# Patientory: Sağlık Hizmeti, Eşler Arası Elektronik Sağlık Kaydı Depolama Ağı v1.1

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

Mayıs 2017

Bu doküman yalnızca bilgilendirme amaçlıdır. Patientory ve Patientory ile ilişkili veya bağlantılı herhangi bir şirketin hisse senetlerini veya tahvillerini satma yetkisi veren bir teklif veya talep oluşturmaz. Bu tür herhangi bir başvuru veya talep sadece mutabakat muhtırası ile ve geçerli tüm tahviller ve diğer kanunların hükümlerine uygun olarak yapılır.

Teori

Blok zinciri destekli bir sağlık bilgisi değiş tokuşu (HIE), birlikte çalışabilirlik ve siber güvenliğin gerçek değerinin kilidini açabilir. Bu sistem, nüfus sağlığı yönetimi göz önüne alındığında mevcut üçüncü şahıs arabulucuların sürtüşme ve maliyetlerini ortadan kaldırma potansiyeline sahiptir. Geliştirilmiş veri bütünlüğü, işlem maliyetlerinin düşürülmesi, merkeziyetçilikten çıkarılma ve güvenin aracısızlaştırılması vaatleri vardır. Hasta bakımı blok zinciri HIE ile koordine edilebildiğinden dolayı, blok zinciri HIE tüm HIPAA kurallarına ve standartlarına uyarken, gereksiz hizmetleri esas olarak azaltır ayrıca maliyetleri düşürerek ve süreklilik bakım döngüsü etkinliklerinin iyileştirilmesiyle testleri kopyalar. Blok zincir teknolojisi ile desteklenen hasta odaklı bir protokol olan Patientory, sağlık hizmeti alanındaki paydaşların elektronik tıbbi veriyi yönetme biçimini değiştiriyor ve klinik bakım ekipleriyle etkileşime giriyor.

## 1 Giriş

### 1.1 Blok Zinciri Nedir?

Bitcoin dijital para biriminin ardındaki teknoloji, blok zincirinin doğuşu, Sahoshi Nakamoto takma adlı, tanımlanamayan kişiye (veya gruba) kadar uzanır. 2009 yılından bu yana, bankacılık sektöründe pazara giren yeni blok zinciri destekli işletmeler ve hizmetler ile blok zinciri daha yaygın bir kullanım kazanmıştır. Blok Zinciri'nin teknolojisi, herhangi bir tek varlık tarafından kontrol edilmeden, bir iş ağı genelinde bir işlem kayıt defteri paylaşmak için kullanılır. Dağıtılan kayıt defteri, merkezi bir kontrol noktası gerektirmeden izlenebilen ve ticarete konu olan hemen hemen her şeyin bulunduğu, uygun maliyetli ticari ilişkiler kurmayı kolaylaştırır. Bu teknoloji, gizlilik ve verilerin kontrolünü bireyin eline koyar. Üçüncü taraf aracılara güvenmeden güven ve dürüstlük kurulur.

## 1.2 Mevcut Sağlık Altyapısı

"Prosedür" temelli odaklanmanın "kişinin bütünsel bakımı" olarak yeniden düzenlenmesi, sağlık uzmanlarının, bakım altındaki hastaların bakımı sonuçlarını iyileştirmek, akut sonrası bakım evreleri ya da Akut bakım evreleri araları için ortak bir hedef doğrultusunda birlikte çalışan "ağlar" oluşturmalarını gerektirir. Uzmanlar, temel bakım hekimleri, hasta bakıcıları ve sağlık uzmanları (beslenme uzmanı ve rehabilitasyon hemşireleri gibi) sağlık hizmeti sağlayıcıları arasında işbirliği ihtiyacı sayısal teknolojilerin kullanımının artmasına neden olur. Bu çözümler, sağlık hizmeti sunmak için izleme ve verimliliği önemli ölçüde geliştirmiş olsa da, öncelikle elektronik tıbbi kayıtlar (EMR) sistemleri dahilinde sağlık bilgileri siloları oluşturmaya karar verdiler.

Sağlık kurumları ve devlet kurumları, geleneksel bilgi sistemleri ve veri alışverişlerini kurmak ve yönetmek için önemli miktarda zaman ve para harcıyor; Sorunların sürekli olarak giderilmesi, alan parametrelerinin güncellenmesi, yedekleme ve kurtarma önlemleri alınması ve raporlama amacıyla bilgi çıkarılması için parasal kaynak gerektiyor.

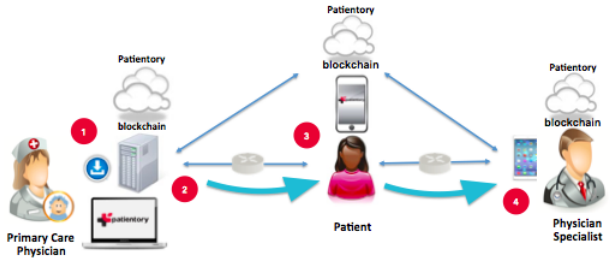
Federal kanunlar ve teşvik programları, Elektronik sağlık kaydının uygulanmasına ilişkin olumsuz tavrına tepki olarak sağlık verilerini daha erişilebilir kılmıştır. Bununla birlikte, hastane sistemlerinin büyük çoğunluğu verilerini kolayca (veya güvenle) paylaşamaz. Sonuç olarak, doktorlar aslında hastalarla konuşmaktan daha çok zamanlarını yazarak harcıyorlar. Hekim tükenmişliği 2011-2014 yılları arasında yüzde 45'den %54'e çıktı [1].

Hem klinik hem de sağlık cephesinde "bireyselleştirilmiş" sağlık bilgisi kavramı mevcut olsa da, bunlar "kişiselleştirilmiş" bakım planlarına çevrilmemiştir. Dahası, bol miktarda veri olmasına rağmen, genel sağlık ekosistemi, bir hastanın gelecekteki bakım evrelerini daha iyi tahmin etmeye yardımcı olması için büyük verilere bir değeri veya riski eklemek için yeterince mühendislik yeteneğine sahip değildir.

Dolayısıyla, Sağlık Bakımı teknolojisi endüstrisinin sürdürdüğü mevcut çözümler, hastalar için sağlık bakımı ve gizlilik / ekonomik dolandırıcılık arasında zor bir seçim yapmakla sonuçlanmıştır. Endüstri tarafından daha fazla veri oluşturulduğunda bu sorunun büyük ölçüde genişlediğini görüyoruz. **Blok zincirinin güvenli teknolojisi, özellikleri ve dağınık yapısı, bu operasyonların maliyetini ve verimliliğini düşürmeye ve uygulanabilir bir güvenlik altyapısı oluşturmaya yardımcı olabilir.**

## 1.3 Hasta-Sağlık hizmeti veren İlişkisi

Yeni sağlık yönetimi paradigması, hastalara daha iyi sağlık hizmeti sonuçları sağlamak için verimli ve optimal sağlık hizmeti gereksinimini talep eder. Bu, Başlıca sağlık hizmeti sağlayıcılarının, ilgili diğer sağlık hizmeti sağlayıcıları ve Laboratuvarlar ve Eczaneler gibi yardımcı sağlık organizasyonları ile aktif olarak koordine olabilmesini ve işbirliği yapabilmesini gerektirir. Sonuç olarak, bunun başarılı bir şekilde yapılması için hasta kayıtları zamanında güncellenmeli ve modifiye edilmelidir.



Şekil 1: Patientory Şema Şeklinde

EMR (Elektronik Sağlık Kaydı) yazılımı halihazırda etkin bir hasta-hizmet veren ilişkisini yasaklar. Hasta portalları, silolaştırılmış hasta tecrübesinin bir sonucu olarak hastalar arasında en az etkiye sahiptir. Dahası, bu yazılım bir sistemden diğerine bilgi aktarımı için sadece kısıtlı bir yeteneğe sahiptir ve genellikle bu bilgiyi aktarabilen belirli bir kişiyi gerektirir. Bu durum, sağlık hizmeti sunan kuruluşlar arasında giderek artan bir gecikmeye yol açmıştır ve ayrıca, sağlık hizmetlerinin kalitesinde genel olarak düşüşe neden olmuştur. Ayrıca sağlık hizmeti sağlayıcıları, zamanlarının çoğunu sağlık hizmetinin koordinasyonuna harcarken, hastaların tedavisinde etkinlikleri ve iş yükü önemli derecede artmıştır. Bu durum, sağlık hizmeti sonuçlarında hastalar için geleneksel kanının aksine bir etki yaratmıştır.

