Kayıtzinciri(Blockchain)'ne Giriş ve Enerji Sektörüne Muhtemel Etkileri

Barış Sanlı, Murat Alanyalı

Not: Bu yazı taslak durumundadır. Amaç bir sistemi mümkün olduğunca basit olarak anlatırken, dünyadaki bu baş döndürücü gelişmelerden okuyucuları da biraz bilgilendirmektir. Bilinçli olarak yanlış bir anlatım yoktur, gene de yakalanan hataları barissanli2@gmail.com adresine gönderirseniz seviniriz.

Kayıtzinciri teknolojileri anlaması biraz zor olsa da enerji gibi giderek dijitalleşen fiziksel sektörlerin çalışma şeklini etkileyecektir. Kayıtzinciri teknolojisini tek başına değil, ama nesnelerin interneti, paylaşım ekonomisi, dağıtık enerji kaynakları, dijitalleşme ile sürekli etkileşim halinde düşünmek faydalı olacaktır. Yani enerji sektöründeki etkisi değişen fakat kalıcı olma ihtimali yüksek olan bir mümkünleştirici teknolojidir. Fakat anlaması zor olan bu gelişmeyi, mümkün olduğunca basit bir şekilde anlatmak neler yapabileceğini anlamak açısından önemlidir.

Bu yazıda, kısaca kayıtzincirinin düşünsel temelleri, Bitcoin örneği ile nasıl çalıştığı anlatılarak, enerji sektöründeki mevcut uygulamaları ve uzmanların gelecek görüşleri verilecektir. Şifreleme kısmından çok özütleme kısmı ve bir matematiksel bulmacayı çözme şekli kalbidir. Her ne kadar gizli, isimsiz bir yapı sunduğu iddia edilse de, algoritmalar dünyasında bir masaüstü bilgisayarın oluşturduğu bulmacayı dünyanın en gelişmiş şifreleme araçlarına sahip devletlerin göremeyeceğine inanmak saflık olur. Zaten sistemde herkes genel anahtarı ile gözükmektedir. Genel anahtarın kime ait olduğunu sıradan insanların bilme ihtimali düşüktür.

Kayıtzincirinin, Bitcoin örneği ile nasıl çalıştığı detaylı anlatılmıştır, çünkü bir çok insan için anlaması ilk bakışta karışıktır.

Giriş

Bir güveni tesis etmenin yolu nedir? Ağ toplumunun bu soruya cevabı, güvensizliği kurumsallaştırmak olmuştur. Yani tarafların birbirine güven duymaya ikna edilmesi yerine, tarafların birbirine güvenmeden, tüm kayıtları bölüşerek güveni kendi kendilerine tesis edebilecekleri algoritma, sayılar, süreçler ve kuralların tasarlanması yani bir anlamda güvensizliği kurumsallaştırmaktır.

Bu sayede kimse kimseye güven duymak zorunda değil, ama bir güven tesis etmek istendiğinde kendi bilgisayarında herkesin tüm işlemlerinin doğru onaylanıp onaylanmadığını, geçerli olup olmadığını test edebilecektir. Her birim, kimseye güvenmeden aynı kuralları uyguladığında ise birbirini -çok büyük ihtimalle- hiç tanımayan ve zerrece güven duymayan taraflar tarafından objektif kurallarla doğrulanmış geçmiş kayıtların değiştirilemediği dağıtık bir "kara kaplı defter" oluşturulmuş oluyor.

Bu dağıtık kara kaplı defterle ne yapılabilir? İlk uygulaması bankacılık sisteminden bağımsız bir değer takas sistemi yani Bitcoin oldu denebilir. Fakat olay burada duracağa benzemiyor.

Düşünsel Temelleri

Bilgisayar çağında, -birçok dönemin yanında- Napster öncesi ve sonrası dönemden bahsetmek mümkün. Napster uçlar arası (peer-to-peer) dosya paylaşım programı olarak 1 Haziran 1999'da hizmet vermeye başladı[i]. İnsanlar birbirleri ile dosya paylaşmaya başladıkları zaman ise müzik dosyaları bölüşmeye başladılar. Önce metal grup Metallica, sonra Dr. Dre gibi ABD'deki önemli müzik isimlerinin davaları sonucunda Haziran 2001'de Napster sistemini kapatmak zorunda kaldı. Ama dağıtık dosya paylaşımı süreci başlamıştı.

Müzikte dijital format ile verilerin bölüşümünün önünün açılması ise önce Apple iPod/iTunes ile mümkün olmaya başladı. Daha sonra ise insanların müzik dosyalarına sahip olmak yerine, bu müzikleri istedikleri zaman istedikleri şekilde dinleyebilecekleri sistemlere geçmeleri ile evrilmeye devam etti. Emtiayı değil (kaset, CD), emtianın sağladığı faydayı elde etme (bulut müzik servislerine) evresine geçildi. Fiziksel bir sektör dijitalleştirilmiş oldu.

