtardır. Tek bir üst geniş özel anahtar, bu anahtarın altındaki tüm özel ve ortak anahtarların kaynağıdır. Bu yüzden tek bir üst geniş özel anahtar ile bu üst anahtara ait tüm alt özel ve ortak anahtarlar tekrar türetilebilir. Ayrıca bu üst özel geniş anahtara karşılık gelen üst geniş ortak anahtarla aynı ortak anahtarları türetmek mümkündür. Bu özelliği farklı iş senaryolarına imkân tanır. Sık sık yedekleme gerekliliğinden kurtulmak için deterministik cüzdanlar, tek bir tohumdan diğer tüm anahtarları türetmeye yarayan temel anahtar oluşturur. 128 bit ile 512 bit arası uzunluğunda bir tohum üretilir ve çevrimdışı bir anahtar deposunda saklanır. BIP-32, secp256k1’in eliptik eğrisini kullanarak hiyerarşik anahtarların türetilmesini gösterir. Şekil 5’te, alt anahtar türetme fonksiyonunda (CKD) tanımlı temel anahtarın nasıl genişletileceği gösterilmiştir.



Şekil 4: Temel Anahtar Oluşturulması (IntKyn. 6

Normal Alt-Geniş Özel Anahtar

Bu anahtara normal denmesinin sebebi HMAC-SHA512 fonksiyonunda kullanılacak olan indeks numarasının 0 ile 2147483647 (2^{31}-1) arasında seçilmesidir.



Şekil 5: Normal-Alt Geniş Özel Anahtar Hesaplama

Özet olarak üst geniş özel anahtar ve indeks numarasını HMAC fonksiyonundan geçirerek (üst ortak anahtar + indeks, zincir kod) o indekse ait normal alt anahtarı üretmek mümkündür.

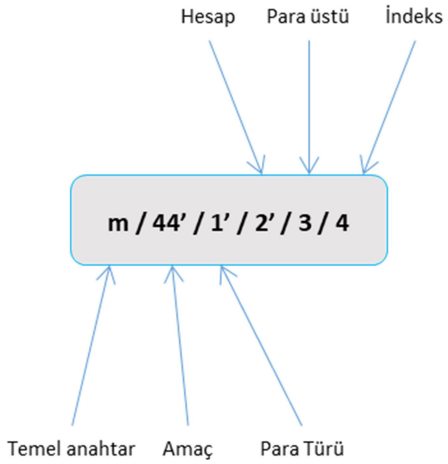
BIP-44

BIP-44, BIP-32'de bahsedilen algoritmaya göre deterministik cüzdan için "Amaç Alanı" sunarak mantıksal bir hiyerarşi önermektedir (IntKyn. 7).

BIP-39'da temel anahtarın üretileceği entropi değeri hesaplandı. BIP-32'de ise ağaç yapısı şeklinde temel anahtardan her genişletilmiş anahtarın kendine ait türetme yolu ile alt ve devam eden daha alt anahtarlar türetildi. Bu türetme yolu istenildiği gibi seçilebilir fakat hiyerarşik deterministik cüzdanın kullanımında anahtarların belli bir yapıda olması cüzdanlar arası uyumluluğu sağlamak adına önem kazanmaktadır. Cüzdanlar arasındaki uyumluluğa yardımcı olması için BIP-44, BIP-32'in türetme yoluna aşağıdaki yapıyı tanıtır.

m / amaç'(purpose') / para_türü' (coin_type') / hesap' (account') / para_üstü (change) / indeks

"/" işareti ağaçtaki derinlik seviyesini ayırmak için kullanılır.