Buna ek olarak, birçok doktor hastaların elektronik sağlık kayıtlarına erişmesini istemediği için, hastalar kendi sağlık durumlarını izlemede pasif bir rol üstlenmektedirler. Bu durum, sonuç olarak hastalara kendi sağlık durumları üzerinde sahiplik ve kontrol eksikliği hissettiriyor; bu da hastaların sinirlenmesine ve sağlık bakımlarından ayrılmalarına yol açıyor. Son zamanlarda bireylerin hayati organlarını ve sağlık parametrelerini izlemelerine yardımcı olan mobil sağlık uygulamalarında artış olsa da, bu yenilik, elektronik sağlık kayıtlarına entegre olmanın getirdiği zorluklarla yüz yüze olduğu için, geliştirilmiş hasta bakımı veya tedaviye uyum ve sonuçlara çevrilememiştir.

## 2 Sisteme Genel Bakış

Bu güncel konular, Patientory Blok zinciri Ağını kullanılarak çözülmüştür. Eski elektronik sağlık kayıtları, hacking'e, sıkı güvenlik düzenlemelerine ve aşırı masrafa maruz kalan merkezi yapılardır. Patientory Blok Zinciri altyapısını uygulayarak, sağlık uzmanları sistemin doğal erişim kontrolü özellikleri nedeniyle minimize edilmiş ihlalleri görür; kolaylaştırılmış sağlık hizmeti koordinasyonu için olan bu kanal sağlık sonuçlarında genel iyileşme ile sonuçlanır. Yukarıda, Patientory blok zinciri altyapısının ve hastalar ile sağlık hizmeti sağlayıcıları arasındaki birlikte çalışabilirliğinin açıklandığı bir şematik çizim bulunmaktadır.

# 3 Sistemin Uygulanması

## 3.1 HIPAA Yönetmelikleri ve Uyumluluk Esasları

Uygulamalarla ilgili anlamlı bir tartışmadan önce, 1996 Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Yasası'nın (HIPAA) emirleri tarafından uygulanan kısıtlamalar ele alınmalıdır. Birincil endişe kuralları, Gizlilik Kuralı, Güvenlik Kuralı ve Bulut Bilişim Yönergeleridir. Bu yazının amacı HIPAA yasasının tam bir incelemesini yapmak değildir. Uygulamaya ilişkin unsurlar, ilgili başvuru anında tanımlanacak ve daha ayrıntılı bir şekilde tartışılacaktır.

### **A.** Gizlilik Kuralı

Patientory'nin iş modeli, özel sağlık bilgilerinin elektronik olarak saklanması ve iletilmesi nedeniyle Gizlilik Kuralının gerekliliklerine uyulmasını şart koşar. Gizlilik kuralının uygulanabilirliği, Gizlilik kuralı (Sağlık planları, sağlık hizmeti kliring odaları ve sağlık bilgilerini elektronik ortamda ileten herhangi bir sağlık hizmeti sağlayıcısına uygulanır ") olarak özetlenmiştir. [2]. Bu acentelere ek olarak, hizmet sağlayıcı olarak kendi adına hareket eden taraflar da HIPAA uyumundan sorumludurlar. Bu ikinci el aracılara İş Ortakları (BA) adı verilir ve BA'nın uyması gereken kuralları ve düzenlemeleri belirleyen yasal belge, İş Ortağı Sözleşmesi (BAC) olarak adlandırır. HIPAA, bu sözleşmelerin niteliği konusunda katı kurallar koymaktadır.

Ϛji qmps”rsp k_b_l cbglgjcl jgw_i_r lmir_j_pÏ* isjj_lÏk gxlglg* igkjgi `gjegjcpglbcl _pÏlbÏpÏjkÏ” `gjegjcpgl isjj_lÏjk_qÏ tc Ęxcj `gjegjcpgl r_lÏkj_lk_qÏlÏ _ČÏiČ_ `cjgprcl lmir_j_pbÏp, ûxcj q_·jÏi `gjegqg &cjcirpmlgi tcpg gČgl NFG tcw_ cNFG'* i_nq_l_l `gp rĞxcjjgi tcw_ g” mpr_·Ï r_p_dÏlb_l fcpf_leg `gp `gČgkbc tcw_ mpr_kb_ &cjcirpmlgi* i_·Ïr tcw_ qĘxjĞ' rsrsj_l tcw_ gjcrgjcl* `gpcwqcj mj_p_i r_lÏkj_l_`gjcl q_·jÏi `gjegjcpg mj_p_i r_lÏkj_lÏp Y0[, Igkjgi `gjegjcpglbcl _pÏlbÏpÏjkÏ” q_·jÏi `gjegqg* @gp ig”gwg r_lÏkj_k_w_l q_·jÏi `gjegqg tc `gjeglgl `gp ig”gwg r_lÏkj_k_i gČgl isjj_lÏj_`gjcac·glc gl_lk_i gČgl k_isj `gp b_w_l_i `sjslk_bÏ·Ïl_ eĘpc `gpcwqcj mj_p_i r_lÏkj_l_k_w_l q_·jÏi `gjegqg mj_p_i r_lÏkj_lk_ir_bÏp Y0[, Igkjgi `gjegjcpglbcl _pÏlbÏpÏjkÏ” tcpg isjj_lÏkÏ iÏqÏrj_k_j_pÏ ”s ”cigjbc Ęxcrjclkcircbgp8 Igkjgi `gjegjcpglbcl _pÏlbÏpÏjkÏ” q_·jÏi `gjegqglgl isjj_lÏkÏ tcw_ gd”_ cbgjkcqg imlsqslb_ fcpf_leg `gp iÏqÏrj_k_ `sjslk_k_ir_bÏp, Igkjgi `gjegjcpglbcl _pÏlbÏpÏjkÏ” q_·jÏi `gjegqg lc `gp ig”gwg r_lÏkj_p lc bc `gp ig”gwg r_lÏkj_k_i gČgl k_isj `gp rckcj q_·j_p Y1[, Kimliği saptanabilen verinin kimliği saptanamayan veriye sınırı, bir bilgi topluluğu ile ilişkilendirilen olası kişi sayısını toplam ABD nüfusunun % 0,04'ünden daha azı olarak kısıtlayan herhangi bir bilgidir.

### **B. Güvenlik Kuralı ve Bulut Bilişim Kuralları**

Bu konuyla ilişkili içeriğin uzunluğu nedeniyle, yalnızca birincil endişe unsurları referans için ayrılmıştır. Bu öncelikli endişeler şunlardır: "Kapsanan bir tüzellik, elektronik olarak korunan sağlık bilgilerini oluşturmak, almak, korumak veya iletmek (eKSB'ni işlemek ve / veya depolamak gibi) bir Bulut depolama sağlayıcısı hizmetleri işine girdiğinde, kendi adına bulut depolama sağlayıcısı HIPAA uyarınca bir iş ortağıdır. Ayrıca, bir iş ortağı elektronik olarak korunan sağlık bilgilerini kendi adına yaratmak, almak, korumak veya iletmek için bir bulut depolama sağlayıcısı ile taşeronluk yaparsa, bulut depolama sağlayıcısının kendisi bir iş ortağıdır.

Bulut depolama sağlayıcısı, yalnızca şifrelenmiş olarak korunan sağlık bilgilerini işler veya depolar ve veri için bir şifreleme anahtarı bulunmaması halinde bile bu kurallar geçerlidir. Şifreleme anahtarı eksikliği, bir bulut depolama sağlayıcısını iş ortağı statüsünden ve HIPAA Kuralları kapsamındaki yükümlülüklerden muaf tutmaz. Sonuç olarak, kapsanan tüzellik (veya iş ortağı) ve bulut depolama sağlayıcısı, HIPAA'ya uygun bir iş ortaklığı sözleşmesi (BAA) imzalamalıdır ve bulut depolama sağlayıcısı, hem BAA'nın şartlarını yerine getirmekle sözleşmeye bağlı yükümlü hem de HIPAA Kurallarının geçerli şartlarına uymakla doğrudan yükümlüdür "[3].

Kapsanmış tüzellik, daha uygun maliyeti ve daha düşük IT yönetim maliyetlerini gerekçe göstererek, sağlık bilgilerini depolamak için çoğu zaman bulut depolama sağlayıcılarını (CSP'ler) kullanır. Bununla birlikte, tüketiciler kişisel verilerini depolamak için bulut sağlayıcılarına güvendikleri için, bu veriler üzerindeki doğrudan denetimi başkalarına bırakırlar ve sonuç olarak, tüketiciler verilere kimlerin erişimi olduğunu ve verilerin coğrafi olarak nereye yerleştirildiklerinden habersizdirler. İş ortağı ve bulut depolama sağlayıcısı arasında açık bir iş ortaklığı sözleşmesi geliştirilmiş olsa bile, bir ihlalin meydana gelmesi durumunda, sadece verilerin gizliliği ve güvenliğinin sorumluluğunu kimlerin aldığı koşulları sağlanır. Tüketici, potansiyel olarak bu veri akışlarına erişimi denetleyebilir, ancak bulut depolama sağlayıcısına bu ayrıcalıkların uygulalanmasında güvenir.