Dağıtık sistemler Internet'in kuruluş felsefesinde olduğu için, internetin oluşturduğu evren dağıtık her türlü hizmete imkan verebiliyor, hatta bu tip hizmetleri arttırıyordu. Fakat Napster bunun "askeri amaçlar hariç" nasıl yapılacağını milyonlara ispatlamış oldu.

Diğer önemli bir akım ise Şifreli-Anarşistler oldu. Timothy C. May'in 1988'lerin ortasında kaleme aldığı ve bir çok siber-punk sitesinde bulunabilen "The Crypto Anarchist Manifesto", Bitcoin için ilham kaynaklarından biridir. Manifesto "Bilgisayar teknolojisi .. kişilerin birbiriyle tamamen isimsiz olarak iletişim kurup etkileşime girebilecekleri bir durumdadır" şeklinde başlıyor. "Gelişen teknolojiler ile birleştiğinde şifreli anarşism kelimelere ve resimlere dökülebilen her türlü materyal için likit bir piyasa oluşturacaktır"[ii] öngörüsünde de bulunuyor. Söz konusu manifestodaki hemen hemen tüm teknolojilerin NSA tarafından geliştirilmiş olması da komplo teorilerine girilmeden not edilmelidir.

May'in öne çıkardığı bir çok teknoloji olmasına rağmen, genel ve özel şifreleme sistemi [public-private key] üzerinden kurulacak bir iletişim çekirdeğinden etkilendiği anlaşılmaktadır. Manifestosunda Bitcoin'i gerçeğe dönüştüren en anahtar teknolojilerden özüt[hash] teknolojisinden ise bahsetmemektedir. Oysa özüt fonksiyonlar 1970'lerden beri biliniyordu[iii].

Bu manifesto daha sonra Wei Dai isimli bir bilgisayar programcısını çok etkiliyor. Dai Microsoft'ta şifreleme araştırma bölümünde çalışan ve meşhur bir C++ programlama dilindeki şifreleme kütüphanesinin de programcısıdır. Dai'nin 1998 yılında "Tim May'ın şifreli anarşisinden çok etkilendim" diye başlayan "B-money [b-para] dosyasında[iv], "anarşi"yi hükümetin kaldırılması olarak değil, "tamamen gereksiz" hale getirmek olarak tanımlamaktadır. Yani merkezi bir kontrole ihtiyaç bırakmayan, onun yanında çalışan bir yapı öngörmüştür. 1998 yılındaki B-Money fikri, "isimsiz, dağıtık bir elektronik ödeme sistemi" olarak tasarlanmıştır. Bitcoin'in gizli tasarımcısı "Satoshi Nakamoto"'da Bitcoin'i anlattığı makalesinde bu dökümana atıfta bulunmuştur. Dai, May'in fikirlerini gerçekleştirebilecek bir ödeme sistemi tasarlamıştır. 1998 yılındaki ödeme sistemi kurma fikri ancak 2009'da gerçekleşebilmiştir.

Dai'nin dökümanında iki protokol tanımlanmaktadır. Bu protokollerde herkes genel şifreleri ile tanımlanmaktadır. İsimler yoktur.

Birinci protokol beş kısımdan oluşmaktadır. Şimdilik önemli olan ilk iki kısmı şöyledir.

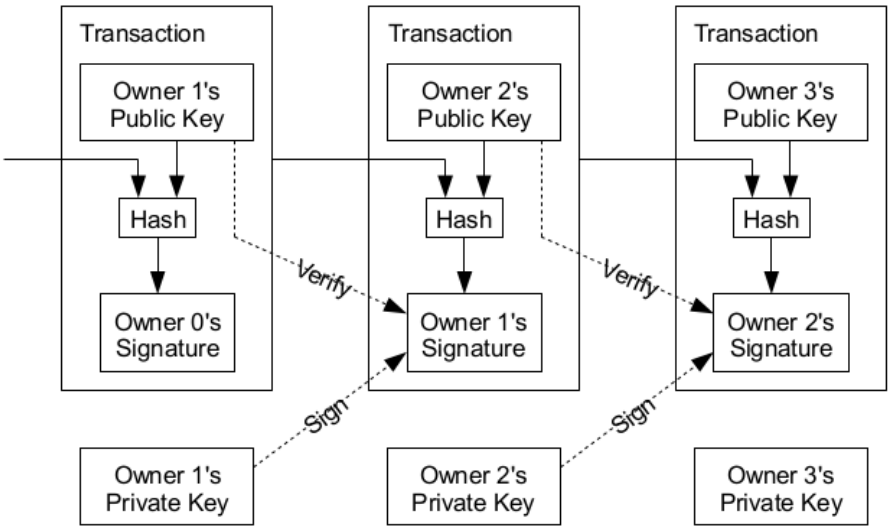
1. "mining" denilen, paranın oluşturulması şöyle tanımlanmaktadır : "Daha önce çözülmemiş bir matematiksel[hesapsal]problemi çözdüğünü duyurarak herkes para yapabilir". Çözüm için harcanan hesaplama eforu ile çözüm değer kazanmaktadır. (matematiksel çözüm için harcanan elektrik mesela)

2. Paranın transferinde ise Ali, Ayşe'ye para gönderirken kendi genel anahtar adresinden Ayşe'nin genel anahtar adresine X miktar kadar para transfer ettiğini duyurur. Bu mesajı Ali kendi özel anahtarı ile imzalar, böylelikle Ali'nin genel anahtarına sahip herkes bu işlemi doğrulayabilir.

