Çok Amaçlı Kullanıcı Egemen KYC'siz Kimlik Çözümü

2 Ağustos 2021

İnternet kelimenin tam anlamıyla bir kimlik krizini ortaya çıkarıyor. Yerleşik bir kimlik katmanının yokluğu, güvenlik ve birlikte çalışabilirlik sorunlarına neden oluyor. Ayrıca, ABD merkezli GAFAM'ın halihazırda kimlik çözümlerini merkezileştirilmesi, ülkeler, kullanıcılar ve hizmet sağlayıcılar için egemenlik ve bağımlılık sorunları yaratıyor.

Kullanıcı egemen kimliklerin yükselişi bu açmaza bir cevaptır. UniknameTM, iş uygulamalarına odaklanan merkezi olmayan bir kimlik platformu önermektedir. Proje, insan tarafından okunabilen merkezi olmayan tanımlayıcılar sağlayan özel bir blok zinciri olan UniknameTM Ağını kullanıyor. UniknameTM, iş uygulamalarının çok yönlülüğünü ve özelliklerini benimsemek için modüler bir tasarım benimsiyor, birçok ihtiyaca cevap vermek için birleştirilebilen uyarlanabilir ve yeniden kullanılabilir özellikler geliştiriyor. UniknameTM halihazırda Avrupa'da yapılan bir yetkilendirme çözümü sunuyor: UniknameTM Connect.

Whitepaper

Sürüm	Yayınlanma	Katkıda Bulunanlar
		Laurent Lourenço
V1	18 Eylül, 2018	Damien Lecan
		Fabien Tr´eguer
		Guillaume Nicolas
V2.1	12 Temmuz 2021	Sophie Dram´e-Maign´e
		Juliette M´egret
V2.2	2 Ağustos 2021	Sophie Dram´e-Maign´e
		Juliette M´egret

İçindekiler

1 Giriş

Dijital kimliklerimizi düşündüğümüzde, profil resimleri, komik tweet'ler, esprili forum gönderileri veya saçma kullanıcı adları aklımıza geliyor. İnternet için titizlikle hazırlanmış bir sunum. Ancak çevrimiçi etkinliklerimiz, paylaşmaya hazır olduğumuzdan çok daha fazlasını ortaya koyuyor. Ve böylece dijital bir kimlik aynı zamanda konumlu gönderilerden, farklı hesapları aynı e-posta adresine bağlayan sızdırılmış verilerden veya bir uyku programını ya da bir zaman dilimini ele veren bağlantı geçmişinden oluşur.

İnternetin mevcut durumunda, dijital kimlikler bu nedenle, bu kimlik tarafından temsil edilen varlığın yalnızca biri üzerinde kontrole veya tam bilgiye sahip olduğu iki bölümden oluşur. Bazı şirketler iş modellerini bu veriler üzerine kurmuştur. Bazı şirketler bunu nasıl güvence altına alacaklarını ve yöneteceklerini güçlükle biliyorlar.

GAFAM, kendilerini küresel İnternet'in kimlik sağlayıcıları olarak tanıtmaktadır. Sonuç olarak, İnternet üzerinden aktarılan kişisel verilerin çoğunluğu ABD merkezli şirketler tarafından kontrol edilmektedir. Bu hem bir egemenlik hem de bir tekel sorunu doğurur. GAFAM, kurallarını daha küçük şirketlere empoze etmek için rutin olarak onların konumlarını kullanır. Örneğin uygulama geliştiricileri, uygulamalarında Apple veya Android'in ödeme sistemini kullanmak, %15 ila %30 arasında bir ödeme yapmak ve Amerikan teknoloji devleri tarafından dikte edilen diğer kurallara uymak zorundadır.

Ancak, yerel mevzuat bunları düzenlemek için hareket ederken, GAFAM çıkarlarını korumak için şiddetli bir lobicilik savaşına girdi. Google, 2014'ten bu yana Avrupa komisyonu ile yaklaşık 250 üst düzey toplantı yaptı [1]. Google, Facebook ve Microsoft'un her biri AB lobi faaliyetlerinde yılda 5,25 milyon Avro'nun üzerinde harcama yapıyor [1]. Öte yandan Twitter, Hindistan hükümetinin Covid-19 pandemisini ele alış biçimini eleştiren tweetleri sansürleme talebine boyun eğdi [2]. Ayrıca birçok hesabı askıya aldı. Bu askıya alma, Google, Facebook veya Twitter kimlik doğrulama hizmetlerini kullanmış olabilecek diğer hizmetleri de etkiliyor.

Daha çeşitli, daha merkezi olmayan bir İnternet herkes için daha güvenlidir. Kötü güvenlik uygulamaları ve sık yaşanan olaylar, kullanıcıların bir zamanlar sahip olabileceği güveni aşındırdı. Daha fazla mahremiyet, daha fazla şeffaflık ve hakkımızda hangi verilerin toplandığı üzerinde daha fazla kontrol için bir baskı var. Ancak dijital dünyanın mevcut versiyonu bu değişimi gerçekleştirmek için oluşturulmamıştır.

Bu kadar derin bir değişikliğin neden iş açısından da gerekli olduğuna dair güçlü argümanlar var. Mevcut haliyle, kişisel verilerin yönetimi hizmet sağlayıcılara büyük bir yük getirmektedir. Güvence altına almanın maliyeti vardır, şirket için bir sorumluluk, potansiyel bir PR1 riski vb. temsil eder. Güvenliklerini veya yönetimini üçüncü bir tarafa devretmek karmaşıklığı ve artan maliyetleri beraberinde getirir.

Kullanıcı Egemen Kimlikler (SSI)

Bir bireyin birden fazla dijital kimliği vardır. Her yeni hizmeti kullandıklarında yeni bir tane oluşturulur. Bu kimliklerin sınırlı bir kapsamı vardır, yalnızca bu hizmet bağlamında var olurlar ve kimliğe gerçekten sahip olan hizmettir. Bazı durumlarda, tanımlama ve kimlik doğrulama delege edildiğinde, hizmetin kendisi kimliğe bile sahip değildir. Bu, her biri kendi tanımlama mekanizmalarına ve sonradan düşünülen birlikte çalışabilirliğe sahip çok sayıda merkezi sistemden oluşan bir koleksiyon olarak inşa edilmiş bir ekosistemin doğrudan bir sonucudur. Sahipler olarak, kimlik sağlayıcılar tek taraflı olarak herhangi bir kimliği silmeye, tanımlayıcısını değiştirmeye veya bunların yapımını, kullanımını veya geçerliliğini yöneten kuralları değiştirmeye karar verebilir.

Önde gelen şifre yönetimi çözümlerinden biri olan Dashlane, 2022 yılına kadar ortalama bir Amerikalının yaklaşık 300 farklı web hesabına ve neredeyse aynı sayıda dijital kimliğe sahip olacağını tahmin ediyor [3].

Güvenlik	Kontrol Edilebilirlik	Taşınabilirlik
Koruma	Varoluş	Birlikte Çalışabilirlik
Kalıcılık	Kalıcılık	Şeffaflık
Minimizasyon	Kontrol	Erişim
	Rıza	

Tablo 1: [5] Kullanıcı Egemen Kimliğin On İlkesi

Temsil edilen tanımlama ve kimlik doğrulama ile kullanıcılar ve hizmet sağlayıcılar, kullanılabilirlik ve güvenlik için kimlik sağlayıcılara bağımlıdır. Aralık 2020'de [4] Google, kimlik doğrulama sistemiyle ilgili bir sorun yaşadı. Sonuç olarak, Google Hizmetlerinin çoğu ve üçüncü taraflar kullanılamaz hale geldi. Benzer şekilde, ister kullanıcı ister servis sağlayıcı olarak Google hizmetlerini kullanırken, veri gizliliği Google'ın koruması kadar güçlüdür. Bireye kimliklerini geri vermek ve işletmenin kimlik sağlayıcılara olan bağımlılığını kırmak için kimliklerin herhangi bir hizmetten bağımsız olarak var olmaları gerekir.

Kullanıcı Egemen Kimlik teriminin sabit bir tanımı yoktur. Bir ilkeler bütünüdür. SSI üç temel üzerine inşa edilmiştir: Güvenlik, kontrol edilebilirlik ve taşınabilirlik [6]. Tablo 1 bu sütunları daha da geliştirmektedir. Bu paradigmada, kimlikler temsil ettikleri varlık tarafından sahiplenilir ve kontrol edilir. Hizmetler arasında kalıcıdırlar. Sahipler, kimlikleriyle ilişkili bilgilere erişebilir ve paylaşılmadan önce izin vermelidir.

UniknameTM Vizyonu SSI'ya geçiş Kullanıcı korkutucu ancak hizmet sağlayıcıların bağımsızlığını korumak, veri hareketliliğini ortaya çıkarmak ve kullanıcıların güvenini korumak için gerekli. Unikname, hem kimlik tabanlı hizmetler hem de bunları taşımak için merkezi olmayan mimari sunan merkezi olmayan bir kimlik platformu oluşturarak bu değişim boyunca işletmelere eşlik etmek istiyor.
Proje dört zorunluluk etrafında dönüyor:

• Güvenlik - İnternet'in kimlik krizine yönelik çözüm, mevcut uygulamalarda güvenlik açığı özelliklerini tanıtamaz. Tanımlama, erişim denetimi, yetkilendirme ve diğer bir dizi kritik sürecin merkezinde yer alır. Bu nedenle UniknameTM'nin yaptığı her şeyde güvenlik birinci öncelik olmalıdır.
• Kullanılabilirlik - Güvenlik, kullanılamıyorsa veya kullanılmayacaksa hiçbir şey ifade etmez. Ayrıca, kullanıcıların ve hizmet sağlayıcıların benzer şekilde yeni SSI paradigmasına alışmaları gerekmektedir. Kullanılabilirlik, Unikname'nin cephaneliğinde benimsenmeyi sağlamak için önemli bir silahtır.
• Modülerlik - SSI uygulamalarının potansiyeli çok büyüktür. Bundan ve yerleşik birlikte çalışabilirliğinden yararlanmak için Unikname'nin tasarımı modüler ve uyarlanabilir olacaktır.
• Bağımsızlık - GAFAM, SSI çözümleri geliştirmeye başlamıştır. Microsoft ION, Mart 2021'de tanıtıldı. Mevcut durumun tekrarını önlemek ve çevrimiçi egemenliği korumak için yalnızca ABD merkezli olmayan altyapılara ve hizmetlere sahip olmak önemlidir.

SSI'yı gerçekleştirmek için araçlara ihtiyaç vardır. Özellikle ikisi: Dijital kimlikleri oluşturmak ve kişiselleştirmek için nitelik verme mekanizmaları ve bunları ele almak için kimlik mekanizmaları. Bu rolleri yerine getirmek için iki teknoloji öne çıkıyor: Doğrulanabilir İddialar ve Merkezi Olmayan IDentier standardı. Aşağıda, ilgili okuyucu için bu iki kavramın daha teknik bir sunumu bulunmaktadır.

Şekil 1: Bir VC'nin Aktörleri

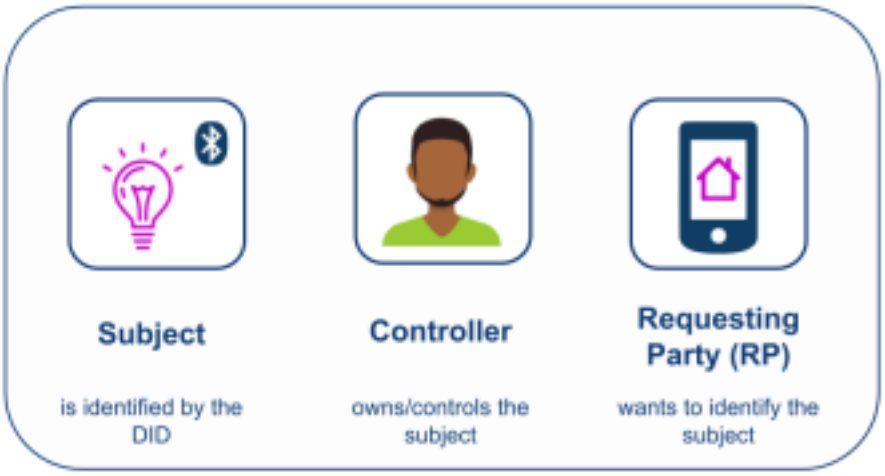
Doğrulanabilir İddialar veya Doğrulanabilir Kimlik Bilgileri (VC)

IETF [7], kimliği, [bir] varlığın tanınabilir veya bilinebilir olduğu bir dizi nitelik değerlerinin kolektif yönü olarak tanımlar.