Bulut depolama alanının kullanımı popüler olsa da, bir tüketici, kişisel veriler için bu mekanizmayı kullanırken üstlendiği bir takım riskler söz konusudur. Bulut tabanlı mimaride, veriler sık sık çoğaltılır ve taşınır, dolayısıyla yetkisiz veri kullanımının riskleri artar. Buna ek olarak, yöneticilere, ağ mühendislerine ve bu verileri barındıran sunucular üzerinde veya bu verilere ev sahipliği yapan sunucular için hizmet sağlayan teknik uzmanlar gibi birden çok kişiye veriye potansiyel erişime izin verilir. Bu da yetkisiz erişim ve kullanım riskini artırır.

Bununla birlikte, veriler sıkı erişim kontrolleriyle ve kaynak noktasında ve transit halindeyken şifrelenmiş olarak güvende olsa bile, Hasta Tarafından Rapor Edilen Sonuç Ölçütleri'nin (PROM'lar) geliştirilmesi için hala bir sorun teşkil etmektedir.

PROM kavramı, hastayı ilgilendiren bir alan ya da odakla ilgili hasta odaklı bir ölçüt geliştirmektir. Hastanın katılımı ve geri bildirimi PROM'un başarılı olarak uygulanması için esastır.

Nesnelerin interneti ağının bir parçası olan çeşitli cihazlardan büyük veri akışlarına erişmek, şu an kullanılan gibi bulut tabanlı hizmetler ile birlikte bir PROM'un temelini oluşturacak bir dayanak sağlayabilir, ancak bulutta silolaştırılmış verilerin, bir hasta için istenilen anlam ve uygunluk düzeyine sahip olacak bir ölçüt oluşturup oluşturmayacağını bilmek zordur.

Sistemle ilişkilendirilmiş tüm tıbbi kayıtların güvenilirliğini sağlamak ve arttırmak için blok zinciri teknolojisinin uygulanması sağlık ihlallerini ve kayıt mülkiyetinin nihai yerinden yönetimini en aza indirebilir. Veritabanına gönderildiğinde farklı algoritmalar kullanılarak verilerin şifrelenmesi ve verilerin geri getirilmesi sırasında şifre çözülmesi kullanılacaktır. Veriler, kanunen zorunlu olduğu gibi, iletim ve geri alma sırasında NIST uyumlu algoritmalar kullanılarak şifrelenecektir. Böylece, tüm bilgi değişimi, NIST spesifikasyonlarında belirtilen en iyi uygulamalara uyacaktır.

**Sağlık sektörünün karşı karşıya kaldığı hızla artan sayıda veri ihlalini ithafen, blok zinciri teknolojisi HIPAA uyumluluğunu hem hastalar hem de sağlık hizmeti sağlayıcıları için mümkün kılmaktadır.**

### C. HIPAA Kısıtlamalarına Bağlı Sınırlamaların Blok Zinciri Sistem Analizi

Ethereum Blok Zinciri, Ethereum Sanal Makinesi'nde yürütülen eksiksiz bir programlama dilinin uygulanması sayesin de çeşitli sistem uygulamalarının alt kümesini kolaylaştırır. Bu sistemlerin Oracle hizmetlerinin kullanımıyla ilgili hiçbir sınırlaması yoktur. Ayrıca, blok zincirinin depolama sınırlamaları, depolama gaz maliyeti ve bu verilere erişmek için kullanılan gaz maliyeti ile uygulanmaktadır. Bu yazının bir sonucu olarak, zincirin blok zamanı, en az on on beş saniyelik değiştirme istekleri için asgari bir sınır oluşturur.

Blok zincirinin özel bilgilere ev sahipliği yapma sınırlaması şifreleme gibi veri gizleme ile sona erebilir. Ancak şifre çözme anahtarının sızdırılmış olması durumunda, hassas verileri blok zincirinden çıkarmanın bir yolu yoktur. HIPAA uyumlu veriler maksadı ile, bu, blok zincirin kendisinin değişmez olması nedeniyle potansiyel olarak bilginin kalıcı, düzeltilemez sızıntısına neden olabilir. Kimlik bilgilerinden arındırılmış veriler, teorik olarak Halka açık Ethereum Blok Zincirinde saklanabilse de, kimlik bilgileri filtreleme mekanizmasının asla hata yapmayacağını veya blok zinciri etkileşimleriyle ile ilişkili yan bant bilgisinin kazara kimliği açığa vuramayacağını varsaymak felaket olurdu. Bu sonuca MedRec Protokollerinin oluşturulması sırasında MIT Medya Laboratuvarı tarafından da ulaşıldı ve MedRec Tanıtım Yazısı [3] 'de özetlendi. Bu yan bant bilgisini elde etmek, tarih bilgilerini ve bilinen veri depolama sözleşmeleri ile etkileşimleri gözlemlemek kadar basit olabilir.

Bu analiz sayesinde, bir kişiyi bir kurumla ilişkilendirmek ve daha da önemlisi, bir tesiste bulundukları zamanı ilişkilendirmek mümkün olabilir. Bazı tesislerin özel nitelikleri göz önünde bulundurulduğunda, pasif bir gözlemcinin kimliğini, yerini, etkileşim zamanını hem de muhtemelen tanı sınıfını ortaya çıkarabilmesinden dolayı, HIPAA uyumluluğu ihlali teşkil etmek için yeterince bilgi vardır.

Bu konumun doğası gereği ücra olması bekleniyorsa, ABD nüfusunun% 0.04'ünden daha aza bir azalma önemsiz hale gelir. Bu gerçekler, kabul edilmesi gereken mantıksız tek nokta hataları oluşturmaktadır. Ayrıca, şifreli bilgilerin bile blok zincirinde doğrudan depolanması, HIPAA veri depolama tesisi olarak yaptıkları eylemlerinden dolayı veritabanı yöneticilerinin bir iş ortaklığı anlaşmasına (BAC) girme sorumluluğunu doğurmaktadır (Bkz. Güvenlik Kuralı ve Bulut Bilişim Yönergeleri başlıklı bölüm). Her madenciğin ve hatta pasif düğüm noktaları barındıran kişilerin HIPAA'ya uyması gerektiği için bu makul olmayan bir beklentidir. Her madencinin ve hatta pasif düğüm noktaları barındıran kişilerin HIPAA uyumlu olma gerekliliği mantıksız bir beklentidir. Bu endişelerden ötürü, Ethereum tabanlı blok zincirinin özel bir uygulamasını kullanarak hassas bilginin kalıcı olarak depolanması için bir mekanizma uyguluyoruz.

### D. Kullanılabilirlik ve Güvenlik için Uygulama Hedefleri

Herhangi bir güvenli sistemin birincil hedefleri, doğrulama, bütünlük, kullanılabilirlik, hesap verebilirlik ve bilgi / kimlik güvencesi olarak özetlenebilir. Bu hedefleri karşılamak için bir saldırgan ve kullanıcı tanımlanmalıdır. Bu rollerden her biri belirli yetenek teyitleri ister. Kullanıcının bakış açısından, sistem, ileri bilgiye ihtiyaç duyulmadan yeterince şeffaf olması gerekir. Ayrıca, normal kullanıcının siber güvenliğin karmaşık hususlarını kavrama konusunda yetersizliği nedeniyle, sürecin kullanıcı eylemlerine karşı dirençli olmalıdır.

Saldırı meydana gelmesi durumunda, bir kaynaktan ödün vermek için yatırım yapılması gereken miktar, kaynağın değerinden daha fazla olacak şekilde sistem oluşturulur. Bunun nedeni, uygun kaynaklara sahip ve yeterince gelişmiş bir tarafın, yeterli zaman ve çaba ile, herhangi bir sistemi her zaman ihlal edebileceğinin farkına varılmasıdır. İşin özü, mükemmel bir savunma yoktur. Bu kısıtlamaları göz önünde bulundurarak, daha önce bahsedilen tüm hedeflere ulaşmamız için uygulanmanın kendisi tartışılacaktır.