İkinci protokolde ise sistemin dağınıklık seviyesi ile ilgili tespitler vardır.

Yani Timothy May, Wei Dai'yi, Wei Dai'de Bitcoin'in mucidi ve gerçek kimliği bilinmeyen -Avustralyalı bir kişi olduğu da iddia edilmekle birlikte-, Satoshi Nakamoto'yu etkilemiştir.

Satoshi Nakamoto'nun "Bitcoin: A peer-to-peer Electronic Cash System" makalesinde[v] Bitcoin uçtan uça, finansal sisteme girmeden, bir tarafın diğer tarafa çevrimiçi ödeme yapmasına imkan veren sistem olarak tanımlanmaktadır.



Nakamoto, bir işlemin geri çevrilebilmesi yani değiştirilebilmesinin güvene olan ihtiyacı arttırdığını, bu yüzden de işlem maliyetlerinin arttığını ve finansal kurumlara ihtiyaç duyulduğunu anlatmaktadır. Bunun içinde "iki defa harcama" problemine(bir kişinin aynı parayı iki defa eş zamanlı harcamasına) çözüm olacak bir yöntem önermektedir.

Teknoloji

Bitcoin teknolojisinde iki önemli bölüm vardır. Birincisi matematiksel kısım. Burada iki anahtar teknoloji kullanılmaktadır.

1. Özüt [Hash): Özüt aslında bir uzun sayıdır. Özelliği, her hangi bir bilgi yığını için -neredeyse- o yığına özel özet bir rakamdır. Bitcoin ABD NSA (ulusal güvenlik ajansı) tarafından tasarlanan SHA-2 ailesinden SHA 256 şifreli özüt fonksiyonunu[vi] kullanmaktadır.

Özüt ne işe yaramaktadır? Özüt fonksiyonuna girdi olarak bir karakter dizini veya bilgi girildiğinde sadece o diziye özgü bir rakam oluşturmaktadır. O dizide en ufak bir değişiklik yapıldığında ise tamamen çok farklı bir rakam oluşturmaktadır. Yani kasa hırsızlığı gibi, birer karakter değiştirerek sonuca yaklaşmak mümkün değildir. Aksine her bir karakter değişimi ile özüt çok daha farklılaşmaktadır. "mining" yani Bitcoin madenciliği tamamen özüt sistemi üzerine kuruludur.

Özütler matematiksel olarak tek yönlü fonksiyonlardır.

f(x)=y için

Yani x'den y'yi elde ederken, y'den x elde edilememektedir. Tek yöntem tek tek x'leri deneyerek y'yi bulmaktır. Bu da sadece x, y birlikte gönderildiğinde, x'de en ufak bir değişiklik olduğunda y'nin de değişeceğini hem de eski haline benzemez şekilde değişeceğini garanti eder.

Bitcoin'de "proof of work" -işin yapıldığının ispatı- yani madenciliğin hak ettiği paranın ispatı, özütleme fonksiyonu ile sağlanmaktadır. Mesela "barış" kelimesinin özütü "5b4eee...." 16lık düzende 64 haneli bir sayıdır.

Wei Dai'nin anlattığı ve Bitcoin makalesinde de yer alan matematiksel bulmaca ise bu SHA256 özütün (Bitcoin de iki defa SHA256 alınır, güvenlik için) ilk belirli sayıda karakterinin 0 olması istenir. Bunun için orijinal metine bir sayı eklenir. Ör:

"barış 78743"'ün özütü "0000281b7…" şeklindedir. Yani 4 tane sıfırla başlamaktadır. Bitcoin terminolojisinde "78743" bir nonce yani ek denmektedir. Metni bu ek ile özütleyen istenen zorluk seviyesinde (Ör: dört tane sıfır ile başlayan) daima aynı rakamı bulmaktadır.

"barış 261173"'ün özütü ise "00000e6d1bf…." şeklindedir. Sıfır sayısı 5'e çıkarken, "barış" metnine eklenen rakamı bulmak daha da zorlaşmıştır.

6 sıfırla başlayan bir özüt bulmak ise, çok daha uzun sürmektedir ki bu "barış 13286012" metni olup, özütü "000000243…."'dür.

Yani yukarıdaki f(x) fonksiyonunda x dizininin sonuna rastgele karakterler ekleyerek başlangıcı belirli miktarla sıfır ile başlayan y'ler elde edilmeye çalışılmaktadır. Özütün başında istenen arka arkaya 0 miktarı zorluk derecesini belirlerken, zorluk derecesini sağlayan ek rakamı bulan ilk kişi de ödülü hak eden kişidir.