Bu nedenle, bir kimlik niteliklerle tanımlanır. Bu bilgilerin bir kimlikle nasıl ilişkilendirileceği anahtardır. Klasik olarak, nitelikler, Kimlik Sağlayıcılar adı verilen özel kuruluşlar tarafından verilir ve onaylanır. Kimlik Sağlayıcılar, merkezi veya federe sistemlerin parçalarıdır. Bir kullanıcının sahip olduğu her özelliği bilirler ve bir kullanıcı özelliklerinden birini bir servis sağlayıcıya her sunduğunda potansiyel olarak haberdar edilirler.
Bir özelliğin kapsamı sınırlıdır ve onu yayınlayan Kimlik Sağlayıcıya bağlıdır. Servis sağlayıcıların iki olası seçeneği vardır: maliyetli, karmaşık ve sınırlayıcı olan kendi Kimlik Sağlayıcılarını işletmek veya birine abone olmak. Kullanıcıların kimliklerinin anahtarlarını ellerinde bulundurdukları için Kimlik Sağlayıcıları arasında geçiş yapmak zor bir süreçtir.
Hem kullanıcıları hem de hizmet sağlayıcıları Kimlik Sağlayıcılardan kurtarmak için SSI, Doğrulanabilir İddialar (VC) kullanır. Bir VC, birisi (ihraççı) tarafından bir şey (konu) hakkında yapılan bir iddiadır. Adres, kullanıcının yaşı veya sağlık durumu gibi özellikleri ifade etmek için kullanılabilirler. VC ayrıca izinleri de ifade edebilir: doktor reçetesi, muayeneye kayıt, güvenlik ekibinden bir program yüklemek için onay vb. Şekil 1 VC'yi çevreleyen farklı aktörleri göstermektedir.
VC, yayıncıları tarafından imzalanır. İmza ve dolayısıyla talep, bir Merkezi Olmayan Açık Anahtar Altyapısı (DPKI) olarak blok zinciri kullanılarak doğrulanabilir. Aynı ihraççıdan gelen birkaç talep, kimlik bilgilerini oluşturmak için birleştirilebilir. W3C, VC verme ve sunumunu normalleştirmiştir (doğrulama için bir hizmet sağlayıcıya iddiaları gönderme eylemi) [8].

Merkezi Olmayan Tanımlayıcı (DID)

Kullanılabilir olması için, bir kimliğin bir tanımlayıcıya, onu benzersiz bir şekilde adlandırmak için bir araca ihtiyacı vardır. Bir dizi dijital tanımlayıcı vardır: e-posta, twitter tanıtıcıları, çeşitli kullanıcı adları vb. Bunların tümü hizmete bağlıdır. SSI'yı tanımlamak için yeni bir tür merkezi olmayan tanımlayıcıya ihtiyacımız var.



Şekil 2: Bir DID'nin Aktörleri

DID, W3C ve Merkezi Olmayan Kimlik Vakfı (DIF) tarafından normalleştirilmiş bir tanımlayıcıdır. Dağıtılmış defterler (yani blok zincirler) sayesinde, DID gerçek bir merkezi olmayan şekilde oluşturulabilir ve yönetilebilir. Kontrol edilebilirlik, güvenlik ve birlikte çalışabilirlik gibi özellikler sunarlar.

Şekil 2'de gösterildiği gibi, bir DID iki varlıkla ilişkilendirilir: öznesi ve denetleyicisi. Konu, DID'nin tanımladığı ve temsil ettiği şeydir. Kontrolör, bu konuyu kontrol eden kişidir. Çoğu durumda, her iki varlık da bir ve aynı olacaktır. Ancak bazen, DID kendini kontrol edemeyen bir şeyi veya birini tanımlar. Bir çocuğu ve onun ebeveynini hayal edin. Bir IoT cihazı ve sahibi veya ağ geçidi. Bir evcil hayvan ve bakıcısı. DID, herhangi birini ve herhangi bir şeyi tanımlamak için kullanılabilir. Onları bu kadar güçlü yapan da budur.

2 UniknameTM Projesi

Projenin amacı, blok zinciri inovasyonundan yararlanarak Merkezi Olmayan Kimlik yetenekleriyle web çözümlerini güçlendirmektir. UniknameTM, özel bir blok zincirine dayanan bir SSI platformudur. Platform, kullanıma hazır merkezi olmayan kimlik ürünlerini ve bir entegrasyon çerçevesini birleştirir.

2.1 Yeni bir tür tanımlayıcı: insan tarafından okunabilen DID

2.1.1 Kurucu İlkeler

UniknameTM projesi evrensel, insan tarafından okunabilen ve merkezi olmayan tanımlayıcılar yaratmayı amaçlamaktadır. DID, kutudan çıktığı anda bu gereksinimlerden ikisini çözmüştür: hem evrenseldirler hem de yapım gereği merkezi değildirler. İnsan tarafından okunabilirlik, UniknameTM projesinin temel taşıdır.

DID kutudan çıktı DID, tasarımlarına entegre edilmiş birlikte çalışabilirliğe sahiptir. Yaratıcıları [9] tarafından ortaya konan temel gereksinimler şunlardır:

• Merkezi olmayan: merkezi bir yayınlayan kurum olmamalıdır;
• Kalıcı: tanımlayıcı doğası gereği kalıcı olmalı ve ast bir organizasyonun sürekli çalışmasını gerektirmemelidir;
• Kriptografik olarak doğrulanabilir: tanımlayıcının kontrolünü kriptografik olarak kanıtlamak mümkün olmalıdır;
• Çözülebilir: tanımlayıcı hakkında meta verileri keşfetmek mümkün olmalıdır.

İnsan Tarafından Okunabilen DID, genellikle kriptografik malzemeden türetilir. Sonuç olarak, makineler tarafından kolayca işlenen, ancak insanlar için kafa karıştırıcı olan uzun karakter zincirleri şeklini alırlar. Bu bir güvenlik riski oluşturur ve kullanılabilirlik açısından kötüdür.
Kendilerine opak olan tanımlayıcıları manipüle ederken, kullanıcıların bir ikame fark etme olasılığı daha düşüktür. Bu dürüst bir hata olabilir (örneğin kopyalarken) veya kötü olabilir (bir hedefin tanımlayıcısını kendinizinkiyle değiştirmek). Her iki durumda da kullanıcıları korumak için ekstra mekanizmaların devreye alınması gerekir. Bu ihtiyaç, insan tarafından okunabilirlik eksikliğinden kaynaklanmaktadır.
Kullanılabilirlik, yeni teknolojilerin ve paradigmaların benimsenmesi için bir gerekliliktir. Bazı kullanım durumları, DID'nin kağıda yazılmasını, sözlü olarak iletilmesini veya dijital dünyanın dışına çıkaracak herhangi bir şekilde (bir kartvizite basılmış, promosyon materyali, radyo reklamı vb.) gerektirebilir. Bu durumlarda, insan tarafından okunabilirlik çok önemlidir. Ayrıca,

kullanılabilirlik açısından, karmaşık tanımlayıcıları teknolojiden anlayan olmayan kullanıcılardan gizlemek en iyisi olabilir, böylece daha önce tanımladığımız güvenlik sorunlarını çoğaltabilir.
Bu bağlamda DID ve IP adresleri arasında bir paralellik kurulabilir. Alan adları, web sitesinin sunucularına hitap etmenin insan dostu bir yoludur. Benzer şekilde, DID'nin neyi temsil ettiğine bakılmaksızın, DID'nin insan tarafından okunabilir tanımlayıcılara ihtiyacı vardır.

2.1.2 Adlandırma sistemi

UniknameTM, aşağıdaki biçimde insan tarafından okunabilen tanımlayıcılar veya UniknameID sunar:

@[TYPE:]AÇIK DEĞER

Burada TYPE, birey, organizasyon ve ağ olmak üzere üç olası kategoriden birini ifade eder. Bir rakam (1,2 veya 3) veya bir dize (sırasıyla bireysel, kuruluş veya ağ) ile temsil edilebilir. Hiçbir tür belirtilmediğinde, tür varsayılan olarak bireysel olur. Bir UniknameID bu nedenle birkaç eşdeğer temsile sahiptir. Aşağıdaki UniknameID eşdeğerdir:

- @bob
- @1:bob
- @birey:bob

AÇIK DEĞER, bir UniknameID'nin insan tarafından okunabilen kısmıdır. Safe-TypoTM alfabesinden rastgele uzun bir dizedir (bkz. Bölüm 2.4.1). Kimlik avı ve kimlik sahtekarlığı girişimlerini önlemek için, çok yakın olan açık değerler eşdeğer olarak kabul edilir. Örneğin, aşağıdaki UniknameID eşdeğerdir:

- @bob
- @BOB
- @b0b
- @b.o.b
- @bob———————

Bir UniknameID'nin nadirliği ve dolayısıyla değeri, uzunluğuna bağlıdır. Modeller, onları sınıflandırmak ve fiyatlandırmak için kullanılır. Bir UniknameID'nin uzunluğu hesaplanırken ayırıcılar dikkate alınmaz. Yukarıdaki tüm UniknameID'lerin üç karakter uzunluğunda olduğu kabul edilir.

2.2 Uniknameʼnin NFTʼsi: UniknameID

İnsan tarafından okunabilirlik gereksinimini çözmek için UniknameTM iki farklı DID türü kullanır. İlk DID, UniknameTM Network hesaplarına eklenir. Bir kullanıcı ağa ilk kez bir işlem gönderdiğinde oluşturulurlar. İkinci tür DID, bir NFT'ye, UniknameID'ye eklenir.

NFT, Fungible Olmayan tokenlar anlamına gelir. Bitcoin, euro veya dolar gibi değiştirilebilir tokenlar, birbirinin yerine kullanılabilen tokenlardır. Bu, bir euronun diğer herhangi bir euroya eşdeğer olduğu anlamına gelir. Buna karşılık, NFT türünün tek örneği tokenlerdir. Sanat eserlerini, koleksiyonluk kedi yavrularını veya gayrimenkulleri temsil etmek için kullanılabilirler.

UniknameTM, insan tarafından okunabilir tanımlayıcıları temsil etmek için NFT kullanır. Bu, bir UniknameID'nin ne kadar değerli ve benzersiz olduğunu vurgular. Tıpkı diğer NFT'ler gibi, bunlar da dövülebilir, satın alınabilir, takas edilebilir, vb. Ünlü bir önceki sahibine ait bir UniknameID edinebilirsiniz!

UniknameID, UniknameTM Ağının temel taşıdır. Delege olmak veya birini desteklemek için fikir birliği protokolünde yer almaları gerekir. Ayrıca UniknameTM altyapısının sunduğu hizmetlerin çoğunu kullanmaları gerekmektedir. Kayıplara ve saldırılara karşı koymak ve bunlardan yararlanmaya devam etmek için UniknameID'nin sahibi tarafından canlı tutulması gerekir.

2.2.1 Özellikler

Bir UniknameID aşağıdaki özelliklere sahiptir:

• Benzersiz - Bir UniknameID'nin sahibi, tanımlayıcısının benzersiz olduğunu ve aynı ad alanında hiç kimsenin aynısını alamayacağını garanti eder. Her UniknameID, UniknameTM Network blok zinciri içinde bir token olarak kilitlenmiş tek bir şifreleme karma kodu ile temsil edilir.

• Değişmez - Oluşturulduğunda, UniknameID blok zincirine yazılır. Bu, değiştirilemeyecekleri veya silinemeyecekleri anlamına gelir.

• Gizlenmiş - Bir UniknameID'nin açık değeri doğrudan zincir üzerine yazılmaz. Bunun yerine bir kriptografik karma kullanılır.

• Kullanıcı Egemen - Her UniknameID, onu kontrol edebilen tek varlık olan belirli bir sahibine aittir.

• Dayanıklı - Bir UniknameID kullanıldığı sürece, süresiz olarak sahibine aittir.

Ek olarak, UniknameID iki tür özellikle kişiselleştirilebilir: kullanıcı özellikleri ve sistem özellikleri. Ayrıca rozet toplayabilirler. Bir UniknameID alınıp satıldığında, bu özelliklerden bazılarını koruyabilir. Premium UniknameID, mülkleri saklamak için daha fazla alandan, daha

uzun kullanım ömründen ve çeşitli hizmetlerde avantajlardan yararlanır.

Sistem özellikleri, zincirdeki diğer eylemlerin sonucu olarak ayarlanır ve değiştirilir. Doğrudan değiştirilemezler. Sistem özellikleri, bir UniknameID'nin yaşam döngüsü durumunu (bkz. Bölüm 2.2.3), açıklanan açık değerleri, doğrulanmış özellikleri, kamuya açık kanıtları vb. içerir.

Kullanıcı özellikleri, kullanıcıların kendileri tarafından belirlenir. Zincir üzerinde kayıtlıdırlar ve herkesin erişimine açıktır. Kullanıcı özelliklerine örnek olarak PGP anahtarları, e-posta adresleri, Bitcoin, Ark veya Ethereum adresleri, web sitesi url'si veya bir kullanıcının UniknameID'sine bağlamak istediği diğer bilgiler verilebilir.

Rozetler olaylara bağlanabilir (Easteregg2021), güvenlik özelliklerini (İkinci Parola), kullanıcıların ağda oynadıkları rolü (Temsilci) ve diğer birçok şeyi gösterir. Başkalarının bir UniknameID'nin durumunu, anlamını ve güvenilirliğini ölçmesine yardımcı olurlar.