## 3.2 Donanım ve Ağ Uygulamasının Tanımı

Yukarıda belirtilen tasarım hedeflerini karşılamak için, seçilen sistem uygulaması birkaç bağımsız sistemi gerektirir. Her sistem otoriteyi alt bölümlere ayırır, yalnızca yetkili kuruluşların onaylı bir şekilde etkileşime girmesini sağlar ve kullanılabilirliği sağlarken güvenliği artırmak için bir mekanizma sağlar. Bu sistem ayrıca öyle tasarlanmıştır ki ölçeklendirme hiyerarşik çağrı şemaları eklenerek kolaylıkla gerçekleştirilebilir. Bu sistemler aşağıda detaylı bir şekilde açıklanmaktadır.

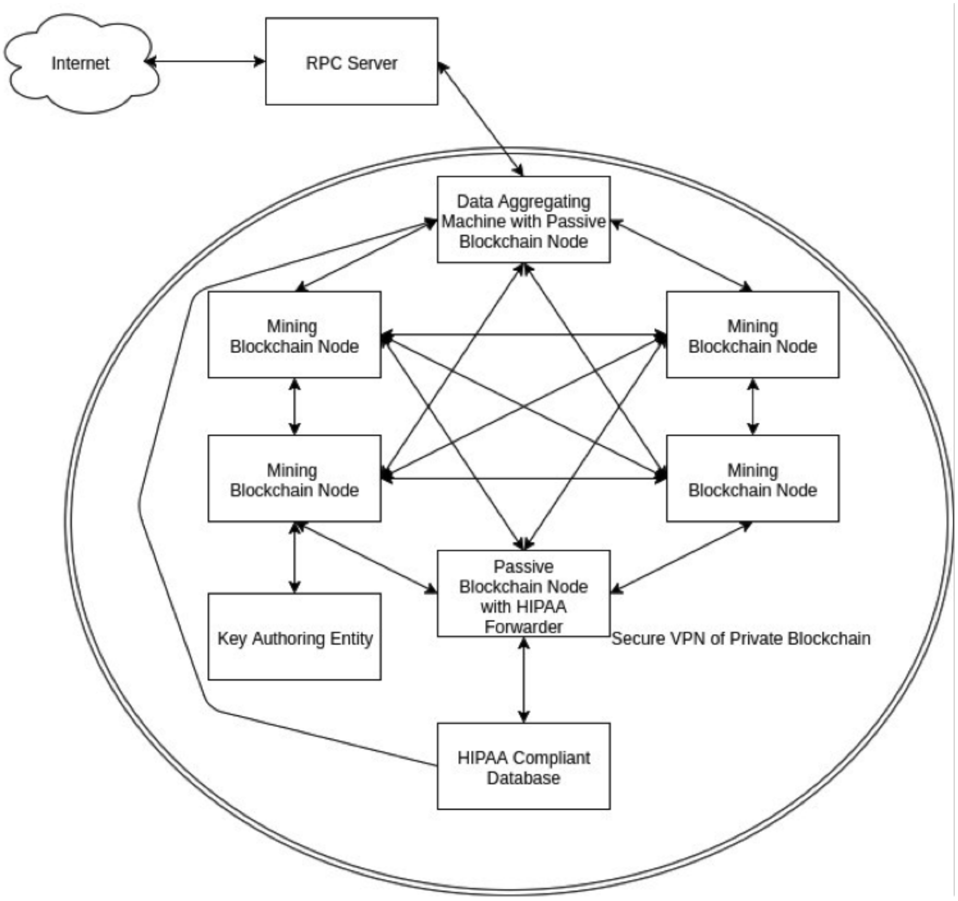
Halka açık tüzellik, Ethereum Blok Zinciri'nin özel bir uygulamasına (izni verilen blok zincirine) arabirim görevi gören bir Uzaktan Yordam Çağrısı (RPC) sunucusudur. Bu blok zinciri düğümleri ağı, sadece diğer blok zinciri düğümleri, anahtar yaratma varlığı, HIPAA uyumlu depolama tesisi ve RPC Sunucusu ile etkileşime girme yetkisine sahiptir. Anahtar yaratma varlığı, blok zincirinde kullanılmak üzere özel / halka açık anahtar çiftleri üreten kaynaktır. HIPAA uyumlu depolama tesisi, elektronik özel sağlık bilgilerini (ePHI) oluşturan gerçek verileri barındırır.

Veri için bir talep oluştuğunda, HIPAA'ya uyumlu sistem, veriyi daha sonra RPC sunucusuna yeniden yönlendiren yönlendirme aracıyla konuşma yetkisine sahip olabilir. Alternatif olarak, HIPAA depolama birimi doğrudan RPC sunucusuna konuşacak şekilde yapılandırılabilir. Her uygulamanın, nihai seçimden önce dikkate alınması gereken faydaları vardır. Her iki durumda da, HIPAA depolama tesisi, talep işleme üzerine veritabanının ilgili bölümlerinin şifresini çözer. Daha sonra bu şifresi çözülen bilgiler, talep eden tarafın halka açık anahtarı kullanılarak gönderim için yeniden şifrelenir. Ayrıca, bu halka açık anahtar, blok zincirinden HIPAA verilerine kontrol arabirimi olarak görev yapan sözleşmenin de halka açık anahtarıdır.

Belirtilenen ağ topolojisinin diyagramı şekil 2'de görülebilir.

## 3.3 Yazılım Uygulamasının Tanımı

Donanım ve ağ uygulamalarındaki sistemlerin fiziksel izolasyonuna ek olarak yazılım erişim kontrolü, verilerin bütünlüğünü ve talep eden tüzelliklerin



Şekil 2: Patientory Blok Zinciri Ağ Topografyası

yetkisinin doğrulanmasını kolaylaştırır. Erişim kontrolü ve veri şifreleme açısından yazılım sistemi aşağıda açıklanmaktadır.

HIPAA uyumlu veritabanı yalnızca HIPAA ileticisinden gelen bağlantıları kabul edecektir. Bu, trafiğin akışının bilinen kontrollü yollara izole edilmesini sağlar. HIPAA ileticisi sadece blok zincirinde geçerli bir işlem gerçekleşene kadar HIPAA depolama tesisine bir talebi iletmek için harekete geçecek ve bu işlem talep edilen olayın gerçekleşmesi ile sonuçlanacak. Bu talep eden etkinlik, talep eden tarafın halka açık anahtarını ve bu veri alanlarının talep edilmesini içermelidir. Son olarak, RPC sunucusu, yalnızca bilinen kullanıcıların sunucuyla etkileşime girebileceği şekilde bir erişim denetimli Uygulama programı arabirimi (API) kullanır.

Sistemin çağrı hiyerarşisini anlamak için, öncelikle erişim kontrolünü kolaylaştıran sözleşme yapısı ele alınmalıdır. Sistemdeki her kullanıcı, özel blok zincirindeki özel bir adrese eşleştirir. Her özel adres blok zincirindeki sadece BİR sözleşme ile doğrudan görüşme yetkisine sahiptir. Bu sözleşme, kişinin sınıf sözleşmesidir. Kurumlar, kurum çalışanları ve müşteriler sınıf düzeyinde nesnelerdir.

Bu sınıf düzeyindeki nesneler, izin tabanlı arabirimlerdir. Kurum Sözleşmesi, kuruma görüntüleme ayrıcalıkları tanıyan tüm müşterilerin bir listesine sahiptir ve Her müşteri sözleşmesi, kurumların sahip olduğu sözleşmeye verilmiş izni olan, kullanıcıdan kuruma herhangi bir izin iptalini kolaylaştıran işlevlere sahip olan tüm kurumların bir listesine sahiptir. Kurum sözleşmesi bu listeyi kendisi değiştiremez, böylece kişilerin kayıtlarına yetkisiz erişimi önler. Buna ek olarak, Kurum Sözleşmesi, yetkili çalışanların tamamen korunabilir bir listesine sahiptir. Bu izin şeması, bir kurumun yanlışlıkla eski çalışanlarının erişim haklarını korumaktan kaçınması için, bir iznin otomatik olarak iptal edilmesinin yarı-düzenli aralıklarla gerçekleştirileceği şekilde çalışmalıdır.