Bitcoin'de her bir kayıt iki kısımdan oluşmaktadır. Başlık ve işlemler kısmı. Herbir başlıkta bir önceki kayıtın özütü de bulunur. Bu şekilde bir kayıt-zinciri oluşturulur.

İşlemlerin Merkle ağacı ile özütlenmesi sonucu elde edilen Merkle kökü, kayıt başlığında yer alır. "nonce" yani ek sayı da kayıt başlangıcına konur. Bitcoin'i değiştirmenin zorluğu ise, her bir blok başlangıcında bir önceki bloğun baş kısmının özütünün olmasıdır. Yani bir blok değiştiği zaman o bloğun özütü, sonraki bloğun özütü vs değişmek zorundadır. Zorluk derecesine göre yeni baştan, özüt rakamın ilk hanelerini sıfır yapan ek sayıları tekrar hesaplamak gerekir. Bu sebeple tüm ağdaki gücün %51 ve fazlasını ele geçirmeyen sistemi değiştiremez deniebilir. Çünkü en ufak bir karakter değişiminde en az önceki kadar efor harcayarak, zorluk derecesindeki özütleri bularak, en son yapılan işleme erişmesi gerekir. Dolayısıyla bir işlem ne kadar eskiyse de değiştirilmesi o kadar zorlaşır. Artan bilgisayar gücüyle problem daha hızlı çözüldükçe, zorluk derecesi de arttırılmaktadır.

2. Genel ve özel anahtar şifreleme: Genel ve özel anahtar iki ayrı sayı dizisidir. Anahtar denilen şeyler sayılardır. Kural olarak bu sayılar o kadar büyük asal sayılardan türetilmiştir ki, genel anahtardan özel anahtar elde edilemez. Dolayısıyla özel anahtarın yaptığı işlemler de elde edilemez.

Genel anahtar, tüm bir ağda para transfer işlemlerinde kullanılan takma isim gibidir. Bu sayı dizisi herkes tarafından görülür. Para gönderen veya alan daima genel anahtardır.

Özel anahtar ise özel saklanan, sadece hesap sahibinde bulunan bir sayılar dizinidir. Genel anahtarla şifrelenen bir metin sadece özel anahtar ile, yani hesap sahibi tarafından çözülerek okunabilir. Özel anahtar çalınır veya kaybedilirse, hesabın sahibi paranın kontrolünü kaybeder.

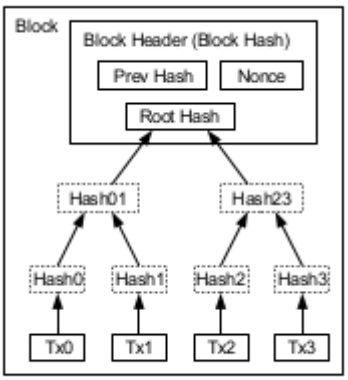
Özel anahtarın bir diğer özelliği ise bir metini imzalayabilir. Metni, imzasını ve genel anahtarını(gene sayılar dizini) karşı tarafa gönderdiğinde, genel anahtar ile imzanın sahibinin genel anahtarın sahibi olan kişiden geldiği ispatlanabilir. Bitcoin'de metin "Ali'den Ayşe'ye X TL transfer et" mesajıdır mesela. Dijital imza ile bu emri verenin Ali olduğu ispat edilir. (Gerçekte biraz daha karışıktır, Ör: A işleminden 2 TL ile B işleminden 3 TL'yi al, Ayşe'ye 4 TL ver gibi)

İkinci grup teknolojiler ise daha çok ağ teknolojileridir:[vii]

1. Uçtan uca ağ: Sisteme giriş engeli çok düşüktür, herkes bir Bitcoin düğümü olabilir

2. Madenciliği: “mining”: Herkes madencilik yaparak, belirlenen zorluk derecesindeki özütü bulabilir. Madenciler aynı zamanda tüm işlemlerinde geçerli olduğunu doğrularlar. Yani olmayan bir paranın harcanmasını engellerler. Bir sonraki bloğa aktarılan özüt, mevcut bloğun sadece baş kısmının özütüdür. Tüm blok özütlenmez.

3. Merkle Ağacı: Bloktaki tüm işlemleri saklayarak bloğun başlangıcına eklemek yerine, tüm işlemlerin ağaç şeklinde özütlenmiş şeklinin nihai özütü bloğun baş kısmına eklenmektedir. Yani bloğun ekinde yer alan işlemlerin hepsinin özütü yerine sadece bunların Merkle ağacı şeklinde özütlenerek kök özütün bulunması bloğun baş kısmında yer almaktadır.