2.2.2 Edinme

UniknameTM ağındaki her insan tarafından okunabilen tanımlayıcı, benzersiz bir şekilde bir UniknameID ile temsil edilir. Bu NFT daha sonra bir kripto-hesabına aittir ve böylece ikisini ilişkilendirir. UniknameID iki şekilde edinilebilir: mevcut sahibinden mevcut bir UniknameID satın alarak veya zincirde yeni bir UniknameID oluşturarak. Herhangi bir zamanda, belirli bir açık değerden yalnızca bir UniknameID olabilir.
NFT Fabrikası, zincire yeni UniknameID ekleme yetkisi olan tek UniknameTM Ağı üzerinde özel bir tür hizmet sağlayıcıdır. Bir UniknameID'nin fiyatı, uzunluğuna bağlıdır. Ne kadar kısa, o kadar nadir, o kadar pahalı.

2.2.3 Bir UniknameID'nin Yaşam Döngüsü

Tüm olası karakter dizilerinin alanıyla karşılaştırıldığında, insan tarafından okunabilen adların alanı çok küçüktür. Kullanıcılar, ele alınması ve ezberlenmesi daha kolay olan daha kısa adları tercih edecek ve böylece sorunu vurgulayacaktır. İnsan tarafından okunabilen tanımlayıcılar, topluluk üyeleri arasında adil bir şekilde paylaşılması gereken sınırlı bir kaynaktır. Zaman içindeki kullanılabilirlikleri önemli bir risktir.
Bir kullanıcı tarafından bir UniknameID alındığında ve bir kripto hesabıyla eşleştirildiğinde, bu eşleştirmeyi yalnızca ilişkili anahtar değiştirebilir. Bu beklenen ve istenen bir davranıştır. Ancak, bir UniknameID sahibi tarafından artık kullanılmadığında (kayıp anahtar, sahibinin ölümü vb.), onu serbest bırakmak avantajlı olacaktır.

Yanıt olarak, bir UniknameID'nin yaşam döngüsünü yönetmek için kurallar getirildi. Bu kurallarla artık kullanılmayan tanımlayıcılar topluluğa sunulur. Kurallar blok zincirine kodlanmıştır. Bu nedenle, herkesin erişimine açıktır ve topluluğun onayı olmadan değiştirilemezler. Aşağıdaki yol gösterici ilkelere uyarlar:

• sahibi tarafından kullanılan bir tanımlayıcının sonsuz bir ömre sahip olması,
• belirli bir tanımlayıcının etkinliğinin kanıtları, sahibi tarafından yayınlanır ve herkesin erişimine açıktır,
• kullanılmayan bir tanımlayıcı, yalnızca başka bir kullanıcının talep etmesi durumunda kaybolur.

Ek olarak, iki tür saldırı düşünülmelidir. İlk durumda, kötü niyetli aktörler mevcut tanımlayıcıların oldukça büyük bir kısmını ele geçirmeye çalışır. İkinci durumda, kötü niyetli aktörler, siber işgal için birkaç belirli tanımlayıcıyı (marka adları, ünlüler, vb.) Bu tehditlere karşı koymak için tanımlayıcılar etkinleştirilmelidir. Aktivasyon iki ilkeyi takip eder:

• hiç kullanılmamış tanımlayıcıların ömrü çok kısadır,
• bir tanımlayıcıyı etkinleştirmek, sahibinin katılımını gerektirir.

İkinci ilke, bu süreci otomatikleştirmeyi zorlaştırmayı amaçlar. Sonuç olarak, UniknameID zamanla gelişen bir yaşam döngüsü durumuna sahiptir.

2.3 Merkezi Olmayan Kimlik Platformu

Covid-19 salgını nedeniyle dünya dijital alana girmeye zorlandı. Sonuç olarak, çok sayıda kuruluş ve hizmet birdenbire çevrimiçi çalışmaya zorlandı: uzaktan çalışma, sanal doğum günleri, çevrimiçi alışveriş vb. Kriz yalnızca kaçınılmaz bir eğilimi hızlandırdı. Bu artan dijitalleşme hızı, mevcut sistemdeki kusurları vurguladı. Bunlar arasında bir kimlik katmanının olmaması.

Proof Point[10]'a göre, 2019'da kuruluşların %88'i hedefli kimlik avı saldırılarına maruz kaldı. Aynı rapora göre, bu saldırılardan en az biri dünya çapındaki kuruluşların %55'i için başarılı oldu. İnternette güven olmaması gerektiği bilinen bir gerçektir. Protokol, insanlardan ziyade makineleri bağlamak için oluşturulmuştur. Yine de insanları birbirine bağlar.

Kullanıcı Egemen Kimlikler, teknolojik ve felsefi olarak çevrimiçi kimliği nasıl yaptığımıza dair bir paradigma değişikliğini temsil ediyor. Kullanıcıları sistemin merkezine yerleştirir ve kimliklerinin oluşturulma ve verilerinin paylaşılma şekli üzerinde kontrol sahibi olmalarını sağlar. Bunu yaparken, aynı zamanda veri depolama ve yönetimini merkezden uzaklaştırır ve yerleşik birlikte çalışabilirlik sağlar.

İş açısından bakıldığında, bu yeni (dijital) dünya düzenine bağlı kalmanın birkaç nedeni var:

Sorumluluk Çoğu şirket, iş modellerini müşteri verileri etrafında oluşturmaz. Onlar için veriler bir sorumluluk olabilir. Yakın tarihli bir rapora göre [11] 2020, açığa çıkan kayıt sayısı açısından

şimdiye kadarki en kötü yıldı. Bir veri ihlalinin maliyeti bölgeye bağlıdır. ABD'de, 2019'da belirli bir şirket için ortalama 8,19 milyon dolar [12].

Ayrıca, Avrupa GDPR gibi yeni düzenlemeler, işletmeleri kişisel veri yönetimine daha yakından bakmaya zorlamaktadır. Bu arada bankacılık sektörü için KYC gereklilikleri gibi diğer düzenlemeler hassas verilerin toplanmasını zorunlu kılıyor.

Bu bağlamda, kullanıcı merkezli bir modelin benimsenmesi, verilerin tekrar kullanıcının eline ve şirketin eline geçmesi anlamına gelir. Veri depolama merkezi olmadığında, ihlal edilecek merkezi bir veritabanı yoktur.

Düşük Maliyet SSI'nın benimsenmesinin maliyetleri düşürmesinin birçok nedeni vardır: Paylaşılan altyapı, daha düşük depolama maliyetleri, daha düşük kurulum maliyetleri, daha az kapsamlı güvenlik önlemleri, daha düşük BT maliyetleri, vb. Bunlardan ikisine odaklanalım.

Blok zincirler ve dağıtılmış defterler, katılımcı şirketler arasında altyapı paylaşımını sağlar. UniknameTM Network'te blokları doğrulayan delegeler, işlem ücretlerinin yanı sıra protokol tarafından telafi edilir. Röle düğümleri, geçmiş verilerin depolanmasını sağlar. Geliştirme çabaları topluluk tarafından desteklenebilir. Tüm bunlar, her bir aktör için daha düşük operasyonel maliyetlere yol açar.

Gatner'a göre, Yardım Masası aramalarının %20 ila %50'si parola sıfırlama istekleridir. 2017 Forrester Research raporuna göre, tek bir parola sıfırlamanın maliyeti yaklaşık 70 ABD dolarıdır. Şifreler sadece bir örnektir. Merkezi dijital kimlik yönetimi ile ilişkili yüksek bir maliyet vardır. Bu maliyeti karşılıklı hale getirerek ve bir kısmını müşteriye aktararak, SSI çözümleri tüm maliyetleri düşürür.

Birlikte Çalışabilirlik ve Veri Hareketliliği SSI teknolojisi, birlikte çalışabilirlik için tasarlanmıştır. UniknameTM, ürünlerinin daha büyük bir ekosistemin parçası olmasını sağlamak için W3C ve DIF tarafından geliştirilen standartları kullanır. Uniname'nin kendi DID yöntemleri herkese açıktır [13, 14].

Bu, ürünler arasında, blok zincirleri arasında, sistemler arasında, bilgilerin özel defterden halka açık deftere veya tersine taşınmasına vb. olanak tanır. Bu, taşınabilir, doğrulanabilir, kullanıcı odaklı verilerin kilidini açar.

Yenilenen kullanıcı güveni Kişisel veriler ve gizlilik hakları söz konusu olduğunda dünya genelinde bir inanç krizi yaşanıyor. Düzenli kayıt ihlalleri ve kişisel verilerin yanlış kullanımı, kullanıcının güvenini sarstı. Sorun şu ki, mevcut paradigmamız güven üzerine kuruludur: güvenilir üçüncü taraflar, hakların devredilmesi, şeffaflık ve kontrol eksikliği, . . .

Gittikçe daha fazla sayıda kullanıcı alternatif arıyor. Kullanıcı merkezli çözümleri benimsemek, rekabetçi bir iş avantajını temsil eder.

Her şey için bir tanımlayıcı Merkezi olmayan tanımlayıcıların uygulanması sonsuzdur. Dijital kimlik, birçoğundan yalnızca biridir. Merkezi Olmayan Tanımlayıcılar evcil hayvanlara, IoT cihazlarına, endüstriyel süreçlere vb. atıfta bulunmak için kullanılabilir. W3C, tüm endüstrilerdeki ilgili kullanım durumlarına genel bir bakış sunar[15].

2.3.1 SSI uygulamaları için bir platform oluşturma

İş amaçlı kullanım durumlarında SSI için büyük bir potansiyel vardır. Teknoloji henüz emekleme aşamasında. Altyapının yapılması gerekiyor. Ve UniknameTM'nin yapmak istediği de budur.

UniknameTM, SSI'yı hizmet olarak sunmak istiyor. Web platformu sahiplerine ve mobil uygulama geliştiricilerine yönelik bir platform önermektedir. Bu platform, merkezi olmayan tanımlayıcıların ve kimliklerin yanı sıra UniknameTM'nin UniknameTM Connect gibi mevcut ve gelecekteki kullanıma hazır ürünleri oluşturma ve yönetimini içerir (bkz. bölüm 3.3). Ayrıca UniknameTM, özelliklerin API, SDK veya komut satırları aracılığıyla dApp'lere ve web ürünlerine entegrasyonunu sağlayan bir entegrasyon çerçevesi sunar.

2.3.2 Özellik odaklı

Uyarlanabilirliği ve kullanılabilirliği artırmak için kimlik platformu, bir dizi farklı iş kullanım senaryosunu karşılamak için birleştirilebilen atomik özellikler etrafında inşa edilmiştir. Özellik geliştirmelerinin planlanması, ya iş gereksinimlerinden ya da topluluktan kaynaklanan talepler tarafından yönlendirilir.
Bu yaklaşım, UniknameTM SSI çözümlerini modüler, uyarlanabilir, birleştirilebilir ve genişletilebilir hale getirir. Özellik örnekleri şunları içerir:

İmza Oluşturma Belirli bir UniknameID ile ilişkili anahtarla bir veri parçası için bir imza oluşturun. Veriler dijital bir belge, bir öznitelik, bir kimlik doğrulama sorgulaması vb. olabilir.

İmza Doğrulaması Belirli bir UniknameID ile ilişkili bir imzayı doğrulayın. Burada blok zinciri bir DPKI olarak kullanılır. Bu özellik, bir kullanıcının bu UniknameID ile ilişkili varlığın gerçekten verileri imzaladığını doğrulamasını sağlar.

Doğrulanabilir Talep Oluşturma JSON ve JSON-LD biçiminde VC oluşturun [8]. Bu özellik VC oluşturma isteklerini alır, ilgili verileri imzalar ve VC'nin bir JSON-LD temsilini oluşturur.

Ve çok daha fazlası Depolama, doğrulama veya sunum gibi VC ile bağlantılı farklı özelliklerden hızlı bir şekilde alıntı yapabiliriz. Oy kullanma kullanım durumlarıyla ilgili özellikler arasında oy

kullanma, toplama, seçim sonuçlarını birleştirme, bunları herkese açık olarak yayınlama vb. sayılabilir. Diğer çeşitli kullanım durumlarından daha fazla özellik türetilebilir.

2.3.3 Entegrasyon Çerçevesi

UniknameTM, ürünü için çeşitli kullanım yöntemleri sunar. My UniknameTM Uygulaması, platformda bulunan en son özellikleri içerir. Geliştiriciler, bunları test etmek, kullanılabilirliklerini değerlendirmek ve hangi seçeneklerin mevcut olduğuna dair bir fikir edinmek için kullanabilir.
Bazı kullanım durumları mevcut yazılımları içerir. Onlar için özellikler, bir SDK aracılığıyla mevcut uygulamalara atomik olarak entegre edilebilir. Modüller, özellikleri web platformlarına entegre etmek için kullanılabilir.
Kullanım durumları bir istemci arabiriminin oluşturulmasını gerektirdiğinde, My UniknameTM Uygulaması olduğu gibi kullanılabilir. Alternatif olarak, UniknameTM Ekibi, ilgili mevcut özellikleri oluşturarak özelleştirilmiş bir uygulama oluşturabilir.