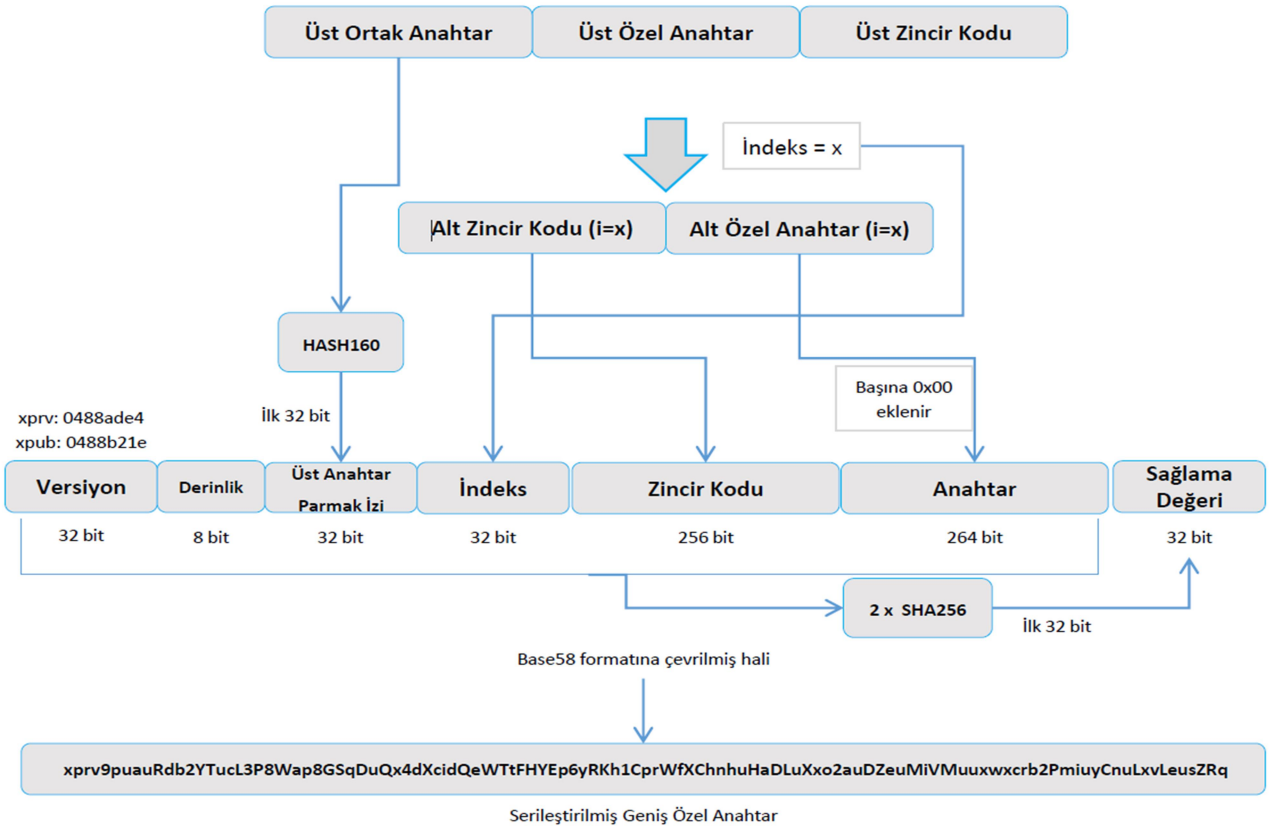


Şekil 6: BIP-44 Derinlik Seviyeleri

Zorlaştırılmış anahtarların gösterimini normal anahtarlardan ayırmak için ise tırnak işareti veya "h" soneki kullanılır. Normal anahtarlar için indeks numarası 0 ile 2^{31} arasında seçilir. Zorlaştırılmış anahtarlar için indeks numarası ise 2^{31} ile 2^{32} arasındadır. Buna göre örneğin indeks numarası 2' veya 2h değeri (2^{31}) + 2 = 2147483650 sayısına eşittir.

Serileştirme

Geniş anahtarlar, blokzincir tabanlı sistemlerde geçerli olmasını sağlayacak son haline kavuşması için serileştirme işleminden geçmektedir. Serileştirilmiş anahtarda Base58 formatında versiyon, derinlik, üst ortak anahtara ait parmak izi, indeks, zincir kodu, özel veya ortak anahtar, sağlama değeri bilgileri yer alır. Şekil 7'de örnek olması açısından özel anahtarın serileştirme işlemine ait adımların gösterimi mevcuttur.