Transactions Hashed in a Merkle Tree

4. Dağıtık konsensus : Genel olarak kararlaştırılan protokol tamamlandığı zaman, doğru düğümlerin[düşman düğümler %50’nin altında] hepsinin aynı değerde uzlaşması olarak tanımlanır. Bitcoinde düğümler her bir işlemde uzlaşmak yerine işlem bloklarında uzlaşırlar. Bir düğüm yeni işlem bloğunu önerir, eğer kabul edilirse o bloğun özütü bir sonraki blokta kullanılır[viii]. Bu da sadece sonuna ekleme yapılabilen bir kayıt mekanizması [append-only ledger] sunar.

Teknik kısmının oldukça karmaşık olduğu düşünüldüğünde, yazarlar ilgilenenler için Princeton Üniversitesinin “Bitcoin ve şifreli parabirimleri teknolojileri” çevrimiçi video derslerini önermektedir[ix].

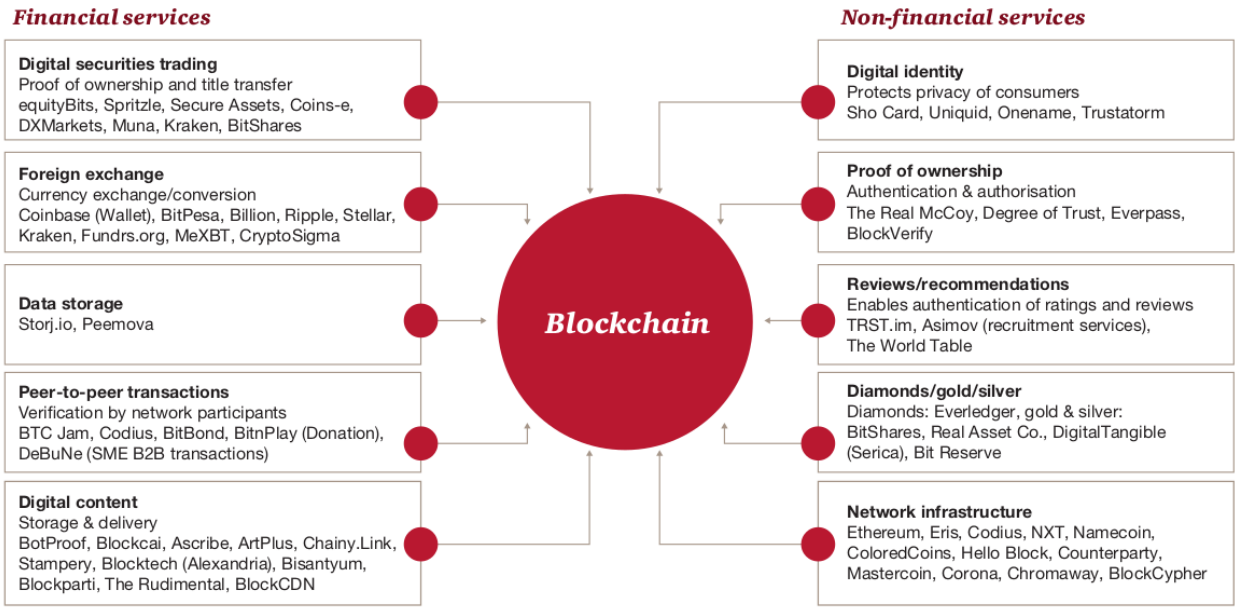
Uygulaması

Tüm bu teknolojiler ile ne elde edilmektedir? Sonunda elde edilen değiştirilemez ve isimsiz olarak işlem yapılabilen bir kayıt defteridir. Bir defa bir kayıt deftere girdiği zaman, isteyen tüm taraflar tarafından geçerliliği doğrulanmaktadır. Sistemde kimin işlem yaptığı bilinmese de, işlem yapanın yaptığı işlemler takip edilebilmektedir. Bu takibi de önlemek için ayrı özel ve genel anahtar üretmek gerekir.

Kayıtzinciri teknolojisini, yazının bu noktasında Bitcoin’den ayırmak gerekir. Çünkü kayıtzinciri ile dağıtık, doğrulanabilir ve tüm tarafların birlikte yönettiği kayıtlar tutulurken, Bitcoin kayıtzinciri ile bir para birimi daha doğrusu elektronik ödeme transferi yönetmektedir. Kayıtzinciri ile örneğin sağlık kayıtları da gizli olarak bölüşülebilmektedir.

Kayıtzincirinin en önemli özelliği üçüncü bir tarafın [Takas tarafı/Banka] dürüstlüğüne ihtiyacı olmamasıdır. Enerji sektörü uygulamasında mesela, bir mahalledeki insanlar birbirine elektrik satıp, hizmet verebilmektedir.

Teknoloji sadece finansal değil finansal olmayan iş ve işlemlerde de kullanılmaktadır. Yani sadece ticaret değil, kimlik bilgileri, sahiplik doğrulanması, ağ altyapıları, tapu işlemleri gibi bir çok konuda kullanılabilmektedir. Çünkü saklanan parasal bir değer olabileceği gibi, herhangi bir veri düzeni de olabilmektedir.