2.4 Tasarım gereği güvenlik

Güvenlik, Unikname'nin DNA'sının bir parçasıdır. Tüm yazılım ürünleri ve yetenekleri, başlangıçtan güvenlik prizmasına kadar tasarlanmıştır. Bir kimlik ve güvenlik sağlayıcısı olarak,UniknameTM, hizmetlerini kullanan sistemlerde bir güvenlik açığı oluşturamaz. UniknameTM Ekibi aşağıdaki yönergelere uyar:

Standartlara güven UniknameTM, DIF üyesidir. Vakıf, DID, VC ve SSI çevresinde endüstri standartları oluşturmak için çalışıyor. DIF, merkezi olmayan ağın geleceğinin şekillendiği yerdir. Bir üye olarak UniknameTM, merkezi olmayan kimlik inovasyonunun nabzını tutabilir.
UniknameTM dev Team'in sloganı, tekerleği yeniden icat etmeyin olabilir. UniknameTM Connect protokolü, OpenID Connect [16] tabanlıdır. Ayrıca DID-Auth, WACI gibi gelecekteki tüm endüstri standartlarıyla ve DIF ile OpenID Foundation'ın (OIDF AB/Connect çalışma grubu) ortak çalışmasından türetilen standartlarla da uyumlu olacaktır [17, 18, 19].
Standartlara güvenmek, birlikte çalışabilirliği garanti eder ve güvenliği artırır. 2021'de UniknameTM, üçüncü taraf güvenlik uzmanlarına bir güvenlik denetimi yaptırdı. UniknameTM Ekibinin iyi uygulamalara güvenmesi sayesinde, önemli bir ihlal tespit edilmemiştir [20].

Açık kaynak kodu üzerine kurulu Aynı ruhla, UniknameTM Ağı açık kaynaklıdır [21] ve açık kaynak kodu üzerine kuruludur. Örneğin, UniknameTM Network Core kodu, ARK Core Blok Zinciri Çerçevesine [22] dayanmaktadır. Unikname'nin yazılımı, özellikle kriptografik işlevler için yalnızca denenmiş ve test edilmiş kitaplıkları kullanır. Kod herkese açıktır ve herkes tarafından denetlenebilir. UniknameTM Ekibi ayrıca topluluktan kaliteli katkıları kabul etmekten mutluluk duyar.

Kişisel verilerin minimum düzeyde toplanması Günümüzde veri ihlalleri, bir şirketin imajı ve banka hesabı için çok ciddi bir tehdit oluşturuyor. Son üç yılda, kişisel verileri işleyen tüm kuruluşlar için tüketici güveni genel olarak azaldı [23]. Aynı zamanda, bir ihlalin maliyeti küresel ortalama 3,86 milyon dolara yükseldi. Müşterilerin kişisel verileri, 2020'nin en pahalı ihlallerinden sorumludur [24].

Bu bağlamda, en iyi hareket tarzı, mümkün olduğunca az kullanıcı verisi toplamak gibi görünüyor. UniknameTM modülleri tasarım gereği özeldir: veri toplama, gerekli verilerle sınırlıdır ve bu veriler yalnızca onu görüntülemekle meşru çıkarı olan aktörlerle paylaşılır. Unikname'nin sunucularında veya istemcilerinde hiçbir hassas veri düz metin olarak geçmez. Tüm kişisel veriler uçtan uca şifreleme kullanılarak şifrelenir.

Güvenlik ve Gizlilik iş başında Unikname'nin güvenlik ve gizlilik yönergeleri, çözümlerinin tasarımında da doğrudan görülebilir. Safe-TypoTM alfabesi ve UniknameID'nin açık değerinin varsayılan olarak gizlenmesi başlıca örnektir

2.4.1 Safe-TypoTM: kimlik avına ve yazım hatasına karşı yerleşik koruma

2021'de, ihlallerin %36'sı, geçen yıla göre %11 daha fazla kimlik avı içeriyordu. Kullanıcılar, sosyal medya uygulamaları, e-posta hizmetleri veya bankacılık platformları gibi popüler veya hassas çevrimiçi hizmetleri kullanırken her gün kimlik avı saldırılarının kurbanı oluyor.

İnternet kullanıcıları uluslararası bir bağlamda gelişiyor: birden çok dil, birden çok alfa bahsi, birden çok alan uzantısı, ... Bu küresel ekosistem, kimlik avı risklerinde artışa neden oldu. Gerçekten de, kötü niyetli bir Twitter tanıtıcısı veya alan adı oluşturmak mümkündür; bu, farklı alfa bahislerinden semboller kullanarak meşru muadili ile çok benzer. Ortalama bir internet kullanıcısı, sahte tanımlayıcıyı meşru bir hizmetle karıştıracak ve kimlik bilgilerini, kişisel bilgilerini, parasını vb.

Safe-TypoTM algoritması, her UniknameID'yi benzersiz bir kurallı temsil ile ilişkilendirir. Örneğin @bob, @b0b, @BOB ve @bOb–'nin kurallı temsilidir. Sistem, mevcut tanımlayıcılarla herhangi bir yeni UniknameID'nin yakınlığını kolayca kontrol edebilir. Yeni değer diğerine çok yakınsa, yani aynı kurallı gösterime eşleniyorsa, UniknameID oluşturulamaz. Bu nedenle kimlik bilgilerini avlamak çok zordur.

UniknameID, yalnızca Safe-TypoTM alfabesindeki karakterlerden oluşur. Bugün, Safe-TypoTM yalnızca genişletilmiş latin'i, yani 648 karakteri desteklemektedir. UniknameTM projesinin uluslararası boyuta yayılmasıyla birlikte çok daha fazla alfabe desteklenecektir.

2.4.2 Açıklanmayan UniknameID

Doğası gereği, blok zincirindeki herhangi bir yazı kalıcıdır ve asla silinmeyecektir. Bu özellik, gizlilik dostu bir çözümün kalbinde garip görünebilir. İşte bu yüzden UniknameTM yeni bir konsept getiriyor: Açıklanmayan UniknameID.

Bir UniknameID'nin açık değeri, yani insan tarafından okunabilir temsili, varsayılan olarak herkese açık değildir. Bunun yerine, bir kriptografik türetme işlevi, daha sonra blok zincirine yazılan bir Id hesaplar. Bir UniknameID'nin açık değeri bu nedenle gizlenmiştir.

Kullanıcılar UniknameID'lerini ifşa etmeyi seçebilirler. Bunu yaparken, insan tarafından okunabilen kimliklerini (açık değer) kamuya açık bir şekilde gizlenmiş kimliklerine bağlarlar.

3 SSI hizmetleri ve kullanım durumları

UniknameTM, merkezi olmayan kimliklerin işletmelere getirebileceği değere odaklanmıştır. Diğer şeylerin yanı sıra SSI, müşteri sadakatini artırma, kullanıcılara güven ve gizlilik sağlama, bir işletmenin siber güvenliğini düşük maliyetle güçlendirme ve merkezi kimlik sağlayıcılarından bağımsızlığı garanti etme gücüne sahiptir.

UniknameTM, platformunu oluştururken genişletilebilirlik ve modülerliğe odaklanmayı seçmiştir. Bu nedenle platform, daha sonra farklı kullanım durumlarında çağrılabilecek temel SSI hizmetleri etrafında inşa edilmiştir.

Bu bölüm, özellikler, modüller, hizmetler ve kullanım durumu gibi terimleri açıklayarak başlamaktadır. Daha sonra temel SSI hizmetlerini sunar: Merkezi olmayan kimlik doğrulama, gizlilik dostu veri paylaşımı, operasyon ve veri sertifikasyonu, anonim oylama, dijital kimlik yönetimi ve son olarak bir ödüllendirme sistemi. Bu liste kapsamlı değildir ve platformun ömrü boyunca büyümesi muhtemeldir.

Aşağıdaki bölümler, UniknameTM çözümlerinin potansiyelini temsil eden üç iş kullanım örneğini incelemektedir: UniknameTM Connect, UniknameTM C.A.R.E. ve UniknameTM Quorum.

3.1 Özellikler, Modüller ve Hizmetler: UniknameTM platformunu yapan nedir?

Özellikler: **yapı tuğlaları** Bölüm 2.3.2'de sunulduğu gibi, özellikler daha büyük şeyler halinde oluşturulabilen atomik SSI fonksiyonlarıdır. Özellik örnekleri, bir UniknameID'ye bağlı bir imzanın oluşturulmasını ve doğrulanmasını içerir. Bu iki özellik daha sonra diğer özellikler için temel olabilir (örneğin bir VC oluşturmak bir imza gerektirir) veya doğrudan modüller ve hizmetler tarafından, muhtemelen diğer özelliklerle bağlantılı olarak kullanılabilir (örneğin, bir belgeyi imzalamak iki ila üç temel işlev gerektirir: belgenin daha küçük temsili, bu temsilin imzalanması ve potansiyel olarak ortaya çıkan imzanın yayınlanması). Bu atomik işlevlerin kod tabanı, aşağıdakilere açık kaynak olacaktır:

- sağlamlığını garanti eder,
- topluluk üyelerinin kendi uygulamalarını bunların üzerine oluşturmasına izin verin.

Hizmetler: iki dünya arasında bir köprü Blockchain ekosistemi, ademi merkeziyetçilik etrafında inşa edilmiştir. Bu, bu ekosistemden (ve özellikle merkezi olmayan kimliklerden) yararlanabilecek, ancak onunla bütünleşmek veya etkileşim kurmak için gerekli değişiklikleri yapma isteğine veya

kaynaklarına sahip olmayan çoğu işletme için büyük bir paradigma değişikliğini temsil ediyor. İşte burada SSI hizmetleri ve ilgili hizmet sağlayıcılar devreye giriyor.
SSI hizmet sağlayıcıları, klasik olarak merkezileştirilmiş mimariler ile SSI ekosistemi arasında bir ağ geçidi görevi görür. Tekil bir adreslenebilir arayüz sunarlar, ancak sundukları hizmetler UniknameTM Network'e, yani merkezi olmayan bir deftere dayanmaktadır.
Ek olarak, bu hizmet sağlayıcı, ham veriler ile blok zincirinde kayıtlı olan kanıtlar (işlemler, sertifikalandırma vb.) arasında bir aracı olarak hareket ederek gizliliği artırabilir.
SSI hizmetlerine ilişkin örnekler Bölüm 3.2'de detaylandırılmıştır.

Modüller: entegrasyon kolaylaştırıldı Merkezi ve merkezi olmayan mimariler arasındaki farkı kapatmak için iki bileşen vardır. SSI hizmetleri olan ağ geçidine ek olarak, işletmelerin SSI işlevlerini yanlarında etkinleştirmeleri ve müşterilerine sunmaları gerekir. Örneğin, SSI'nın ana kiracılarından biri kontrol edilebilirliktir: kimlikler yalnızca sahiplerinin kontrolü altındadır. Bu nedenle, SSI kullanıcılarına, kimliklerini ve kriptografik materyal gibi kimlikleriyle ilgili şeyleri ele alacak araçlar sağlanmalıdır.
Modüller, bu nedenle, bir kullanıcı arabiriminde kaplanmış, SSI hizmet sağlayıcılarına yapılan çağrılarla tematik olarak paketlenmiş özelliklerin bir karışımıdır. Web platformlarına veya uygulamalara kolayca entegre edilmek üzere yapılmıştır.

Kullanım Durumları: SSI hizmetinizdedir SSI hizmetleri çok geneldir ve birçok uygulamaya sahip olabilir. Okuyucuların ve müşterilerin potansiyel uygulamalara yansıtmalarına yardımcı olmak için kullanım senaryoları gereklidir. Kullanım durumları, belirli durumları, gereksinimleri ve SSI modüllerinin ve hizmetlerinin bir sorunu veya mevcut bir teklifi daha iyi bir şekilde çözmek için nasıl kullanılabileceğini ayrıntılı olarak açıklar.
Kullanım örneklerine ilişkin örnekler, Bölüm 3.3'ten 3.6'ya kadar olan bölümlerin odak noktasıdır.

3.2 SSI Hizmetleri Örnekleri

Merkezi olmayan kimlik doğrulama SSI'ye yapılan ilk uygulamalardan biri kimlik doğrulamadır. UniknameTM, tek adımlı, güçlü ve e-postaya veya parolaya dayanmayan yeni nesil bir kimlik doğrulama sunar. Yalnızca bir UniknameID gerektirir.

Gizlilik dostu veri paylaşımı Bu hizmet, kullanıcının Merkezi Olmayan Kimliğine gömülü özel veya gizli verilerin kendi seçtikleri bir platformla (web sitesi veya uygulama) paylaşılmasını sağlar. Bilgi paylaşımına örnek olarak, bir hesap oluştururken bir e-postanın paylaşılması veya bir ödeme sırasında banka bilgilerinin paylaşılması verilebilir.

İşlemler ve veri sertifikasyonu Blok zincirleri genellikle KYC ile ilişkilendirilir. Ancak merkezi

olmayan kimliklerin değerli olması için resmi bir kimliğe güçlü bir şekilde bağlı olması gerekmez. Bu hizmet, belgeleri ve işlemleri KYC olmadan onaylamayı sunar. Bunun yerine, bir UniknameID'yi sertifikasyon gerektiren verilerle güçlü bir şekilde ilişkilendirir. Daha sonra, UniknameID'yi ve temeldeki dijital kimliği gerçek dünyadaki bazı muadilleriyle ilişkilendirmeleri gerekip gerekmediğine ve nasıl yapılacağına karar vermek işletmelere kalmıştır.
Şirketler, işlemleri onaylamak (ör. kritik bir süreçteki adımları onaylamak, toplantıya katılımı onaylamak, ...) veya verileri onaylamak (ör.