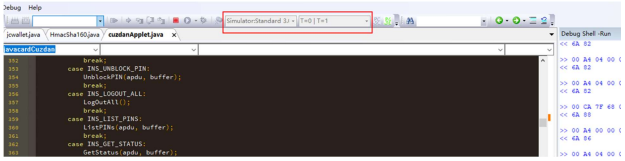


Şekil 7: Serileştirilmiş Özel Anahtar

Base58, büyük sayıları daha kısa ve daha kullanıcı dostu bir biçimde göstermek için kullanılan 58 adet karakterdir. Bu karakterler: “1 2 3 4 5 6 7 8 9 A B C D E F G H J K L M N P Q R S T U V W X Y Z a b c d e f g h i j k m n o p q r s t u v w x y z”. Bu karakterlerde görüldüğü gibi 0, O, I, l gibi karıştırılası kolay harfler bulunmamaktadır.

3.3 *Donanımsal Deterministik Cüzdan Uygulaması*

Bu bölümde java akıllı kartına yüklü HD cüzdan uygulaması ile bitcoin transferi yapılmıştır. İlk olarak uygulama kodları derlendikten sonra oluşan “cap” dosyası karta veya kart simülatörüne yüklenecektir. Şekil 8’de uygulama simülatöre yüklenmesi gösterilmiştir.



Şekil 8: Uygulamanın (Applet) derlenip karta ya da simülatöre yüklenmesi

Karta yüklenen uygulamanın AID’si “cuzdanApplet” kelimesinin hex halidir: 63 75 7A 64 61 6E 41 70 70 6C 65 74.Daha sonra kart ilklendirilecek ve cüzdana ait anahtarlar üretilecektir. “cuzdanApplet” uygulaması için 00 A4 04 00 0C 63 75 7A 64 61 6E 41 70 70 6C 65 74 Select komutuyla karttaki cüzdan uygulamasını seçilir. B0 3C 00 00 00 Get Status komutuyla cüzdanın durumuna bakılır. Get Status komutu akıllı kartta yüklü cüzdan uygulamasına ait versiyon bilgisi (4 bayt), PIN deneme sayısı gibi genel bilgileri vermektedir. Karta Setup komutuyla PIN’ler başarılı şekilde yüklendiyse kartın Get Status komutuna döndüğü değer: versiyon bilgisi (4 bayt) + PIN0-PUK0-PIN1-PUK1+deneme sayısıdır (4 bayt). Karta henüz Setup komutuyla PIN yüklenmediyse 9C04 hatası döndürülür.

Karttaki uygulamaya ait PIN’lerin yüklenmesi, BIP-32 objelerinin oluşturulması gibi uygulamanın hassas bilgilerinin ilklendirilmesi ve kart belleğinde yerlerinin ayrılması Setup komutuyla gerçekleştirilir. Karta Setup komutuyla PIN’ler başarılı şekilde yüklendikten sonra B0 42 00 00 04 3x3x3x3x (PIN: xxxx) Verify komutuyla kullanıcıdan istenen PIN doğrulanır. Karta gönderilen Import BIP32 Seed komutu ile kartta temel anahtar ve zincir kodu üretilir ve bu üretilen değerler kart içerisinde set edilir. Belirlenen türetme yoluna ait indeksler karta Get BIP32 Extended Key komutuyla

gönderilir. m/44'/1'/0' türetme yolu için örnek Get BIP32 Extended Key komutu; B06D03400C8000002C8000000180000000.

Karta gönderilen Get BIP32 Extended Key komutu ile temel anahtardan genişletilmiş alt anahtar hesaplanır ve dönüş olarak alt zincir kodu, alt ortak anahtar ve anahtarların imzalı halleri döndürülür. Kartın bu komuta verdiği cevabın yapısı: 32 bayt zincir kodu, 4 bayt ortak anahtar uzunluğu, ortak anahtar, 4 bayt imza boyu, imza, 4 bayt imza2 boyu, imza2'dir.

Kartın ilklendirmesi tamamlandıktan sonra cüzdana ait adresler Şekil 9'deki gibidir.