Enerji sektöründeki kayıtzinciri uygulamalarına yönelik olarak en ilginç inceleme ve değerlendirme raporu PWC'in "Blockchain Opportunity for Energy Producers and Consumers"'dir. Kayıtzinciri'nin 3 jenerasyonundan söz edilirken Bitcoin Kayıtzinciri 1.0; akıllı kontratlar Kayıtzinciri 2.0 ve dağıtık otonom organizasyonal yapılarla akıllı kontratlar da Kayıtzinciri 3.0 olarak değinilmektedir.

Raporda ayrıca Bitcoin kadar dağıtık bir sistem yerine bir güvenlik sübabı olarak bir işletmecinin önemine de değinilmektedir. Kayıtzinciri ile paylaşım ekonomisinin, dağıtık elektrik sistemleri ile bir adım daha ileri taşınacağı öngörülmektedir.

Enerji sektöründe ise:

- Dağıtık işlem verilerinin kaydı ile güvenliğin arttırılması ve daha çok bağımsızlığın sağlanması,
- Akıllı kontratların işletilmesi ve dijital işlemlerin yapılması,
- Üçüncü taraflara ihtiyaç bırakmayan iş modellerinin geliştirilmesi

potansiyeli bulunmakla birlikte, bu tip bir teknolojinin mevcut düzenleme yapısında nasıl bir konumda yer alacağı merak konusudur.

Özellikle sayaç, akıllı ev cihazları, ev, akıllı uygulamalar ile varlıkların, işlemlerin, ödemelerin kayıtları, doğrulanması, kontrol edilmesi mümkün olacaktır.

Enerjide Örnek Uygulamalar

New York'da LO3 Energy'nin yönettiği Brooklyn Microgrid(BMG) Nisan 2016'da dağıtık olarak üretilen elektriği komşular arasında kayıtzinciri sistemi ile ticarete konu edilmiştir. 3 hane arasında yapılan işlemin yanında, BMG uçtan uca enerji piyasası iş modeli sunmaktadır[x].

Almanya elektrik şirketi Innogy, ZF ve UBS ile bir araba elektronik cüzdanı teknolojisi [Car eWallet] sistemi geliştirmiştir. Sadece otoyol geçiş ücretleri değil, kırmızı ışıkta durduğunda da elektrikli arabaların endüktif şarj ederek ödeme yapmaları mümkün olacaktır. "Merkezi olmayan bir ulaştırma platformu prototiplenerek inşa edilmiş .... kayıtzinciri, enerji interneti ve hareketlilik lojistik ile yeni bir işlem katmanı oluşturmuştur[xi].

Ethereum tabanlı Slock.it ile Alman RWE ile iki proje yapmaktadır. Birinci projede akıllı kontratlar ile elektrikli arabaların şarj edilmesi, ikinci proje "Blockcharge" ile tüketicilerin akıllı fişler yardımı ile elektrikli arabaların şarjını izlemesi ve kontrol etmesi sağlanmaktadır.

Havayolları milleri mantığı ile çalışan SolarCoin (güneş para)'de ise güneş enerji elektrik üretim noktası ve başvuran doğrulandıktan sonra her 1 Mwh'e 1 SolarCoin verilmektedir. 1 SolarCoin'de ABD Enerji bilgi dairesine göre(ABD için) 680 kg karbondioksit'in engellenmiş olması anlamına gelmektedir.

Ideo Co Lab'ın Akıllı Güneş projesi ise kendi enerjisini takip ederek, kendi yenilenebilir enerji sertifikasını oluşturan ve işlem yapan otonom bir sistem geliştirmiştir. Filament ve Nasdaq ile işbirliği yaparak çalışan bir sistemleri de mevcuttur[xii].

IBM'e göre ise kayıtzinciri dağıtık kaynakların biraraya getirilmesi konusunda yardımcı olabilir, bu da sistem işletmecilerinin istediği yönetilebilir güç kaynaklarını toplulaştırarak (nihai tüketicilerin bir araya getirilerek) hizmet olarak sunabilir[xiii].

Kayıtzincirleri sadece elektrikte kullanılmayıp, petrol ve gaz sektörlerinde de örnek uygulamalarla gündeme geldi. Deloitte'un "Blockchain's Future in Oil and Gas" raporuna göre, petrol ve gaz şirketleri için de değer oluşturulabilecek bir çok uygulama mevcut[xiv]. Bunlar

1. Şeffaflık ve uyum: Kayıtzinciri ile Dodd-Frank Act, EITI ve AB direktifleri kapsamındaki raporlamalar daha şeffaf ve düşük maliyetli yapılabilir.

2. Siber tehditler ve güvenlik: Önemli verilerin küçük parçalara ayrılarak dağınık olarak saklanması ile veri güvenliğinin arttırılmasını sağlayabilir

3. Kayıtzinciri ile nakit, varlık, endüstriyel parçaların hepsi dijital varlığa dönüştürülebilir.

4. Akıllı kontratlar: Dağıtık kayıt sistemi ile kimin ne zaman, nasıl, nerede, neden, kim tarafından ve hangi işlemler gerçekleşince alacağı dijital işlemlerinn merkezinde yer alabilecek.