Anonim oylama Bu hizmet, kuruluşların veya bireylerin anketler, seçimler veya anketler oluşturmasını sağlarken, katılımcıların gizliliğine ve anonimliğine saygı gösterir. Hizmet sağlayıcı oy pusulalarını toplar ve oylamanın sonucunu onaylar. Hiçbir bireysel oy geri alınamaz. Her katılımcı, oylarının dikkate alındığını doğrulayabilir.

Dijital Kimlik Yönetimi Resmi kimliklerin aksine dijital kimlikler çok yönlü olabilir. Bu hizmet, bireylere birden fazla dijital kimliği ve bunlarla ilgili verileri yönetmek için gerekli araçları sağlar. Tematik olarak ayrık dijital kimliklerin örnekleri arasında artırılmış, platformlar arası bir oyun sözde oyunu veya kalıcı, işverenden bağımsız, çalışanların sahip olduğu profesyonel kimlik sayılabilir.

Ödüllendirme Sistemi Müşteri deneyimini geliştirmek ve işletmelere paradigma geçişi boyunca kullanıcılarını teşvik etmek ve onlara eşlik etmek için araçlar sağlamak için, bu hizmet sağlayıcı bir sadakat programı ve dijital tokenlara dayalı bir ödüllendirme sistemi sunar.

3.3 UniknameTM Connect: Tek adımda 2FA Kimlik Doğrulaması - Parolasız Oturum Açma

UniknameTM Connect, UniknameTM Ekibi tarafından uygulanan ilk kullanım örneğidir. Kullanıcıların yüksek düzeyde basitlik, gizlilik ve güvenlikle UniknameID'leriyle her yerde oturum açmasına olanak tanır. Merkezi olmayan kimlik doğrulama çözümü, heterojen oturum açma arabirimlerini birleştirmenin bir yolu olarak hem müşterilerle hem de bir kuruluş içinde kullanılabilir.
UniknameTM Connect, My UniknameTM Uygulamasında [25] yalnızca bir UniknameID ve bir insan onayı gerektirir. Bu Uygulama halihazırda işlevseldir ve yüzlerce kullanıcı tarafından çevrimiçi hesaplarının güvenliğini sağlamak için kullanılmaktadır.

3.3.1 Yenilikçi bir kimlik doğrulama sistemi

Platform kimlik doğrulaması, ister kayıt olun ister oturum açın, zahmetlidir. Ancak her şirket aynı sorunla karşı karşıya. Bu bağlamda kullanılabilirlik önemlidir. Baymard Enstitüsü'ne göre, bir

satın alma işleminden vazgeçen kullanıcıların %25'i hesap oluşturmadan vazgeçtiklerini söylüyor [26]. Uzun ve karmaşık kayıt süreçleri suçlanabilir. Alternatif olarak, kullanıcılar bir sonraki veri ihlaliyle sonuçlanabilecek kendi oturum açma bilgileri ve ilişkili parolalarıyla başka bir hesap oluşturma konusunda temkinli olabilirler. UniknameTM Connect, her iki sorunu da ele alır ve hem güvenlik hem de kullanılabilirlik sunar.

Evrensel, parolasız oturum açma UniknameTM Connect, parolasız bir kimlik doğrulama çözümüdür. UniknameID sahipleri, tek bir kimlikle (UniknameID'leri) ve akıllı telefonlarıyla katılan herhangi bir web sitesine veya uygulamaya giriş yapabilir (Şekil 3).

Şekil 3: UniknameTM Connect: Evrensel oturum açma

UniknameTM Connect, kullanıcıların kimliğini doğrulamak için bir parola gerektirmez. Bunun yerine, genel anahtar bilgilerini almak ve doğrulamak için blok zincirini bir DPKI olarak kullanır ve onu bulmak için kullanıcının UniknameID'sini kullanır. Kullanıcının akıllı telefonunda saklanan özel anahtar, bir kimlik doğrulama faktörü görevi görür. Uygulamaya erişim de doğrulanır (örneğin bir PIN kodu veya biyometri ile). Bu nedenle, UniknameTM Connect parolasız, İki Faktörlü Kimlik Doğrulama (2FA) kimlik doğrulama çözümüdür.

UniknameID, herhangi bir hizmetten bağımsız olarak tanımlandığından, herhangi bir katılan hizmete bağlanmak için kullanılabilirler. Yeni servis sağlayıcılara kaydolurken yeni bir kullanıcı adı tanımlamanıza gerek yoktur. Bu anlamda UniknameTM Connect evrensel bir oturum açma deneyimi sağlar: aynı UniknameID, aynı süreç, farklı hizmetler.
UniknameTM Connect ortakları, UniknameTM web sitesinde [27] listelenmiştir. Gelişmiş bir oturum açma deneyimi arayan kullanıcılar, muhtemelen başka türlü asla bilemeyecekleri platformlar bulacaklar.
İki faktörlü evrensel, parolasız kimlik doğrulama zaten mevcuttur. Meraklı okuyucular deneyip kendileri için kullanabilirler 2.

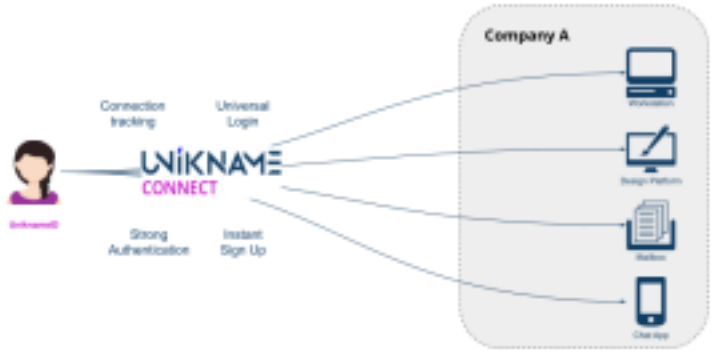
Anında Kayıt UniknameTM Connect ile web platformları sorunsuz bir kayıt olmanın keyfini çıkarır ve dönüşüm oranlarını artırır.
Dijital kimlikler (SSI), My UniknameTM Uygulaması içindeki profiller aracılığıyla tanımlanır. Bağlama bağlı olarak, profiller gerçek hayat bilgisi gerektirebilir veya gerektirmeyebilir: bir oyun forumunda takma adlar kabul edilir, bir banka aboneliği için doğrulanabilir devlet tarafından verilmiş kimlikler gerekir. Her durumda, UniknameTM Connect doğrulanabilir kimlik bilgileri yönetimi sunar.
Profiller oluşturulduktan sonra kayıt, oturum açmaya benzer tek adımlı bir işlemdir. Profil verileri, kullanıcının uygulamasından hedeflenen platforma şeffaf bir şekilde iletilir.

Gizlilik odaklı UniknameTM, kullanıcının verilerine erişemez. Profiller, merkezi olmayan bir şekilde saklanır ve yalnızca kullanıcının telefonundaki dApp'inde bulunur. Bir kullanıcı verilerini bir platformla paylaşmayı seçtiğinde, UniknameTM'nin bundan haberi bile olmaz. Protokol, tasarım gereği özeldir.
Kullanıcılar özel bir geçmişe erişir ve internet navigasyonlarını takip eder.

Ödüllendirme Sistemi Opsiyonel olarak UniknameTM Connect, $UNIK tokenlarına dayalı bir ödüllendirme sistemi sunar. Bu hizmete abone olan şirketler, her başarılı bağlantı için kullanıcılarına $UNIK dağıtabilir. Bu, özellikle UniknameTM kimlik platformundan diğer hizmetleri zaten kullanan kullanıcıları geri dönmeye ve yeni kullanıcıyı katılmaya teşvik eder.

3.3.2 İç güvenliğin iyileştirilmesi ve zaman tasarrufunun anahtarı

Bir şirkette çalışanların kendileri için seçilen araçları kullanmaktan başka seçeneği yoktur. Ancak, yanlış araçlarla, parolaları veya diğer kimlik doğrulama bilgilerini unuttuklarında (belki de uzun bir tatilden sonra) sıfırlamak için önemli ölçüde zaman kaybedebilirler. Ek olarak, arayüzlerin çokluğunu yönetmek kolay değildir. UniknameTM Connect her şeyi basitleştirir ve çalışanların işlerinin özüne odaklanmasını sağlar.
UniknameTM Connect, çok sayıda mevcut ürünle [28] entegre edilebilir, böylece işverenlerin güvenlik düzeylerini artırırken iş gücüne birleşik bir bağlantı arabirimi sağlamalarına olanak tanır. Şekil 4, UniknameTM Connect ile entegre edilebilecek çeşitli uygulamaları göstermektedir.
[2]https://www.unikname.com/en/partners/



Şekil 4: UniknameTM Connect: Dahili araç

3.4 UniknameTM C.A.R.E.: Salgını Anonim Olarak Bildiren Vatandaş

2020'nin başlarında, SARS-Cov-2 pandemisinin gelmesiyle birlikte birçok ülke vatandaşları için temaslı izleme uygulamaları geliştirdi. Amaçları, kullanıcıları enfekte kişilerle temas halinde olduklarında bilgilendirerek virüsün yayılmasını kontrol altına almaktı. Ancak bu strateji genel olarak iyi çalışmadı: çok az kişi uygulamaları yükledi ve kişi izleme çabasına katıldı [29]. Gizlilik endişeleri, bu uygulamaları yüklememek için en sık belirtilen ikinci nedendi [30, 31].

Aşılar yaygınlaştıkça, yeni uygulamalara yerleştirilmiş sağlık pasaportu etrafında yeni stratejiler geliştiriliyor. Soru şudur: Kişi izleme uygulamalarında karşılaşılan tuzaklardan nasıl kaçınılabilir? Bu yeni uygulamalar, hassas tıbbi verileri nasıl kullandıkları konusunda nasıl güven uyandırabilir? UniknameTM, SSI'nın yeni, gizlilik odaklı çözümlerin kalbi olması gerektiğine inanmaktadır.

UniknameTM C.A.R.E. dijital Covid-19 testi ve aşı tasdikleri sunar.

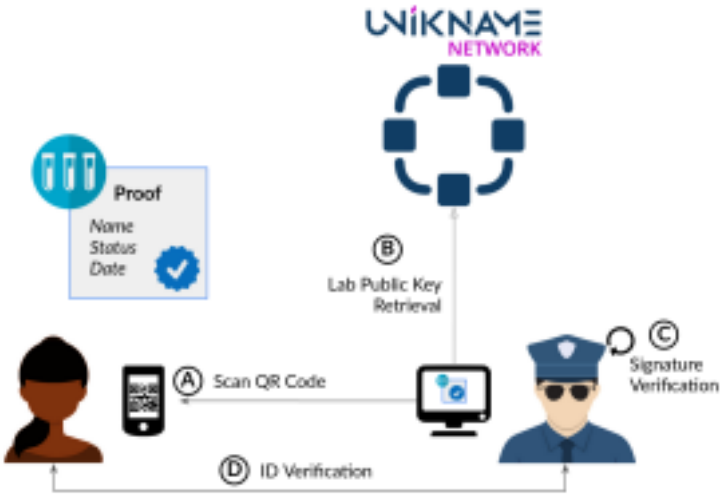
Aşı sertifikası ve sağlık kontrolü UniknameTM C.A.R.E ile COVID-19 test sonuçları veya aşı sertifikaları vatandaşın dijital kimliğinin bir parçasıdır. Dijital onaylar, sonuçları onaylayan veya aşıyı uygulayan sağlık yetkilileri tarafından imzalanır. Onaylar, otoritenin kendi UniknameID'si kullanılarak doğrulanabilir. Onaylar sahiplerinin uygulamasında tutulur ve izinleri olmadan paylaşılamaz, danışılamaz veya doğrulanamaz.

Kullanılabilirlik, benimsemeyi yönlendirmek için gerekli olduğu için burada bir odak noktası olmaya devam ediyor. UniknameTM C.A.R.E ile vatandaşlar, sağlık kontrolörlerinin onaylarını almak için tarayabilecekleri bir QR kodu oluşturur (Bkz. Şekil 5). Daha sonra UniknameTM Network'e danışarak geçerliliğini kontrol ederler.

Protokol yine tasarım gereği özeldir ve genel güven artar.

Sıfır bilgi kanıtlarıyla iyileştirilmiş gizlilik Bazı durumlarda, denetleyicinin, zaman eksikliği, izin eksikliği veya kişisel sağlık verilerini cihazlarında tutmama konusunda güvenilmemesi nedeniyle kimliği kontrol etmesine izin verilmez. Sıfır bilgi ispatını doğrulanabilir iddialarla

birleştirerek, süreci iyileştirmek ve vatandaşların sağlık durumlarını ve kimliklerini aynı imzada bağlamadan kanıtlamalarına izin vermek mümkündür.



Şekil 5: UniknameTM C.A.R.E: Sağlık kontrolü

DIF'den alınan BBS+ imzaları gibi yeni ortaya çıkan standartları kullanarak, kısmi mesajlarda imzalar doğrulanabilir. Bu, kullanıcıların ifşa etmek ve doğrulama için sunmak istedikleri özellikleri seçmelerine olanak tanır ve böylece gizliliği artırır.