Bu sistem içinde, tüm harici taraflar, talep eden çağrıyı kodlayan imzalı işlemlerin ibrazı yoluyla etkileşime girer. Bu işlemler, kullanıcı doğrulaması üzerine RPC sunucusu aracılığıyla gönderilir. RPC sunucusu, bu istekleri veri toplama sunucusuna gönderir, veri toplama sunucusu daha sonra bu istekleri bir yük paylaşım mekanizmasına dayalı madencilere iletir. Madenciler daha sonra, işlemi, talep eden taraf adına, tarafın kendi kontrol sözleşmesine ibraz ederek işleme koymaktadır. Bu sözleşme, tüzelliğin sözleşmenin dahili erişimi için yetkili olduğuna dair veri izinlerini tutar. Bu sözleşme, dış talepten gelen bir işlemi kabul eden tek tüzelliktir. böylece, blok zincirindeki çağrı işlemlerini tamamen kontrol etmek için bir mekanizma kurulmuştur.

Herhangi bir işlem için, çağıran tarafın değişmez bir kaydı oluşturulur. Bu, bilgiye erişmek üzere yapılan her girişimin kaydedilmesini sağlar. Kullanıcı sözleşmesinde depolanan gerçek veriler, HIPAA depolama sunucusu tarafından çözüldüğünde uygun verilerin geri gönderilmesiyle sonuçlanan bir komut işaretçileri sistemidir. Bu bilgi, geçerli bir istek işleminin uygulanmasıyla HIPAA ileticisine kabarcıklanır. Bu iletişimi kolaylaştıran mekanizma dolaylıdır ve blok zinciri olay mesajlaşma sistemi vasıtasıyla kendini gösterir.

İstek sahibinin veritabanını sadece geçerli işlemle sorgulayabilmesi ve kullanıcının kendi bilgilerini doğrudan değiştiremeyebileceği sınırlamasından dolayı, erişim denetimi kanıtlanabilir. Kurumların bakış açısından, veri talep edebileceği kullanıcıların bir listesini ve çalışanlar olarak bu kurumla etkileşim kurabilecek kullanıcıların bir listesini barındıran kurum sözleşmesi dışındaki mekanizmalar benzerdir. Bir talep işlemi, bir kurum çalışanının sözleşmesinden kaynaklandığında, kontrol sözleşmesi, kullanıcı sözleşmesini ePHI'yi çözen veri işaretçilerini istemek üzere çağıran kurum sözleşmesini çağırır. Sözleşme, kullanıcı için onaylanmış kurumlar listesinde bekleyen kurum için uygun komut işaretçilerini döndürür. Bu işaretçiler daha sonra yine HIPAA depolama tesisine kabarcıklanan bir olay mesajı olarak yayınlanır.

**Daha açık bir şekilde, tek bir isteğin tüm süreci şu şekildedir: Harici taraf, blok zincirine gönderilmek üzere, kriptografik olarak imzalanmış bir işlemle RPC sunucusunu çağırarak servisten veri talep eder. RPC sunucusu, bir oturum açma isteğinin imzasıyla harici tarafın kimliğini doğrular.**

İzin verilen halka açık anahtarların veri tabanındaki bir girdi imza eşleşmelerini beklerken, RPC sunucusu isteği kabul eder ve Veri Toplama Makinesine ibraz eder. Ardından, Veri Toplama Makinesi istekleri özel blok zinciri doğrulayıcılarına gönderir. Doğrulayıcılar,talebi, bir blok zinciri hesabından bir hedef sözleşmeye karşı bir çağrı olarak alırlar. Doğrulayıcılar bu çağrıyı yerine getirir ve isteğin izin verilebilir bir eylem olması durumunda, işlem bir sonraki bloğa girilir. Bu işlem aynı zamanda blok zincirinde bir olay iletisinin yayınlanmasına neden olur. Bu olay iletisi, olay iletisinin komutları temel alınarak HIPAA depolama alanına karşı şifrelenmiş bir talep oluşturan HIPAA İleticisi tarafından gözlemlenir. Bu ileti ayrıca talep eden tarafın halka açık anahtarını da içerir. HIPAA uyumlu veritabanı sistemi, bu talebi gözlemler ve bilginin şifrelenmiş bir kopyasını, istekte bulunan tarafın halka açık anahtarını kullanarak RPC sunucusuna iletir. RPC sunucusu, daha sonra bu bilgiyi, istekte bulunan IP'yi, iletideki halka açık anahtara yeniden eşleyerek istekte bulunan kişiye geri döndürür. RPC sunucusu, bu iletiyi altta yatan verileri hiç görmeden iletir. Bu veriler daha sonra RPC sunucusu tarafından derhal kullanılmaz hale getirilir, böylece RPC sunucusunun HIPAA uyumlu olmasına gerek olmayan bir kanal görevi görmesini sağlanır.

Verileri yayınlama mekanizması yine benzer niteliktedir, ancak gönderilecek veriler HIPAA depolama tesisinin halka açık anahtarı ile şifrelenir. Olay iletisi sistemi aracılığıyla kabarcıklananarak gönderilen veriler dışındaki diğer işlemler aynıdır. Böylece, düşük çatışmalı karma fonksiyonları ve zaman damgalı işaretler kullanılmasından dolayı, gönderilen verinin HIPAA depolama tesisinde bulunduğu adresi hesaplayabilen sözleşme ile veri depolanabilir.

Son olarak, özel anahtarların tüzelliklere dağıtımı ele alınmalıdır. Bu akıllı telefon kullanıcıları için optik araçlarla kolaylaştırılabilir. Bu, Ethereum adresleri için QR kodlarının adres olarak kullanılmasıyla benzerdir. Hem masaüstü bilgisayarlarda hem de tablet / akıllı telefon aygıtlarındaki uygulamalar kullanılarak alternatif araçlar kurulabilir. Bir kontrol sözleşmesinin erişim kontrolünü yönetici olarak bir anahtardan kaldırma ve başka bir anahtara verme becerisinden dolayı bir anahtarın kaybı felaket değildir.

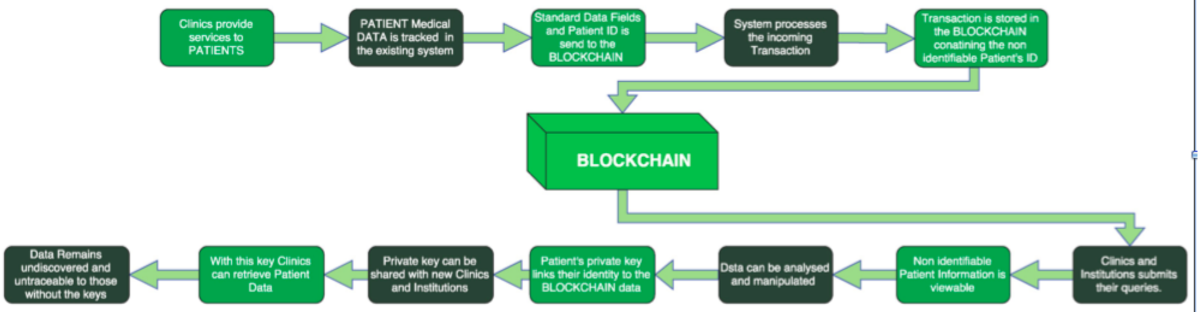
## 3.4 Birlikte çalışabilirlik

EHR sistemleri, hasta verilerinin ayrı sistemlerin her birinde tutulduğu izole bir kimlik doğrulama doğrulama mimarisine dayanır. Bu, diğer sağlık uzmanları ve yardımcı sağlık kuruluşları arasında sağlık hizmeti koordinasyonunu sağlamak için bu sistemlere bire bir sağlık hizmeti koordinasyon yazılımı "eklentiler" çözümleri getirdi. Ancak, ana Sağlayıcı organizasyonundan diğer organizasyonlara bilgiye erişim, yalnızca Okumak, İbraz etmek, Göndermek veya Bildirmek gibi durumlarda sınırlı kapasitedir. Dahası, Hasta / Tüketici, bu bilgi alışverişinde çok sınırlı etkileşim ya da katılıma sahiptir. Buna ek olarak, mevcut veri alışveriş mekanizmalarının bir dezavantajı, ibraz işlemi sırasında oluşan hataların giderilmesindeki zorluktur.

Blok zinciri ve onun akıllı sözleşmeleri bir kere yapılandırıldıktan sonra, parametreler mutlak hale gelir. Hasta, herhangi bir yazılımın sık güncelleme ve sorunlarının giderilmesi gereksinimini çürüterek, sağlık bilgisi gönderme ve alma konusunda birincil aracı olur. Ayrıca blok zinciri kayıtları değişmez olduğundan ve katılan tüm kullanıcılar arasında depolandığından, kurtarma ihtimalleri gereksizdir. Dahası, blok zincirin şeffaf bilgi yapısı birçok veri alışverişi entegrasyon noktalarını ve zaman alan raporlama faaliyetlerini ortadan kaldırabilir.