Fransız bankası Natixis, IBM ve Trafigura ile dağıtık kayıt sistemi Hyperledger Fabric ile ham petrol ticareti için ilk kayıtzinciri çözümünü önerdi. Farklı bankalar da aynı kayıt sistemi üzerinden kayıt tutmakla, tüm taraflar eş zamanlı olarak, işlem durumu, ticaretin doğrulandığı, ham petrolün incelendiği, nihai teslim noktasına kadar bir çok bilgiyi görebiliyorlar[xv].

ING ve Societe Generale kendi kayıtzinciri platformlarını ticaret şirketi Mercuria'nın Çin'e Afrika petrol kargosu satmasında kullanılmak üzere önerdiler. 3 saatlik işlemlerin 25 dakikaya kısaldığını ve maliyetlerin de %30 düştüğünü belirttiler[xvi].

Son dönemde ise Avrupalı 10 büyük enerji şirketi Energy Web Foundation[xvii] adlı bir oluşum başlatarak enerjide küresel bir kayıtzinciri insiyatifi başlattılar. Merkezi doğu Avrupa'da ise PONTON tarafından geliştirilen Enerchain ticaret aracı ile Iberdrola ve Total arasında ilk kayıtzinciri ticareti yapıldı[xviii].

Tartışma

Kayıtzincirlerinin geleceği nasıl olacak? Bunu anlamak için benzer örneklere bakmak fikir verecektir. Müzik dinlemek için daha önce kaset sahibi olmak gerekiyorken, şimdi kasete sahip olmak yerine müziğin "dijital bir varlığa[asset]" dönüştüğü, tüketicinin emtianın sahibi olmak yerine emtianın sağladığı faydaya -müzik dinlemek- eriştiği veya erişmek istediği bir sisteme geçildi.

Amartya Sen'in Kapasite Yaklaşımına göre, insanların kapasitelerine göre emtiaları işe yarar fonksiyonlara çevirebilmeleri nihai faydayı[utility] oluşturur. Yani emtialara sahip olarak içinde bulunduğumuz durumdan

emtianın bize sağladığı fonksiyonları kapasitemize göre kullanarak amaçladığımız duruma erişmeye çalışırız[xix].

Bu noktada varlıkların dijital varlıklara dönüşmesini sağlayan teknolojiler, bizleri emtia tarafından fayda tarafına doğru yönlendirmekte ve bir verimlilik oluşturmaktadır. Yeni fonksiyonel kapasiteler sağlamaktadırlar.

Örnek olarak tüm eski CD'leri mp3 yaparak cep telefonunda saklamak yerine, bulut bir hizmetten limitsiz müzik dinleme hizmeti daha verimli olabilmektedir. Ayrıca bitler, atomlara göre daha az düzenlemeye tabidir, inovasyon daha hızlıdır.

Enerji ise çok hayati bir hizmet olmakla birlikte, enerji sektörü işlemleri hataya çok duyarlıdır. Bu işlem ve emtiaların dijitalleştirilmesi için çok çok güvenilir sistemlere ihtiyaç vardır. Dijital sistemler sonunda sayılar ve algoritmalardan ibarettir. Kayıtzinciri teknolojisi bu sayı ve algoritmalardan değiştirilmesi imkansız(geçmiş bir kayıt değiştiğinde tüm kayıt defterinin bozulduğu), dağıtık, tüm taraflarca doğrulanabilen, izlenebilen bir yöntem önermektedir.

Kayıtzinciri bu sebeple enerji sektöründe bir oyun değiştiriciden çok "mümkünleştirici" teknolojidir. Düşünsel olarak bakıldığında dağıtık üretim, tüketicinin üretici olması, merkezi elektrik üretiminin tehdit altında olması gibi yeni enerji dönemi kavramları, kayıtzincirinin düşünsel temellerine yakındır. Yani dağıtık bir enerji geleceği olacak ise bu gün ki anlamı ile kayıtzinciri olmasa da benzer bir teknolojinin olması çok büyük ihtimaldir.

Sayaçların okunması, tüketicilerin kendi aralarında elektrik ticareti, elektrikli arabalar, şebeke hizmetlerinin dağıtık verilmesi, nesnelerin internetinin enerji sistemindeki yeri, toptan satış faaliyetleri, kısaca enerjinin bir değer üretmekte kullanıldığı veya enerji hizmet ve kaynaklarının kullanıldığı her noktada kayıtzinciri teknolojileri olacaktır.

Fakat bu nasıl olacaktır? Sektör birlikler kurarak, denemeler yaparak "vurucu uygulama" (killer application)'lara dayalı iş modellerini geliştirmeye çalışmaktadır. Şu aşamada enerjide (petrol ve gaz dahil) toptan satış faaliyetleri alanında çok daha fazla uygulama görmek mümkün olacaktır. Ticaretin kolaylaştırılması ile sağlanacak fayda, zamanla nihai tüketiciye ve dağıtık enerji sistemine de sirayet edecektir.