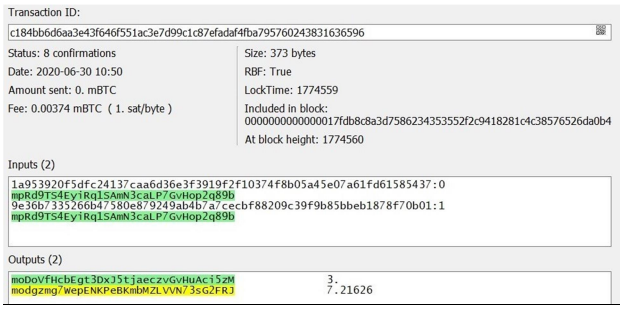
Type	Address	Balance	Tx
receiving	mpRd9TS4EyiRq1SAmN3caLP7GvHop2q89b	0.	3
receiving	moDoVfHcbEgt3DxJ5tjaeczvGvHuAci5zM	3.	1
receiving	mnhUbk58RWqZ9dk5G47QsSsQVppXfwxwVp	0.	0
receiving	myc2vVArj4M97poiTCaXM44vwdYZJ7gZCq	0.	0
receiving	msCkFmoc8grEKmLUuguR37n1TGmpXKQzje	0.	0
receiving	mwqoAgJTy58g9u1sLKNMjb56L2WUkDjnpa	0.	0
receiving	mtMvx2fCBi313Ygf8yA52t2T474pP3dggk	0.	0
receiving	muGzPmQZSuhaqiLNBqX1iZ3oMKm5ks5qCC	0.	0
receiving	n4Jem6VLFNCJYNWMxCCZdcssufjRA3gmvm	0.	0
receiving	mh6YBCS82k87HBeVCBKP4QFG2xkLHwQaDk	0.	0
receiving	miiikJ5wVziHjS8QQHu2gZ68KG6KqeRtqt	0.	0
receiving	n1rfrPvJxopZZrsQ18CsFDeCVjMkwt2r8S	0.	0
receiving	mqstTPYzfVvjdWFY5ajWHTCs29kSADHArr	0.	0
receiving	mnDRUpAKsSJUYs13BNsxvsGHKtYzjRPrp7	0.	0
receiving	muUqsMr9UbAdDRi9Uqcd3Cueg4DtHsJxuZ	0.	0
receiving	mnKq9hjCtUWRuLBpRgXhkL89GQqGraRBZz	0.	0
receiving	n1BiJoqDv2P5GcCnQHzTctoTAwwAGzWutD	0.	0
receiving	mrnyxVm2U2FLPDmBzKpbygeJtfyDz6gEwc	0.	0
receiving	mrm9XiCDU488V8nfMAPrDzF7iKkPY2TFwi	0.	0
receiving	mjKesKdfTgf46aenJWnn8nAGaA7HRVisVK	0.	0
receiving	mhR4iVdfmfKzCBrxiHDzX4h29n5KX7Xdfi	0.	0
receiving	mxTJKBPU9z4K2G7gHJtjkTa5QpzN52rUFr	0.	0
change	modgzmg7WepENKPeBKmbMZLVVN73sG2FRJ	7.21626	1
change	mmgy1Epo9WR9wQDVmdrmWB16W1gGQUN75P	0.	0
change	moGVZmyQ5KcYCw7TXZkdGyFwwSkF7wZGv3	0.	0
change	mnwzJJY1AxkW722Nq55gK3MFP6hefz5tWy	0.	0
change	mvfShh1mx6LnmayG9njT3uwHAxHxeiG91x	0.	0
change	mmYGszJMoAWg5ch7NukTxvTvfqBC5WV2Xd	0.	0
change	mxhHKCzA5625PUx11uP1ccoVuJB2HC52hW	0.	0

Balance: 10.21626 mBTC

Şekil 9: Cüzdana ait adresler

Transfer işleminin gerçekleşmesi için kartın işlem özetini güvenli bellekte tutulan alt özel anahtarı ile imzalaması gerekir. Karta gönderilen Sign Transaction APDU komutu bunu yapmaktadır.