## 3.5 Süreçler ve Ölçeklenebilirlik

Kullanıcılar, eksiksiz, tutarlı, zamanında, doğru ve yaygın olan ve böylece dayanıklı ve güvenilir hale gelen yüksek kalitede veri sağlayan tüm bilgilerinin ve transferlerinin kontrolüne sahiptir. Merkezi olmayan veri tabanı nedeniyle, blok zinciri merkezi bir başarısızlık noktasına sahip değildir ve kötü niyetli saldırılara karşı daha dayanıklıdır.



Şekil 3: Blok Zinciri Süreç Akışı Diyagramı

Herhangi bir Sağlık hizmeti ağı içinde, birlikte çalışan katılımcıların, onlardan beklenen gerekli hizmetleri sunmaları için birbirlerine güvenebilmelerini sağlamak gerekir. Bunu başarmak için, zamanında teslim edilmesi beklenen görev ve hizmetlerin hesap verebilirliğini sağlamak ve beklenen kalite düzeyinde zamanında teslim edilmemesi durumunda ilgili sorumluluğu sağlamak için bir araç olmak zorundadır. Bu nedenle, herhangi bir Sağlık Altyapısı, Ana Sağlık Hizmeti Sağlayıcının Sağlık hizmeti ağını değerlendirebilmesi için gerekli bilgiyi sorunsuz bir şekilde izleyebilmelidir. Dahası, Sağlık hizmeti ağı büyüdükçe ve ağ sağlık hizmeti sağlayıcıları arasındaki bu etkileşim arttıkça Sağlık Altyapısı bu ölçeğe etkili bir şekilde hitap edebilecek nitelikte olmalıdır.

Oldukça ölçeklendirilebilir ve dağıtılmış bir Sağlık Hizmeti Yönetim sistemi oluşturmak için kilit nokta, eşler arası mimari bir sistemdir. Böyle bir sistem, medya, spor, emlak, tedarik zinciri gibi bazı endüstri bölümlerinde kullanılmaktadır, bu, blok zincirinin, kolayca mevcut merkezileştirilmiş sistemlere bir eklenti yazılım bağlayıcısı olabileceğini göstermektedir[7]. Bu, blok zinciri sistemi kullanımını, sağlık hizmeti için eşler arası bir sistemin etkinleştirilmesinde uygulanabilir olduğu için keşfetmemize yol açtı.

Blok zinciri, bir "sağlık hizmeti işlemi" yapan iki veya daha fazla tüzelliğin geçerliliğini onaylama sözünü tutar. Bu, merkezi bir kimlik doğrulama modeli ile karşılaştırıldığında iki temel özellik sağlar. Birincisi, ilgili tarafların, "işlem seviyesinde" bir "güven ilişkisi" ile birbirleriyle etkileşime girebilmeleridir. İkincisi, böyle bir ilişkide sorumluluk maruziyetinin sadece "işlem seviyesi" ile sınırlı olmasıdır. Bu taraflar arasındaki bilgi ve yükümlülüklerin erişimini sınırladığı ve aynı zamanda, bir tarafın, sağlayıcıların özel kabiliyetlerine ve hastalara sunulacak bakım hizmetinin türüne göre bir dizi başka sağlayıcılarla işlem ilişkisine girmesine olanak sağladığı için, çok yararlıdır. Bu, erişim ve yükümlülükleri yönetmek için gerekli olan çaba nedeniyle geniş çapta hasta ihtiyaçları sağlayıcılarının sayısını sınırlamaya ihtiyaç duyan geleneksel merkezileştirilmiş sistemlerden çok daha iyidir.

## 3.6 Sağlık Bilgisi Alışverişi ve Token

Patientory tokeni (PTOY), blok zinciri altyapısını sürdürmek için yakıttır. Tokenin birincil kullanımı, ağ depolama dağılımını, sağlık kalitesi önlemlerini ve gelir ödeme döngülerini düzenlemektir.

Hastalara Patientory ağı üzerinde ücretsiz olarak bilgi depolamak için tahsis edilmiş bir miktar alan verilir. PTOY, hastane sistemlerinde kurulmuş düğümlerden ekstra depolama alanı satın almalarını sağlar. PTOY, platform veya bir borsa aracılığıyla satın alınabilir.

Sağlık kuruluşları da bu durumda PTOY kullanmaktadır. Ayrıca akıllı sözleşmeler sağlık sigortası şirketleri tarafından icra edildiğinde ve değer bazlı model metriklerini düzenlemek için bir mekanizma görevi gördüğünde PTOY ödemelerde de kullanılır.

ABD'nin hizmet ücreti modelinden mevcut değer temelli modele başarılı bir şekilde geçmesi için kuruluşların tıbbi müdahalelerin kalitesini, değerini ve etkinliğini saygın bir ücret modeli ile birleştirmesine olanak tanıyan bir sağlık hizmeti IT altyapısı olmalıdır.

Ücret, bakım ve sağlıklı yaşam kalitesinin iyileştirilmesini sağlamak için birlikte çalışan sağlık hizmet sağlayıcıları ağının ne kadar etkili olduğuna ve aynı zamanda ilişkili bakım maliyetinin azaltılmasına dayanacaktır. Ağdaki farklı katılımcıları gerçekten daha iyi bakım sistemleri üretmeye teşvik etmek için paylaşılan tasarrufların liyakata dayalı bir ücreti (Geri ödemeler) gerekir. Ağ üzerindeki toplam tasarruflara en çok katkıda bulunan sağlayıcıya, orantılı bir payı etkin bir şekilde tahsis etmek için blok zinciri üzerindeki akıllı sözleşmelerle gerçekleştirilen katkılarının net bir şekilde izlenebilmesi ölçülebilir.

Yeni sağlık hizmeti paradigmasının bir diğer kilit etkisi, sağlık uzmanlarının verilen bakımın ötesinde ilave ücret almak için uygun olduğu ücret modelidir. Bu ücret, sağlık uzmanlarının hastanın sağlık sonuçlarının bakımını ne kadar etkin bir şekilde yönettiklerine bağlı olarak üretilen tasarrufların sonucudur (teşvikler). Hastanın bakımının verimli bir şekilde yönetilmesi yoluyla sağlanan tasarruflar, sağlık hizmeti sağlayıcıları ve ağ ortakları tarafından yeni sağlık paradigmasının paylaşılan tasarruflar özelliğinin bir parçası olarak muhafaza edilebilir.

Teklifimiz, ödeme yapanların, bu kalite metriklerine ulaşan sağlık hizmeti sağlayıcılarına teşvik olarak token aktarmalarına olanak sağlar. Faydaların önemli ölçüde kolaylıkla itfa edilebildiği akıllı sözleşmeleri sorunsuz bir şekilde takip etme ve yönetme olanağı, sağlık hizmeti sağlayıcıları ve hastalar için aktif bir şekilde simbiyotik bir işbirliği yapmaları için gerekli "havuç" sağlar. Buna karşın, bir veya daha fazla katılımcı uygun cezaları hafifletirse yükümlülükler yoluyla benzer kolaylıkla cezalandırılabilir. Bu "havuç / sopa" yaklaşımı, sağlık sektörünü bir hastalık yönetimi zihniyetinden sağlıklı yaşam tarzı zihniyetine kaydırmak için gereken itme gücünü sağlayacaktır.

Şimdiye kadar, Patientory, Patientory platformunun yerli tokeni olan tokenleri (PTOY) piyasaya çıkardı. Kullanıcılar, PTOY tokenleri karşılığında, sağlık bilgisi depolama alanı kiralamak, sağlıkla ilgili akıllı sözleşme ödemeleri ve işlemleri gerçekleştirmek için ağı kullanabilecekler.

Muhtemel yakın gelecekte bu altyapıyı desteklemek için en iyi ödeme sisteminin token kullanımı olduğuna inanıyoruz. Sağlık hizmeti kapalı döngü bir ödeme sistemi gerektireceği için gelecekte pek çok tokenin canlı bir ekosistemi var olacak. Sonuç, şu anda sağlık hizmeti ödeme sistemine atfedilen milyarlarca dolarlık dolandırıcılıkta önemli azalma ile verimli bir bakım döngüsü yönetimi olumlu geri dönüş döngüsü olacaktır [4].