En önemli uygulama alanı, "akıllı kontratlar" olabilir. Bunun nasıl şekilleceği merak konusudur. Mevzuatın bilgisayar kodlarını hukuki terimleri olarak görmesi nasıl olacaktır? Aynı zamanda akıllı kontrat işletiminde iki "nesnelerin interneti" cihazı arasındaki anlaşmazlığın çözüm yöntemleri neler olacaktır? Muhtemelen hukuki tartışmalar ve içtihatlar ile şekillenecektir. Fakat uluslararası tanımlarda da bir yakınlaşma olacağı kaçınılmaz görülmektedir.

İkinci nokta ise "nesnelerin interneti" uygulamalarıdır. İnsanlar kendi aralarında güveni üçüncü taraflar vasıtası ile sağlıyorlardı. Kayıtzinciri ile oluşturulan algoritmik sistem, makineler arası da bir güven protokolü oluşturabilir. Yani makineler arasında kontratlar oluşturulup, işletilip, doğrulatılan otonom bir finansal enerji işletim sistemi görülebilir. Bu da daha yüksek çözünürlükte daha fazla faydanın dijitalleştirilmesine yol açacaktır.

Tüm bir elektrik sisteminin daha fazla dağıtık ve "paylaşım ekonomisi" temelli bir noktaya gittiğini söylemek abartı olmaz. Daha fazla derken tamamen anlaşılmamalıdır. Sistem sonunda dağıtıklık ile merkeziyetçilik arasında dinamik bir dengeye gelecek ise de, o noktaya şimdilik çok uzak olduğumuzdan daha fazla dağıtık sistemleri görmemiz kaçınılmazdır.

Belkide bir elektrik piline sahip olmak, onu evimizde saklamak yerine onun sağladığı faydayı isteyebiliriz. Yani elektronik olarak rezervasyon, enerji depolama, gerektiğinde kullanma ve komşuya satabilmek veya komşunun fazla elektriğini alıp depolamaya aktarmak mümkün hale gelebilir. Bu işlemlerin hepsine imkan veren bir kağıt, kalem yöntemi çok masraflı olacaktır. Bu sebeple kayıtzincirinin şansı yüksektir.

Petrol ve doğalgazda ise nihai tüketiciye yönelik kayıtzinciri uygulamalarına rastlanılmamıştır. Bu iki emtiada da daha toptan satış ve hacime yönelik uygulamalar vardır. Sonunda bu sektörlerde dağıtıklık elektrik kadar hissedilmemektedir. Çünkü petrol ve gaz daha çok emtia, elektrik ise daha fazla fayda tarafına yakındır.

Bu sebeple kayıtzinciri teknolojilerine enerji sektöründe farklı alanlarda farklı uygulamalar ile daha fazla duymaya başlayacağız. Çünkü herkes kayıtzinciri teknolojilerinin Google'ı, Facebook'u, Twitter'ini aramaktadır.

İletişim için: barissanli2@gmail.com

i https://en.wikipedia.org/wiki/Napster

ii https://www.activism.net/cypherpunk/crypto-anarchy.html

iii https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj4xdzO3tvUAhXKKlAKHRFbDB4QFggjMAA&url=https%3A%2F%2Fwww.cosic.esat.kuleuven.be%2Fpublications%2Farticle-1532.pdf&usg=AFQjCNGaTUBq4r4IWHRmSBIPh9Kp6JFn5w

iv http://www.weidai.com/bmoney.txt

v *https://bitcoin.org/bitcoin.pdf*

vi https://en.bitcoin.it/wiki/SHA-256.

vii https://www.coursera.org/learn/cryptocurrency/lecture/eZPiF/centralization-vs-decentralization

viii https://www.coursera.org/learn/cryptocurrency/lecture/71F3l/consensus-without-identity-the-block-chain

ix https://www.coursera.org/learn/cryptocurrency/home/welcome

x http://brooklynmicrogrid.com/

xi https://innovationhub.innogy.com/news-event/2isB4LLzhKwwi4MiagAa46/blockchain-car-payments-at-ces

xii http://www.ideocolab.com/prototypes/smartsolar

xiii http://spectrum.ieee.org/energywise/energy/the-smarter-grid/will-energy-offer-the-next-market-for-blockchain

xiv https://www2.deloitte.com/us/en/pages/consulting/articles/blockchain-future-in-oil-and-gas.html

xv https://www.finextra.com/newsarticle/30350/ibm-natixis-and-trafigura-team-on-blockchain-platform-for-oil-trades

xvi http://www.lngworldnews.com/ing-socgen-to-test-lng-trading-with-blockchain-in-months/

xvii http://energyweb.org/

xviii http://www.energytradingcsee.com/blockchain

xix http://www.iep.utm.edu/sen-cap/