3.5 UniknameTM Nisabı: Anonim, sansürsüz ve tartışmasız oylama

Her yıl şirket veya derneklerde genel kurullar toplanır ve çeşitli konularda oylama yapılır. UniknameTM Quorum ile bu süreç dinginlik ve sadelikle organize edilebilir. Her katılımcı veya hissedar kendi UniknameID'si ile oy kullanır. UniknameID'lerinden özellikle oy için yeni bir kimlik türetilir. Bu kimlik tamamen geri döndürülemez, yani hiç kimse kimliği orijinal UniknameID'ye kadar izleyemez. Seçmenler için anonimlik tamamlandı.
Oylar bir Merkle ağacında birleştirilir [32, 33]. Oylama bittiğinde ağacın kökü UniknameTM Network'e yazılarak seçimi onaylar. Bu işlemle seçmenler, Merkle ağacının kökünü kendi oyları da dahil olmak üzere kısmi bir daldan yeniden hesaplayabilir ve oylarının göz ardı edilmediğinden veya sansürlenmediğinden emin olabilirler. Sonuçlar deftere yazıldığı için değiştirilemez. Onlar tartışılmaz.

3.6 Diğer kullanım durumları

UniknameID etrafında çok daha fazla iş kullanım örneği düşünülebilir. Olasılıkların kapsamı bütün bir kitabı dolduracak kadar geniştir. İnsan tarafından okunabilen SSI ve DPKI bir araya geldiğinde, profesyonel bağlamlarda pek çok durumu çözebilir. Ek kullanım durumlarının kısa ve ayrıntılı olmayan bir listesi aşağıda verilmiştir.

- Güven Sertifikalarının teslimi;

• Kısıtlı alanlarda fiziksel erişim haklarının yönetimi;
• Bir emlak tapusu gibi bir avukatlık bürosunda noterlik işleminin onaylanması; • Doğrulanmış bir özgeçmiş almak için diploma sertifikası;
• Formasyonun reddedilemez imzası:
- kesin sayıda katılımcı için bir kursu faturalandırmak,

– to certify attendance to an exam.
• Güçlü kimlik doğrulama ile özel sohbet
• . . .

4 UniknameTM Ağı

UniknameTM projesinin hedefleri iddialı. Onlarla tanışmak için UniknameTM Ekibi kendi blok zincirini, UniknameTM Network'ü geliştirmeyi seçti. Bitcoin veya Ethereum gibi mevcut blok zincirleri, projeyi hayal edildiği gibi desteklemek için bazı yönlerden yoksundu. UniknameTM Network Livenet bir yıldan fazla bir süredir yayında3. İşte UniknameTM Ağının birkaç özelliği.

Uzmanlaşmış UniknameTM bir kimlik platformu oluşturmak için yola çıktı. Bu nedenle, merkezi olmayan tanımlayıcımız UniknameID için zincirin kalbinde yer almak önemliydi. Özel bir blok zincirine sahip olmak bize bunu sağlar. UniknameID, fikir birliği protokolüne gömülüdür. Bunların üretimi ve yaşam döngüsü, ağ için yapısal unsurlardır.
Ek olarak, uzmanlaşma, bir blok zinciri ve tek bir hedefin arkasında federe bir topluluk anlamına gelir: adlandırılmış, kolayca manipüle edilen, Kullanıcı Egemen Kimlikler. Kod bu amaca hizmet eder. Cemaat buna uyuyor. Bu amaca yönelik protokoldeki gelişmelerin ağdaki tüm aktörler tarafından kabul edilmesi daha olasıdır. Çekirdek kod, gerekli olmayan şeylerle şişirilmez. Zincir, yönetişim ve işleyişinde genel olarak daha verimlidir.
Özel bir blok zincirine sahip olmak, blok alanını ilgisiz uygulamalarla paylaşmak zorunda kalmamak anlamına da gelir. Bu, işlem entegrasyonu için daha kısa süre, daha iyi kullanılabilirlik ve daha düşük işlem ücretleri sağlar.

Çevre Dostu Tarihsel olarak, İş Kanıtı (PoW), fikir birliği seçimi yöntemidir. Hala oradaki büyük, genel blok zincirleri tarafından kullanılıyor. Sonuç olarak, bir bütün olarak blok zincirler genellikle karbon ayak izleri nedeniyle eleştirilir[34]. Yenilik, zamanımızın büyük zorluklarını hesaba katmalıdır. Özel bir blok zinciri geliştirmek, enerji açısından daha verimli olan bir fikir birliği protokolünün, yani Delegated Proof of Stake (DPoS) seçimini sağlar.

NFT uyumlu UniknameTM projesi bağlamında, merkezi olmayan tanımlayıcıların kendilerine ait

bir ömrü vardır. Onlar benzersiz. Bunlar, sahip olunan ancak kullanılmadıkları takdirde topluluğa iade edilebilen paylaşılan bir varlık havuzudur. Bu nedenle, kabul edilmesi ve kutlanması gereken geçmiş kullanıcıların geçmişini biriktirmek zorundadırlar.
NFT, bu davranışı temsil etmek için en iyi teknik seçim gibi görünüyor.

Mevcut çalışmayı temel alır UniknameTM Ağ Çekirdek protokolü ARK.io'yu temel alır. Bu, UniknameTM'nin güçlü bir yenilikçiler topluluğunun yanı sıra sağlam, açık kaynak kodlu, iyi denetlenmiş bir kod tabanından faydalanmasını sağlar. Bir çekirdek tabanı paylaşmak, UniknameTM Ağı ile birçok blok zinciri veya genişletilmiş Ark ekosisteminden ürün arasında yerleşik uyumluluk da sunar.

4.1 Uzlaşma

Konsensüs protokolleri, herhangi bir blok zincirinin temel yapı taşlarıdır. Bir blockchain, protokolü beklendiği gibi çalıştığında sağlıklıdır. Bu, işlemlerin bloklar halinde sıralandığı, zincire düzenli olarak yeni blokların eklendiği ve blok doğrulayıcıların merkezileştirme veya sansürü önleyecek kadar çeşitli olduğu anlamına gelir.
Konsensüsün kesin kuralları, UniknameTM Network topluluğu tarafından belirtildiği şekilde evrime ve değişikliklere tabidir.

[3]Uniname™ Network Livenet launched in May 2020

4.1.1 Temsil Edilen Hisse Kanıtı (DPoS)

Delegated Proof of Stake (DPoS), ağdaki diğer aktörlerin oylarına dayalı olarak yeni blokları onaylamak için az sayıda düğümün seçildiği bir fikir birliği protokolüdür. UniknameTM Network'te oy yerine destek terimini tercih edeceğiz. Oy genellikle uzun vadeli etkileri olan ayrı, planlanmış bir olaya atıfta bulunmak için kullanılırken, bir delegeyi destekleme eylemi süreklidir (yani, birden fazla seçim döngüsü için geçerlidir). Bir aktör, istediği zaman bir delege için destek vermeyi veya geri çekmeyi seçebilir.
Konsensüs protokolüne katılmak için aktörlerin, desteklemek veya temsilci olmak için aktif bir UniknameID'ye sahip olmaları gerekir.
DPoS, Proof of Work'ten çok daha az bilgi işlem gücü gerektirir. Destekçiler arasında tokenlerin yeniden dağıtımını teşvik eder. Bu sistemde, daha az miktarda tokena sahip aktörler demokratik seçim sürecine hala katılabilir. Benzer şekilde, büyük hesaplar, kendilerini temsilci olmaya gerek

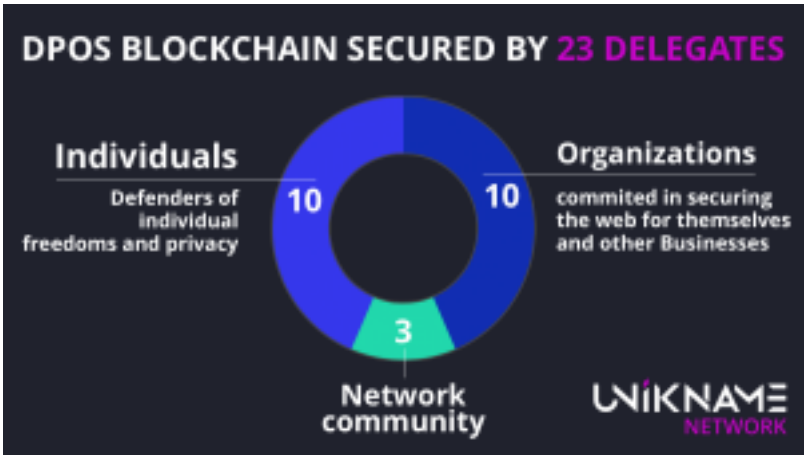
kalmadan ağın yönetimini etkileyebilir.
DPoS, belirli bir bloğu hangi düğümün doğrulayacağına önceden karar vererek, bir blok oluşturmak için gereken etkileşim miktarını önemli ölçüde azaltır. Bu, daha kısa blok süresi ve daha hızlı bir doğrulama süreci sağlar.

4.1.2 Destek ağırlığı

Temsilci desteklerinin nasıl hesaplandığı, farklı DPoS yinelemeleri arasında büyük farklılıklar gösterir. Ortak nokta elbette desteğin bir aktörün ağdaki hissesine, yani sahip olduğu token miktarına bağlı olmasıdır. UniknameTM Ekibi, kendi DPoS'unu tasarlarken aşağıdaki hedefleri göz önünde bulundurur:

1. **Aktör payı** - Bir oyuncunun desteğinin ağırlığı, ağdaki payından türetilmelidir.
2. H**esap başına bir oy** - Daha büyük paydaşların etkisini azaltmak için, bir hesap yalnızca bir delegeyi destekleyebilmelidir. Daha fazla delegeyi desteklemek için fonlar hesaplar arasında bölünebilir. Ancak bu, orijinal ağırlığı seyreltmelidir.
3. **Delege davranışı** - İyi bir hizmet sağlamayan delegeler (yani, düşük kullanılabilirlik, güncel değil, genellikle bir blok imzalama penceresini kaçırıyor vb.), ağı tehlikeye attıkları için protokolün bir parçası olarak cezalandırılmalıdır.
4. **Son zamanlardaki destek** - Topluluk içinde sürekli, aktif katılımı teşvik etmenin yanı sıra yeni aktörlerin daha eski, iyi kurulmuş delegelere karşı mücadele etme şansına sahip olmalarını sağlamak için, yakın zamanda yenilenen veya ödüllendirilen desteğin daha fazla ağırlığı olmalıdır.

2021'in sonuna kadar sürmesi öngörülen ağ Başlatma Aşaması sırasında, Livenet'te yalnızca birinci ve ikinci kurallar uygulanır. Daha iyi güvenlik, kullanılabilirlik ve topluluk katılımı için, konsensüs protokolü 2. Aşama sırasında üçüncü ve dördüncü kuralları içerecek şekilde güncellenecektir (bkz. Bölüm 5.2).
Üçüncü kurala göre, eksik blokları tutan bir delege, toplam desteklerinin kademeli olarak azaldığını görecektir. Davranış devam ederse, sonunda, bu temsilci desteği toplamına uygulanan ağırlık sıfıra ulaşacak ve böylece etkin ve geçici olarak katılımları yasaklanacaktır. Bu hesaplama için yalnızca en son bloklar dikkate alınacaktır. Bir süre sonra, delegenin davranışı düzelmiş olsun ya da blok doğrulama fırsatına sahip olmasın, eski kaçırılan bloklar puanlamalarını ve yasağı etkilemeyecek veya düşük puan geçerlilik kazanacaktır.



Şekil 6: UniknameTM Network'ün üç koleji

Dördüncü kurala göre, bir aktörün bir delegeye verdiği destek, destek işleminin hangi bloğa gönderildiğine göre ağırlıklandırılacaktır. Ne kadar yakın zamanda olursa, ağırlık o kadar yüksek olur. Örneğin, A ve B aktörlerinin her ikisinin de yüz tokenu varsa ve her ikisi de delege olarak kendilerini destekliyorsa, desteklerinin nihai ağırlığı, işlemi en son hangisinin gönderdiğine bağlı olacaktır.

4.1.3 Üç Delege Kolejleri

UniknameTM Network konsensüsünün bir özelliği, kolejleri kullanmasıdır. Blok zinciri üç tür UniknameID'yi destekler: birey, organizasyon ve ağ. Her bir UniknameID türünün arkasındaki aktörler çok farklı çıkarları savunuyor. Her grubun çıkarlarını adil bir şekilde temsil etmek için kolej kavramını tanıttık. (Bkz. şekil 4.1.3)

Her kolejin sabit bir temsilci kümesi vardır: bireyler için 10, kuruluşlar için 10 ve ağ varlıkları için 3. Belirli bir türde yeterli delege yoksa, koltuk tahsisleri bireyler ve kuruluşlar arasında aktarılabilir. Örneğin, yalnızca 5 kuruluş delege olarak kaydolursa, bireyler için kalan 5 koltuk kullanılabilir hale gelir ve 10 yerine 15 bireysel delege seçilir. Yeni bir kuruluş delege olarak kaydolduğunda, koleji için bir koltuk talep eder. Dolayısıyla bir sonraki seçimde gelen blokları doğrulamak için 6 kuruluş, 14 kişi ve 3 ağ kuruluşu olacak. Yeterince kişi delege olarak kaydedilmediğinde bunun tersi de mümkündür. Bu, 23 düğümün ağı her zaman güvence altına almasını sağlar.