Sistem ayrıca geniş bir sunucu depolama alanına sahip olan bu büyük organizasyonları, doğrudan bir düğüm uygulamaya gerek duymadan blok zinciri sağlık ağına doğrudan erişim ihtiyacı duyacak küçük ila orta büyüklükte sağlık kuruluşları ile token ticareti yapmaya teşvik eder. Yeni sağlık politikaları, sağlık hizmeti sağlayıcılarını, bakım yollarını iyileştirmek için birlikte çalışmaya teşvik etme potansiyeline sahip olsa da, mevcut EHR mimarileri bu kabiliyeti sağlamakta yetersiz kalırlar, dolayısıyla basitçe hibe edilen veya verilen tokenler bu işlemi kolaylaştırır. Bu nedenle, tokenlerin değeri, ağda yürütülen işlem hacmine bağlıdır. Patientory ağının token işlemleri sürekli olarak arttıkça, token talebi artmakta ve böylece değer artmaktadır.

Şekil 4: İşlemlerin bir Fonksiyonu olarak Patientory Token değeri

## 3.7 Token Edinimi

PTOY, Patientory'nin yerli uygulaması, kripto para marketleri ve başka bir hasta, hekim veya sigortacılardan transfer yoluyla edinilebilir. Platform kullanıcısı, ön satış sırasında blok zincirindeki PTOY oluşturma sözleşmesine Ether ("ETH") göndererek PTOY edinme olanağına sahip olacaktır. Patientory arayüzü, ETH kullanmayan kullanıcılar için Shapeshift ve Coinbase gibi üçüncü parti ticaret çözümlerini entegre edecektir.

İlk Patientory Token dağıtımı ön satış şeklinde olacaktır. Herkes, token satışı akıllı sözleşmesine ETH rehin vererek bir indirim oranı ile PTOY elde edebilecektir. ETC veya BTC gibi diğer kripto para birimlerine sahip olanlar, ön satış sayfasında bulunacak bir üçüncü taraf dönüşüm hizmeti yoluyla PTOY oluşturabilir.

Kurucu ekip, on iki aylık bir tutma süresine tabi tutulan, PTOY tahsisinin % 10'luk kısmını alacaktır. Bu tokenler, Patientory kurucu ekibi için uzun vadeli teşvik görevi görür. Ek bir %20 blok zinciri teknolojisinin sağlık hizmetinde kullanım vakaları ile ilgili araştırma ve geliştirme için kullanılmak üzere Patientory Vakfı fonuna tahsis edilecektir.

## 3.8 Akıllı Sözleşmeler ve Sigorta Talebi İşleme

### A. Otomatik hüküm

Tıbbi faturalandırma ve hastalar için üçüncü taraf harcamalarını karşılama süreçlerinin karmaşıklığı, çoğunlukla hasta, sağlık hizmeti veren ve sigortacı arasında karışıklığa ya da yanlış anlaşılmaya neden olur. Bu komplikasyonlar, bazı tüketicilerin bir tıbbi fatura için ne zaman, kime veya ne miktarda borçlu olduklarından habersiz olmalarına veya ödemenin sorumluluğunun kendilerine mi veya sigortacı ya mı ait olup olmadığını bilmemelerini neden oluyor.

Patientory, verimlilikleri artırmak, gerçek zamanlı hak talebine olanak sağlamak, paydaşlar arasında şeffaf sözleşmeler sağlamak ve sahtekarlığı azaltmak için hem Ethereum blok zinciri teknolojileri hem de Hızlı Sağlık Hizmeti Birlikte Çalışılabilirlik Kaynakları (FHIR) uyumlu uygulama programı arabirimlerinden (API'ler) yararlanılarak tasarlanmış bir platformdur.

FHIR, eski sağlık hizmeti ve sigorta sistemleri için entegrasyon karmaşıklığını azaltarak verileri biçimlendiren bir endüstri standardı olarak yaratılmıştır. Çözümümüzün kilit bir özelliği, blok zincirine veri ekleme maliyeti nedeniyle, söz konusu verilerin yalnızca akıllı sözleşmelerin yürütülmesi için gerekli olanla sınırlandırılmasıdır.

2018'de 315 Milyar ABD Dolarına ulaşması beklenen Fatura ve Sigorta ile ilgili masraflar ve her hafta 3.8 saat'i ödeme yapanlarla etkileşimde bulunarak harcayan tıbbi bürolara karşın platformumuz bu operasyonel maliyetleri önemli oranda azaltabilir.

Teşhisle ilgili bilgi için çapraz korelasyon analizi elde etmek üzere kullanılabilen yöntemler, hileli faaliyet için talep verisini analiz etmek üzere de kullanılabilir. Bu analiz, birden fazla talebin bulunması nedeniyle ilaç arama davranışı gibi eylemleri de ortaya çıkarabilir. Bu kullanım örneklerinin her ikisi de, bu sistemin sigorta şirketleri tarafından kullanılması için değer önermeleri ekler, ancak nihai fayda bu bilginin ötesindedir.

Akıllı sözleşme sistemi tarafından zorlanan kural tabanlı sistem nedeniyle, tüm sigorta kapsamı anlaşmaları son kullanıcılara atıf yapılan akıllı sözleşmelere kodlanabilmektedir. Bu, tıbbi bir tesisin, hizmet sunumundan önce sigorta kapsamı alanının varlığını doğrulaması için sistemi sorgulamasına izin verir. Sistemin maliyet bilgilerine ev sahipliği yapmak için kullanımı, kurumlar ve şahıslar arasında token tabanlı borç olarak otomatik fatura vermeye de olanak tanır. Böylece, bir kurum ve bir birey, maruz kaldıkça maliyetler konusunda kolayca bilgili olabilir. Bu, muhasebe departmanlarından gelen iş yükünü ve böylece sistemin benimsenmesi için ek bir değeri ortadan kaldırır.

**Bu nedenle, Patientory kapalı devre ödeme sistemidir. Çapraz zincir bağlantısının bile, halka açık Ethereum Blok Zinciri sayesinde güvenli bir değer değişimine izin verebileceği umuluyor. Bu mekanizma, güvenilir bir tüzelliğin bir Oracle gibi hareket etmesini gerektirmesine rağmen Bitcoin işlemlerinin arabuluculuğu için çoktan çözüldü.**

### B. Uygulanabilirlik

Mevcut mekanizmalar kullanılarak bu mimari kolayca oluşturulabilir. Böyle bir örnek, Amazon Web Service'in HIPAA uyumlu veri depolama sisteminin kolaylıkla konuşlandırılabilir ErisDB'ye bağlanması olabilir. Bu SAAS(Hizmet olarak yazılım), yukarıda belirtilenler gibi tam izinli erişim denetimleri olan Ethereum akıllı sözleşmeli bir blok zincirinin hızlı bir şekilde kurulmasını sağlar. İlave pasif düğümlerin kurulması gerekecek, ancak bu bütün mimarinin geliştirilmesine kıyasla minimal bir geliştirme maliyetidir.

Patientory'nin üç katmanlı Akıllı Sözleşme mimarisi ile, akıllı bir sözleşmenin özelliklerinden yalnızca bir alt küme Ethereum blok zincirinde uygulanır. Karmaşık iş mantığı, uygulama yolundan kaldırılır; bu, veri katmanının, ağın dağıtılmış niteliğini yansıtacak şekilde optimize edilmesini sağlar.

Ethereum blok zincirinde uygulanan akıllı sözleşme paketinin bileşenleri: veritabanı şeması, blok zincirine eklenen işlemlerin onaylanması ve doğrulanması ve zinciri okumak için sorgu optimizasyon mantığıdır.

İş mantığı Ethereum blok zincirinin üstünde ayrı bir orta (iş) katmana çekilir. Bu mantık kodu, Patientory'nin çeşitli sağlık konsorsiyumlarına bağlanmasını ve konsorsiyumlarda rol almasına izin veren güvenli yürütme, tasdik, kimlik, kriptografik destek, veri biçimlendirme, güvenilir mesajlaşma, tetikleyiciler ve bu kodu herhangi bir sayıda blok zinciri üzerindeki belirli akıllı sözleşmelerde şemaya bağlama yeteneği de dahil olmak üzere çeşitli servislere erişir. Bu hizmetler akıllı sözleşmeleri destekleyen bağımsız kod parçalarının, yürütülebildiği, blok zinciri düğümlerine işlem gönderebildiği ve veri katmanındaki şemaya bağlı olabileceği bir sistemde sağlanır.