Transfer işlemi gerçekleştirilmeden önce cüzdandaki "mpRd9TS4EyiRq1SAmN3caLP7GvHop2q89b" adresinde 10.22 mBTC bakiye bulunmaktaydı. Transfer işlemi ile birlikte cüzdandaki diğer "moDoVfHcbEgt3DxJ5tjaeczvGvHuAci5zM" adresine gönderilen 3 mBTC transferine ait işlem bilgileri Şekil 10'daki gibidir. Girdi olarak "mpRd9TS4EyiRq1SAmN3caLP7GvHop2q89b" adresinden harcanmamış işlem olan 10 mBtc ve 0.22 mBtc bakiyelik 2 çıktı seçilmiştir. İşlemin çıktısı, gönderimi yapılan adres "moDoVfHcbEgt3DxJ5tjaeczvGvHuAci5zM" (3 mBTC) ve para üstü adresi olan "modgzmg7WepENKPeBKmbMZLVVN73sG2FRJ" (7.21626) adresidir. 10.22 – 3 – 7.21626 = 0.0074 mBTC, işlemi bloğa ekleyen madenciye verilen ücret miktarıdır.



Şekil 10: İşlem Bilgileri

3.4 AKiS Kart Donanımsal Deterministik Cüzdan Tasarımı

AKiS yerli ve milli imkânlarla TÜBİTAK BİLGEM tarafından geliştirilmiş akıllı kart işletim sistemidir. Kimlik, pasaport, ehliyet, elektronik imza gibi farklı uygulamalar için altyapı sağlamaktadır. Ortak Kriter (Common Criteria) CC EAL 5+ ve üstü güvenlik değerlendirmelerinden geçmiş ve sertifikasını almış akıllı kart mikroişlemcileri üstünde koşmaktadır. Bu mikroişlemciler arasında İnfineon, NXP ve milli yonga olan UKTUM çipleri yer almaktadır.

AKiS'in en yeni sürümünde kart canlandırıldıktan sonra ilk olarak uygulamaların bellek alanlarını kontrol eden, kısıtlarını belirleyen ve uygulamayla çekirdek arasında iletişimi sağlayacak olan Kart Yöneticisi uygulaması yüklenmektedir. Yeni sürüm AKiS'te kimlik, pasaport, ehliyet, e-imza, bilet gibi uygulamalar tek bir kart içinde toplanabilmektedir. Uygulamalar için karttaki bellek alanı bölünebilmektedir ve bir uygulama diğer uygulamanın bellek alanına erişmesini engelleyecek güvenlik duvarı mekanizması kartın donanımı tarafından sağlanmaktadır. Böylece her uygulama kendine tahsis edilen bellek alanı dışına çıkıp diğer uygulamaların bilgilerine erişemez.

Bu sürümle birlikte kartın içinde olan uygulamalardan biri de cüzdan uygulamasıdır. Yukarıda uygulaması yapılan kripto para olarak bitcoin transfer işlemlerini yapabilecek özellikte

tasarlanmıştır. BIP-32, BIP-39, BIP-44 ve eliptik eğri kriptografik işlemlerini destekleyecek şekilde geliştirilmektedir. BIP-32, BIP-44, BIP-39'a göre anahtarlar türetilmekte ve bitcoin kripto para transfer işlemi için standart eliptik eğri "secp256k1" üzerinde ECDSA kullanılarak imzalama işlemleri yapılabilmektedir. AKiS cüzdanın nihai durumuna gelebilmesi için geliştirilmesi devam etmektedir.

Bitcoin'den farklı diğer kripto paraları da destekleyecek nitelikte olabilmesi için çalışmalar başlamıştır ve devam etmektedir. Bununla birlikte cüzdan ile blokzincir ağına bağlantısını sağlayacak ara yüz çalışması yapılması planlanmaktadır. Bu bağlantı mobil ve masaüstü makineler için düşünülmektedir.