Belirli bir UniknameID, yalnızca aynı koleje ait bir temsilci için oy verebilir: bireysel destek bireysel delegeleri türünde UniknameID, kuruluş destek organizasyonu delegelerinde UniknameID ve ağ destek ağı delegelerinde UniknameID.

Kolejler, DPoS blok zincirlerinin iki yaygın tuzağını, merkezileştirme ve kartelleştirmeyi azaltır. Ayrıca çatallanmaya karşı bir önlem oluştururlar.

4.2 Tokenlar

UniknameTM Ağının yerel simgesi $UNIK'tir. $UNIK tokeni, zincirdeki hizmetler için değiştirilir. token, kimlik platformunun ve hizmetlerinin çıkarlarına hizmet eder. Sonuç olarak, UniknameTM Network'ün tokenomikleri, platform olgunlaştıkça, proje popülerlik kazandıkça ve $UNIK'in likiditesi arttıkça gelişmeye ayarlanmıştır.

Ağın tokenlerinin her evrimi, UniknameTM Ağı için bir aşamaya karşılık gelir. Blok zinciri şu anda Başlatma Aşaması olan Aşama 1'dedir ve başlangıç bloğundan beri olmuştur.

Aşama 1'in amacı, yeni kullanıcıları çekerek, tüm hizmetlere erişimi garanti etmek için yeterli token üreterek ve minimum likidite sağlayarak ağın lansmanını hızlandırmaktır. Aşama 1'in sonu, bir token satışından hemen önce bir Token oluşturma etkinliği ile işaretlenecektir. Bu etkinliğin 2021'in sonunda yapılması planlanıyor. Bundan sonra ağ yavaş yavaş Aşama 2'ye geçmeye başlayacak.

Aşama 2, uzun vadede sorunsuz çalışması için yeterli token ve aktörün bir araya getirildiği UniknameTM Ağının olgun bir sürümünü temsil eder. Bu aşamada, $UNIK tokeni, bir ERC20 [35] sarmalayıcı kullanılarak bir DEx'te alıntılanacaktır.

Aşama 2, tokenlar dağıtıldıktan hemen sonra kotasyon piyasasındaki satış baskısını sınırlamak için hak kazanma kurallarını içerir. Kurallar, token alıcısının profiline bağlıdır. Hak kazanma kurallarıyla ilgili ayrıntılar, token satışının bir parçası olarak iletilecektir.

4.2.1 Tedarik

$UNIK tedarik üretimi, ağın mevcut aşamasına bağlı olarak değişecektir.

Aşama 1 (Fırlatma Aşaması) Yaratılışta 10 milyon $ unik üretildi. O zamandan beri ve 1. Aşamanın tamamı boyunca, blok ödülü blok başına 2 $UNIK olarak belirlendi. Bu $UNIK, bloğu doğrulayan temsilciye verilir. Yaklaşık her 8 saniyede bir yeni bir blok oluşturulur. Delegeler ayrıca boş bloklar için ödüllendirilir.

Ek olarak, benimsemeyi teşvik etmek için bir UniknameID oluşturulduğunda öncü ödüller basılır ve dağıtılır:

- birey türünde bir UniknameID basmak için 100 $UNIK;
- UniknameID türünde bir organizasyon basımı için 10.000 $UNIK;
- Ağ türünde bir UniknameID basımı için 1.000.000 $UNIK.

Öncü ödülünden alınan tokenlar, UniknameID'nin sahibi ile bir pazarlama havuzu arasında dağıtılır. Bu, ilk blok zinciri hizmetlerinin çalışmasına izin verir. Bugün4, öncü ödülleri kullanılarak yaklaşık 6 milyon $ unik üretildi.

Aşama 2 Aşama 2'de öncü ödülleri artık basılmıyor. Bir Token Üretim Etkinliği, toplam $UNIK arzını en az 400 milyona getirecektir.
Blok ödülü blok başına 1 $UNIK'e düşürülecek. Bu, yılda 3.942.000 yeni birim dolara veya 4 milyonun biraz altında. Bu nedenle enflasyon seviyeleri yıllık %1'in altında tutulacaktır. Bu düşük enflasyon, örneğin kayıp anahtarlar nedeniyle kaybolan tokenları telafi eder. Ayrıca blok ödülleri, delegeleri boş blokları doğrulamaya teşvik eder. Bu, işlem hacminden bağımsız olarak blok oranını sabit tutar, böylece güvenlik ve güvenilirliği artırır.
Böyle düşük bir enflasyon oranı ile, Faz 2 arzı sabit olarak kabul edilebilir. **4** 6 Temmuz 2021

Arz paylaşımı $UNIK arzı üç kısma ayrılır:

• **Topluluk** - Tedarikin bir kısmı topluluğa aittir. Bu tokenlar, diğer şeylerin yanı sıra, bir kamu veya özel token satışı yoluyla elde edilebilir.

• **Şirket** - Tedarikin bir kısmı UniknameTM projesinin arkasındaki şirkete aittir. UniknameTM ekosisteminin gelecekteki gelişimini sağlamak için bu gereklidir. Şirket payı özellikle pazarlama amacıyla kullanılacaktır. Bu tokenların bir kısmı da likidite havuzlarında kilitlenmek içindir.
• **Rezerv** - Rezerv, UniknameTM projesinin arkasındaki şirkete aittir. Kilitlidir ve yalnızca ağ saldırısı gibi sorunların üstesinden gelmek için topluluğun onayı ile açılabilir.

Token satışının bir parçası olarak daha ayrıntılı bir token dağıtımı kamuya açıklanacak.

4.2.2 Token yardımcı programı

$UNIK, UniknameTM Network blok zincirinde kullanılan bir yardımcı program tokenidir. $UNIK hizmet belirteçları, UniknameID sahiplerinin SSI işlemlerini etkinleştirmek ve SSI hizmetlerine erişmek için ihtiyaç duyduğu SSI kredileridir. Tüm UniknameTM hizmetleri, etkin bir UniknameID gerektirir. Tek başına $UNIK, yani UniknameID olmadan, çok kısıtlı bir yardımcı programa sahiptir. Yalnızca yeni UniknameID ve ilgili NFT'yi vermek için kullanılabilirler.
UniknameID, onları kontrol edebilen tek varlık olan benzersiz bir sahibine sahiptir. UniknameTM Ağı üzerinde bir NFT ile temsil edilirler. UniknameID ve NFT temsilleri temel olarak üç şekilde kullanılır:

• bireyler veya kuruluşlar için merkezi olmayan tanımlayıcılar olarak adlandırılmış; • bir DPKI'ye hizmet eden güven sertifikaları olarak;
• SSI servis sağlayıcı kimliği olarak.
UniknameID sahipleri aşağıdakiler için $UNIK kullanabilir:

SSI operasyonlarını etkinleştirme SSI hizmetlerini entegre etmek ve etkinleştirmek için (Bölüm 3'te açıklandığı gibi), işletmelerin bir birim harcaması gerekir. $UNIK, hem kurulum hem de çözümün sürekli kullanımı için gereklidir.

SSI hizmetlerine erişim veya sağlama Entegrasyonlarından sonra (örneğin müşterilerin web sitelerinde veya uygulamalarında), SSI hizmetlerinin çalışması için $UNIK tokenleri gerekir. Maliyetin kullanıcıları tarafından mı yoksa kendisi tarafından mı karşılanacağına karar vermek her işletmeye kalmıştır. Bu şekilde kullanıldığında $UNIK SSI kredisi olarak değerlendirilebilir. Her SSI hizmet sağlayıcısı, bir hizmeti kullanmak için gereken SSI kredisi miktarını (yani $UNIK) belirler. Krediler, sunulan hizmetten önce sağlanmalıdır. Hizmet sağlayıcılar, bunun nasıl gerçekleştiğine ilişkin kendi yönetim uygulamalarını belirler.

UniknameID edinimi UniknameID NFT, $UNIK tokenları karşılığında NFT Factory adlı özel bir hizmet sağlayıcı tarafından verilir. Bir UniknameID'nin fiyatı, büyük ölçüde uzunluğuna, aynı zamanda türüne ve ücretsiz mi yoksa premium mu olduğuna bağlıdır.

Kişiler veya kuruluşlarla ilişkili verileri güncellemek İster kişi ister kuruluşlar olsun, UniknameID sahipleri, adlandırılmış tanımlayıcılarını daha sonra blok zincirinde herkese açık olarak erişilebilir olacak bir dizi mülkle ilişkilendirmeye karar verebilir. Zincir üstü özellikleri ayarlamak ve güncellemek için $UNIK tokenleri gerekir.
Sertifikalı zincir dışı mülkler, SSI hizmetleri aracılığıyla elde edilebilir.

UniknameID'nin yaşam döngüsünün yönetilmesi UniknameID'nin düzenli olarak canlı tutulması gerekir (bkz. bölüm 2.2.3). Bu işlemler için gereken $UNIK miktarı, UniknameID'nin türüne, uzunluğuna veya türüne (ücretsiz veya premium) bağlıdır.

SSI ödülleri UniknameTM'nin SSI çözümlerini kullanmaya karar veren işletmeler, bazı SSI işlemleri gerçekleştirdiklerinde kullanıcılarını $UNIK ile ödüllendirebilir, örn. bir karara oy vermek.

Destekleyen ağ delegeleri $UNIK, UniknameTM Ağı fikir birliğinin merkezinde yer alır (bkz. Bölüm 4.1). $UNIK'i edinmek ve biriktirmek, aktörlerin Ağ yönetiminde aktif rol almalarına olanak tanır. Oy verme gücü, bir destekçinin sahip olduğu $UNIK miktarıyla büyük ölçüde bağlantılıdır.

UniknameID yönetiminden sorumlu kuruluş, yarı merkezi olmayan bir yapıya sahiptir. UniknameTM bunu kontrol eder, ancak bu varlığın rolüyle veya sağladığı hizmetten verilen tokenlerin dağıtımıyla ilgili büyük değişiklikler topluluk anlaşması gerektirir. Aşama 2'den başlayarak, bu fonların bir kısmı topluluğa işlem ücretleri olarak yeniden dağıtılacaktır. Belirli bir hizmet için işlem ücretleri, fiyatıyla orantılı olacaktır.

Token likiditesi UniknameTM kimlik platformundan çözümler entegre eden her şirket, müşterileri, işbirlikçileri vb. için UniknameID'nin verilmesini gerektirir. Tüm UniknameID'nin canlı tutulması gerekir. Blok zincirinin salt okunur kullanımıyla bile, UniknameID yaşam döngüsü tarafından token likiditesi sağlanır.

Kendi kendini finanse eden geliştirme Ağ tipi UniknameID ve özellikle delegeleri özeldir. UniknameTM tarafından kontrol edilirler ve değiştirilemezler. Rolleri, ağın çıkarlarını fikir birliği içinde temsil etmek ve korumaktır. Böyle üç delege var. Böylece işlem ücretlerinin %12'si UniknameTM tarafından tahsil edilir. Bu fonlar, ağı korumak ve UniknameTM Ağının gelişimini garanti etmek için kullanılır.

4.3 Açıklayıcı bir örnek: @CrazyShop

SSI hizmetleri bağlamında $UNIK tokenlarının nasıl kullanıldığını ve değiş tokuş edildiğini göstermek için, Crazy Shop adlı bir işletmeyi ve müşterilerinden biri olan Bob'u örnek alıyoruz. Aşağıdaki örneklerin tümü için bir ön koşul olarak, hem Crazy Shop hem de Bob, sırasıyla organizasyon ve bireysel tipte kendi UniknameID, @CrazyShop ve @bob'larını aldı ve etkinleştirdi. Ayrıca, delege olarak, piyasadan satın alarak veya başka herhangi bir yolla $UNIK tokenları da edindiler.
Aşağıdaki örneklerin her biri farklı bir SSI hizmet sağlayıcısını içermektedir.

Örnek 1: Giriş Crazy Shop, güçlü bir kimlik doğrulama yöntemi sunarken hassas parola veritabanından kurtulmak için web sitesine UniknameTM Connect'i kurmak istiyor. Burada SSI hizmet sağlayıcısı, Merkezi Olmayan Kimlik Doğrulama sağlayıcısıdır.