## 3.9 Ek Benzersiz Faydalar

Bu düşünceyle, acil durumlarda yanıt vermeyen bir kişinin kayıtlarına erişmek için bir tıbbi tesis olması ihtiyacı, kullanıcı tarafından daha önce bu erişimi yetkilendirdiği takdirde imtiyaz artışından yararlanacak bir durum teşkil etmektedir. Bir kişinin yanıt vermemesi ve cep telefonunun bulunması durumunda, kurum, bir akıllı telefonun kilit ekranından edinilebilen ikincil imza yöntemini kullanarak bir kişinin cihaza sahip olduğunu ispatlayabilir. Bu ikinci anahtar, birincil hesapla aynı özel anahtar olmamalıdır. Böylece, bir kurum, blok zincirine bir kişinin halka açık anahtarı ve söz konusu kişinin acil durum imzası gönderdiği akıllı telefonu bulunduran bir istekte bulunursa, Blok zinciri, aksi halde erişilemeyecek tıbbi kayıtlara erişimi izin vermek için ayrıcalığı artırabilir. **Bu özel anahtar yakılabilir olmalı ve mümkün olan en kısa sürede birey tarafından değiştirilebilmelidir. Bu şekilde, bir şahıs ile yetkili bir kurum arasında güvenli bilgi alışverişi acil durumlarda kolaylaştırılabilir.**

Bir kurum uygun izni olmadan bu bilgiyi talep ederse, kişi eylemlerin farkına varır. Kişi bu isteği bir eşik aralığı zarfında reddederse, veriler paylaşılmaz. Ayrıca, bir kurum çok sayıda hileli istekte bulunmaya kalkarsa, kurum, imtiyazın iptali, para cezası ve / veya yasal işlemler yoluyla cezalandırılabilir. Cep telefonunun kaybedilmesiyle oluşan hasar hem cep telefonu hem de kurum seviyesi anahtarı gereğinden dolayı azdır. Öngörülebilir bir gelecekte, tüm sigorta kartları, akıllı bir telefondan bağımsız olarak aynı işlemi kolaylaştıracak, modern kredi kartlarının sahip olduğu gibi şifreleme mikro denetleyicileri ile gömülebilir.

# 4 Ulusal / Uluslararası Sağlık Hizmeti Öncelikleri

## 4.1 Kişiselleştirilmiş Bakım

Etkili üstün bakıma ulaşmak için, kişi odaklı bir yaklaşım önemlidir. Böyle bir yaklaşım, sadece klinik yönleri değil, aynı zamanda kişinin sürdürülebilir sağlığı getirmek için bakım uyumu ve sağlıklı yaşamı başarıyla yürütmesini engelleyen, sosyal ve ekonomik faktörleri de dikkate almalıdır.

Efektif bakım sonuçlarını vermek, bireysel sağlığın ve yaşam durumlarının engellerini açıkça belirlemeyi gerektirir. Eş zamanlı 2 hastalığa sahip hasta sayısı arttıkça, "silo haline getirilmiş" tek tip bakım tüm bakımlara uyar yaklaşımı, etkili bakım sonuçlarının motive edilmesinde ve ele alınmasında elverişli değildir. Bu nedenle, hastaların çok yönlü sağlık ve sağlıklı yaşam gereksinimlerini içerecek şekilde uyarlanmış daha esnek bir bakım modeli düşünülmelidir. Bu, hastanın şahsi bakımını aktif olarak takip edebileceği, yönetebileceği ve ona katılabileceği kapsamlı ve dinamik bir interaktif bakım planının hayati önem taşıyor olmasını gerektirir.

## 4.2 Klinik Sonuçlar

Hastayla doğrudan ilişkili olan sonuçlara odaklanan Hastaya bağlı sonuç ölçütleri (PROMs), son birkaç yıl içinde önem kazanmıştır. Bunun nedeni, kısmen, hasta bakım deneyimine odaklanan artan dikkat ve hastalığın yükü ve etkisi üzerine hasta odaklı bir değerlendirme sağlamaktır. PROM'lar, fiziksel veya sosyal işlev, tedavi uyumu ve tedaviden memnuniyet gibi sağlıkla ilişkili yaşam kalitesi göstergelerinin semptomlarını ve diğer yönlerini içerebilir. Ayrıca, kanser veya çoklu skleroz gibi spesifik koşullar için tedavilerin daha detaylı ve tam bir değerlendirmesini sağlayarak, tedaviye bağlı morbiditelerin yükü açısından daha doğru hasta-hekim iletişimini kolaylaştırabilirler.

PROM'lar, hastalığın ve tedavisinin etkisini hastanın bakış açısından doğrudan gösterdikleri için geleneksel klinik etki ölçütlerinden (örn., Kanserde hayatta kalma, sigarayı bırakma) farklıdır. Bu ölçütler, tedavinin verimi ile hasta üzerindeki yükü arasındaki dengeyi inceleyebilir. Fiziksel işlevsellik, genel iyilik hali gibi alanlara bakmanın ve genel klinik yararına göre tedavilerin güvenilirliğini ve emniyetini vurgulamanın da etkili olduğu düşünülmektedir. Ölçütlerin kendisinin hastanın bakış açısıyla geliştirildiğinden, tedavide karar verme sürecinde, hastanın daha fazla katılımını sağlamanın yanı sıra sağlık hizmeti kararlarında rehberlik sağlayabilir. Esasen, bir blok zinciri PROM altyapısının takviye edilmesi, hizmet sağlayıcıları ve ödeme yapanları bakım standartlarını karşılama konusunda teşvik etme kabiliyetini güçlendirir.

# 5 Sonuç

Blok zinciri, sağlık hizmeti IT(Bilişim teknolojileri)'sinde gittikçe önemli bir rol oynayacak ve ekosistemdeki tüm paydaşlara yeni verimlilikler ve faydalı bir parçalanma getirecektir. Sağlık kuruluşlarının, teknolojinin gerektirdiği değişikliklere hazır olduklarından emin olmak için blok zinciri teknolojisinin özünü anlamaları çok önemlidir.

Sonuç sağlık sektöründe gelecek dönemi şekillendirecek yeni nesil güçlü blok zinciri tabanlı uygulamalar olacak. Blok zincirinin sağlık sektöründe potansiyelini gerçekleştirmesi için, silolaştırılmış sağlık sistemi peyzajı içindeki uyumluluğu ve birlikte çalışabilirliği temin etmek standartlara dayanmalıdır.

www.patientory.com
Google Slack Twitter Facebook Reddit BitcoinTalk GitHub Telegram Medium

# Kaynakça

[1] "A Begoyan. An overview of interoperability standards for electronic health records." In: (2007.).

[2] Charles N Mead et al. "Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still dicult. do we really need a better mousetrap?" In: (2006.).

[3] Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. "MedRec". In: (2016). URL: www.pubpub.org/pub/medrec.[Accessed:05-Apr-2017].

[4] National Healthcare Ant-Fraud Association. "The Challenge of Health Care Fraud". In: (). URL: https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

[5] Vitalik Buterin. "A next-generation smart contract and decentralized application platform. White Paper". In: (2014.).

[6] Yan-Cheng Chang and Michael Mitzenmacher. "Privacy preserving keyword searches on remote encrypted data.In International Conference on Applied Cryptography and Network Security". In: ().

[7] Mayo Clinic. "Changes in Burnout and Satisfaction With Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014". In: (). URL: www.mayoclinicproceedings.org.

[8] Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. "Reidao: Digitising Real Estate Ownership". In: (). URL: http://reidao.io/whitepaper.pdf.

[9] et al. Centers for Disease Control Prevention. "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services." In: (2003.).

[10] Roy Thomas Fielding. "Architectural styles and the design of network-based software architectures." In: (2000.).

[11] HHS.gov. "H. H. S. O. of the Secretary Summary of the HIPAA Privacy Rule". In: (2013). URL: www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.[Accessed:04-Apr-2017].

[12] HHS.gov. "Methods for De-identification of PHI". In: (2015). URL: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected.[Accessed:04-Apr-2017].

[13] Alex Mizrahi Iddo Bentov Charles Lee and Meni Rosenfeld. "Proof of activity: Extending bitcoin's proof of work via proof of stake." In: (2014).

[14] Sunny King and Scott Nadal. "PPCoin: Peer-to-peer crypto-currency with proof-of-stake." In: (2012).

[15] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: (2008).

[16] Stean D Norberhuis. In: ().

[17] Pishing Chiang Philip Chuang Maureen Madden Rainer Winnen-burg Rob McClure Steve Emrick Olivier Bodenreider Duc Nguyen and Ivor DSouza. “The NLM Value Set Authority Center.” In: (2013.).

[18] Amit P Sheth. “Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In Interoperating Geographic Information Systems,” in: (1999.).

[19] Nick Szabo. “Formalizing and securing relationships on public networks.” In: (1997.).

[20] “US GPO. CFRx 164 security and privacy. 2008.” In: (). URL: http://www.access.gpo.gov/nara/cfr/waisidx08/45cfr16408.html.Accessed:2016-08-06..