4. Sonuç

Çalışmada ilk olarak, neredeyse insanlık tarihi kadar eski olan paranın tarihsel süreci ve süreklilik arz eden değişimi ile birlikte özellikle son zamanlarda kullanım alanın kripto paraya doğru genişlemesi durumundan bahsedilmiştir. Ayrıca mevcut merkezi sistemden dağıtık sisteme geçilmesinin anlatıldığı bir giriş sunulmuştur. Kripto paranın güvenli bir ortamda saklanabilmesini sağlayan cüzdan kavramından bahsedilmiştir. Sonraki bölümlerde blokzincirin işleyişinin ve mekanizmasının anlaşılması, cüzdan çeşitlerinin incelenmesi ve karşılaştırılması, donanımsal hiyerarşik cüzdanın yapısı, işleyişi ve akıllı kartlar ile kullanımı detaylı şekilde incelenmiştir. Çalışma mekanizması kısmında BIP-32, BIP-39, BIP-44 protokollerine göre cüzdanın anahtarlarının üretilme adımları sıralanmıştır. Uygulama kısmında ise örnek donanımsal cüzdanda tanımlı APDU komutları ile akıllı karta HD cüzdan uygulaması yüklenmiş, kartın ilklendirilmesi yapılmış ve Bitcoin Testnet ağında para transferiyle örneklendirilmiştir. Son kısımda ise AKiS işletim sisteminden bahsedilmiştir. Yerli ve milli işletim sistemi olan çoklu uygulamayı destekleyen AKiS'in yeni sürümüyle cüzdan uygulamasının tasarımı yapılmıştır. Bu versiyonda anahtarlar türetilip bitcoin kripto para transfer işlemi için standart eliptik eğri "secp256k1" üzerinde ECDSA kullanılarak imzalama işlemleri yapılabilmiştir. Diğer para türlerinin de desteklenmesi için çalışma ve geliştirmeler sürmektedir.

Teşekkür

Bilgi ve deneyimleriyle çalışmanın tamamlanmasında bana yön veren danışmanım Sayın Dr. Hüseyin YÜCE'ye teşekkürlerimi sunarım. Bu süreçte katkılarıyla değerli Dr.Ercan ÖLÇER'e teşekkürü bir borç bilirim.

5. Kaynaklar

Bamert, T., Decker, C., Wattenhofer, R. and Welten, S., 2014, September. Bluewallet: The secure bitcoin wallet. In International Workshop on Security and Trust Management. Springer, Cham, 65-80.

Bulut, Y.E., 2019. Secure Hardware Cryptocurrency Wallet within Common Criteria Framework. Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 105.

Buterin, V., 2013. Ethereum white paper. GitHub repository. EOS. IO technical white paper v2.

Dursun, T., 2020. Blokzincir Teknolojisi. *TÜBİTAK BİLGEM Kurumsal Dergisi*, **8**, 10-15.

Karayew, D., 2012. The history of credit cards. Doctoral dissertation, Видавництво СумДУ.

Mishkin, F.S., 2007. The economics of money, banking, and financial markets. Pearson education.

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

Skála, M., 2018. Bitcoinová peněženka pro Android podporující zařízení TREZOR. Bachelor's thesis, České vysoké učení technické v Praze. Vypočetní a informační centrum, 71.

Smithin, J., 2000. What is Money? Routledge international studies in Money and banking. ISBN 9780415206907. URL https://books.google.com.tr/books?id=MDU-NTEJziMC. (erişim: 01.12.2019).

Usta, A., 2018. Paranın Serüveni-Kripto Paraların Öncesi ve Sonrası. Bankalar Kart Merkezi, 0-23.

İnternet Kaynakları

1- https://www.ibm.com/blockchain/hyperledger, (erişim: 05.07.2020). IBM Blokchain based on Hyperledger Fabric from the Linux Foundation.
2- https://wiki.trezor.io/Trezor. (erişim: 12.02.2020). Trezor Hardware Wallet.
3- https://github.com/LedgerHQ/ledger-javacard. (erişim: 26.11.2019). Java Card implementation of Ledger Bitcoin Hardware Wallet.
4- https://coinmarketcap.com/all/views/all/, (erişim: 24.03.2020). CoinMarketCap. All Cryptocurrencies.
5- https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki (erişim: 19.02.2020). Mnemonic code for generating deterministic keys.
6- https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki. (erişim: 19.02.2020). Hierarchical Deterministic Wallets.
7- https://github.com/bitcoin/bips/blob/master/bip0044.mediawiki. (erişim: 19.02.2020). Multi-Account Hierarchy for Deterministic Wallets.