İlk olarak Crazy Shop, Merkezi Olmayan Kimlik Doğrulama sağlayıcısına kaydolur ve sağlayıcıya özel kurulum adımlarından geçer. Bu durumda kurulum, Crazy Shop'un web platformu URL'sinin "https://www.crazyshop.com" URL Denetleyicisi adlı bir yardımcı hizmet sağlayıcı tarafından doğrulanmasını gerektirir. Doğrulama, belirli bir miktarda $UNIK gerektirir ve zincir üzerinde URL'nin yayınlanmasını içerir.
Kurulum tamamlandıktan sonra Crazy Shop, Merkezi Olmayan Kimlik Doğrulama sağlayıcısına SSI kredileri (yani $UNIK tokenları) gönderir. Her hizmet sağlayıcı, müşterilerini kendi şartlarına

göre yönetir ve kendi oranlarını belirler. Burada, Merkezi Olmayan Kimlik Doğrulama sağlayıcısı bağlantı başına ücret alır. Crazy Shop, hizmet sunulmadan önce hesabını bir sağlayıcıya yatırmalıdır. Crazy Shop'un Merkezi Olmayan Kimlik Doğrulama sağlayıcısıyla olan bakiyesi çok düşerse hizmet garanti edilemez.

Bob şimdi Crazy Shop platformunu ziyaret ediyor ve oturum açmak istiyor. Merkezi Olmayan Yetkilendirme sağlayıcısına yönlendiriliyor. Bob tüm adımlardan geçiyor (UniknameID'sini giriyor ve uygulamasında bağlantı isteğini doğruluyor). Merkezi Olmayan Kimlik Doğrulama sağlayıcısı, Bob'un kimlik doğrulamasını onaylamak için UniknameTM Network'ten okur, doğrular ve Bob'u Crazy Shop'a yeniden yönlendirir. Merkezi Olmayan Kimlik Doğrulama sağlayıcıları, Crazy Shop'un sağlayıcıya özel hesabından SSI kredilerini kaldırır.

Crazy Shop, UniknameTM Connect'i kullanmayı bırakmak istediğinde, kullanılmayan tüm SSI kredileri iade edilir.

Örnek 2: Onaylı resimler Kimlik doğrulamadan sonra Crazy Shop, platformunda ikinci bir SSI hizmetini etkinleştirmek istiyor: resim sertifikası. Bu, kullanıcıların fotoğraf yüklemesine ve fotoğrafın belirli bir UniknameID'nin sahibi tarafından yüklendiğinden emin olmasına olanak tanır. Bu örnekte, SSI hizmet sağlayıcısı, Veri Sertifikasyon sağlayıcısıdır.

İlk olarak, yine Crazy Shop, Veri Sertifikasyon sağlayıcısına kaydolur ve hizmeti ayarlar. Kurulum, $UNIK cinsinden bir ücret gerektirir. Ancak bu sefer Crazy Shop'un sağlayıcıya özel bir hesaba kredi vermesi gerekmez. Hizmetin maliyeti Crazy Shop kullanıcıları tarafından karşılanacaktır.

Bob bir resim yüklemek istiyor. Crazy Shop'un web platformuna gider ve dosyayı yükler. Başarılı bir yüklemeden sonra Crazy Shop, sertifikasyon için Veri Sertifikasyon sağlayıcısıyla iletişime geçer. İstekler, Bob'un UniknameID'sini içerir.

Bob, mobil uygulamasında belgenin kendisine ait olduğunu ve belgenin onaylanmasını istediğini doğrulamak için bir istek alır. Bu istek, işlemin Bob tarafından ödenecek $UNIK cinsinden maliyetini içerir. Bob talebi kabul ederse, kripto hesabından $UNIK alınır ve belge onaylanır. Bob reddederse, hizmet iptal edilir.

Örnek 3: Ödüller Crazy Shop, kullanıcılarını müşteri memnuniyeti anketlerini yanıtlamaya motive etmek için onlara biraz $UNIK teklif etmek istiyor. Burada SSI hizmet sağlayıcısı Ödüllendirme sağlayıcısıdır.

Crazy Shop, hizmeti kurmak için bir miktar unik harcıyor. Ayrıca, bir ödülü neyin tetiklemesi gerektiğini ve ödülün ne kadar yüksek olması gerektiğini bildirmek için hizmeti parametreleştirir. Crazy Shop daha sonra SSI kredileriyle, yani $UNIK tokenlarıyla sağlayıcıya özel bir hesaba kredi verir. Kredilendirilen miktar, hizmetin yanı sıra dağıtılacak ödülleri de hesaba katmalıdır.

Bob, müşteri memnuniyeti anketini doldurmasını isteyen bir e-posta alır. Ankete devam ediyor. Bunu tamamladıktan sonra Bob, Ödüllendirme sağlayıcısına yönlendirilir. Burada Bob, @bob

ödülü ile kredilendirilmesi gereken UniknameID'yi girer. Ödüllendirme hizmeti, Crazy Shop'un sağlayıcıya özel hesabından ödül ve hizmet maliyetini kaldırır. Ödül doğrudan @bob'a gönderilir.

Crazy Shop, Ödüllendirme hizmetini kullanmayı bırakmak istediğinde, kullanılmayan tüm SSI kredileri iade edilir.

4.4 Teşvik modeli

UniknameTM, UniknameTM kullanıcılarını işletmelere UniknameTM'yi önermeye teşvik etmek için Ekosistem Geliştirme fonlarını kullanmayı amaçlamaktadır. Ambassador programı, önerilen platformlarda SSI hizmetleri uygulandığında UniknameTM sahiplerini ödüllendirecek.

5 Yol Haritası

5.1 Proje durumu

Bu teknik incelemede açıklanan proje, iki yılı aşkın bir inovasyona dayanmaktadır. Bu bir kuruntu değil, sağlam bir projedir, mevcut çalışma üzerine inşa edilmiştir. UniknameTM'nin arkasındaki ekip, iddialı hedeflerine ulaşmak ve projeyi elde edilen başarıların gösterdiği gibi yürütmek için tüm anahtarlara sahiptir.

5.1.1 UniknameTM Ağ Canlı Ağı

Livenet adı verilen UniknameTM Ağı ana ağı, Mayıs 2020'den beri tam olarak çalışır durumda. Temel kodu Açık Kaynak'tır. Lansmanından bir yıl ve 4.191.353 blok sonra, ağ 7371 UniknameID

5'i sayıyor ve her gün daha fazlası oluşturuluyor.
Ağın mevcut durumu, gezgini [36] aracılığıyla herkese açık olarak erişilebilir. Gelişimini takip etmek için UniknameTM Network Core github deposunu [37] da kontrol edebilirsiniz.

5.1.2 Patentli bir teknoloji

UniknameID, insan tarafından okunabilir kimlikleri nedeniyle özel DID'dir. Hem özel hem de kişisel olan bir kullanıcı adı seçmek merkezi ayarlarda bariz görünüyor, ancak merkezi olmayan dünyada bu oldukça karmaşık. UniknameTM bu konuda patent almış olmaktan gurur duyar.

5.1.3 Merkezi Olmayan Kimlik Temeli ve DID yöntemleri

UniknameTM, ademi merkeziyetçiliğin kimliğin geleceği olduğuna gerçekten inanıyor. Bu nedenle, DID'nin yayılmasına ve ekosistemi desteklemeye kararlıyız. Standardizasyon ve birlikte çalışabilirlik bu çabanın anahtarıdır. Bu nedenle DIF üyesiyiz. Zaten vakıf tarafından tanınan iki DID yöntemimiz var [13, 14].

5.1.4 İlk kullanım durumları: cüzdan ve UniknameTM Connect

Kullanım durumlarımızdan ikisi zaten geliştirildi ve denemeniz için hazır: $UNIK cüzdan ve UniknameTM Connect (bkz. bölüm 3.3). Bu kullanım durumları My UniknameTM Uygulaması [25] ile test edilebilir. My UniknameTM Uygulaması Mayıs 2020'den beri çalışıyor ve şu anda 1.416 sürümünde.
Süreci test etmek için, UniknameTM SSI cüzdanını, My Unikanme Uygulamasını kurmalı, UniknameID'lerini almalı ve ortaklarımızdan birinin web sitesine giriş yapmalıdır 6.

5.1.5 Denetlenmiş bir kod tabanı

Bu Livenet çekirdeği ve kimlik doğrulama protokolü, 2021 yılında güvenlik denetimlerinde uzmanlaşmış bir şirket tarafından başarıyla denetlenmiştir.

5 Veriler 18 Haziran 2021'de çıkarıldı
6 https://www.unikname.com/en/partners/

UniknameTM Yol Haritası

6. Sonuç

UniknameTM, Kullanıcı egemen kimlikler vaadine inanır. SSI, kullanıcılar ve hizmet sağlayıcılar için büyük bir fırsattır. Dijital dünyaya güvenin yanı sıra kontrol ve bağımsızlığı geri getirecektir. UniknameTM, güvenlik, kullanılabilirlik ve pratik kullanım durumlarına odaklanan merkezi olmayan bir kimlik platformu geliştirerek bu değişim boyunca işletmelere eşlik etmek istiyor.

Bu proje, adlandırılmış tanımlayıcılar önererek, SSI'nın yeni zirvelere ulaşmasını ve bir web sitesinin alan adı kadar kolay bir şekilde dijital alanın dışında paylaşılmasını sağlar. UniknameTM kendi blok zincirini, UniknameTM Network'ü geliştirdi ve bu tek hedefin arkasında büyüyen bir topluluğu birleştirdi. Özel bir blok zinciri olarak UniknameTM Network, projeyi ve gelecekteki

gelişimini desteklemek için mükemmel bir altyapıdır.

UniknameTM, dijital kimliklerin kendi başlarına var olabileceğine inanmaktadır. Çoğu SSI uygulaması, fiziksel olanı dijitale aktarmaya odaklanır. Bu, adreslere, kimlik belgelerine, ... Ancak, bir tüzel kişilik tarafından sertifikalandırma gerektirmeyen dijital kimliklere yönelik başka uygulamalar da vardır.

SSI birden fazla kişiye uygulanabilir. IoT'nin yükselişi ile bağlantılı cihazlar kitlesel olarak çevrimiçi hale geliyor. Endüstriyel uygulamalardan akıllı şehirlere kadar tüm bu cihazların ele alınması gerekiyor. Aynı şekilde SSI, tedarik zinciri takibi, envanter yönetimi, evcil hayvan tanımlama vb. alanlarda uygulama bulabilir.

Dijital kimlik yönetiminin ademi merkeziyetçiliği, birlikte inşa etme ve birlikte çalışabilirlik fırsatı sunar. Hizmetler arasında kesintisiz veri hareketliliği sağlar. Ayrıca, paylaşılan varlıklar ve altyapılar sağlayarak işbirliğinin kurulum maliyetini düşürür. Bu, merkezileştirmenin hizmet sağlayıcılara yüklediği yükü hafifletir: sorumluluk, güvenlik, kullanılabilirlik, ölçeklenebilirlik, ...

UniknameTM Connect, UniknameTM SSI platformunun ilk kullanım durumudur. Basit, şifresiz, evrensel, 2FA çözümü ile web platformları ve uygulamaları sağlar. Çözüm, müşterilerin kimliğini doğrulamak veya ortak çalışanlar için bağlantı arayüzlerini uyumlu hale getirmek için kullanılabilir. Her iki durumda da, oturum açma yalnızca bir akıllı telefon ve bir UniknameID gerektirir. UniknameTM Connect, her gün yüzlerce kişi tarafından İnternet erişimini güvence altına almak için kullanılmaktadır.

Bugün, UniknameTM merkezi olmayan kimlik platformu, İnternet bağlantılarının kimlik doğrulamasının ötesine geçiyor. Kimlikleri ve uygulamalarını oluşturmak ve yönetmek için araçlar sağlar: oylama, belge doğrulama, katılım sertifikası, iddia beyanı, vb. Modüler tasarımı sayesinde platform, özel modülleri uygun şekilde reddederek ve birleştirerek genişletilebilir bir dizi kullanım durumunu ele alacak şekilde inşa edilmiştir. yeni gereksinimler.

Referanslar

[1] T. I. EU, “Integrity watch - eu lobbyists.” https://www.integritywatch.eu/ organizations. Last Checked July, 12th 2021.

[2] T. Verge, “Twitter censored tweets critical of india’s handling of the pandemic at its government’s request.” https://www.theverge.com/2021/4/24/22400976/ twitter-removed-tweets-critical-india-censor-coronavirus, Apr. 2021. Last checked: July, 12th 2021.

[3] C. Michelle, “World password day,” *Blog Dashlane*, May 2018. Last checked July 9, 2021.

[4] H. Alex, “Google suffers worldwide outage with gmail youtube and other services down,” *The Guardian*, December 2020. Last checked July 9, 2021.

[5] A. Tobin and D. Reed, “The inevitable rise of self-sovereign identity,” *The Sovrin Foundation*, vol. 29, no. 2016, 2016.

[6] A. M¨uhle, A. Gr¨uner, T. Gayvoronskaya, and C. Meinel, “A survey on essential components of a self-sovereign identity,” *Computer Science Review*, vol. 30, pp. 80– 86, 2018.

[7] R. W. Shirey, “Internet security glossary,” RFC 4949, IETF, Aug. 2007.

[8] M. Sporny, D. Longley, and D. Chadwick, “Verifiable credentials data model 1.0: Ex pressing verifiable information on the web,” tech. rep., World Wide Web Consortium (W3C), 2019.

[9] W3C, “Use cases and requirements for DID.” https://www.w3.org/TR/ did-use-cases/. Last checked July 9, 2021.

[10] Proofpoint, “State of the fish,” tech. rep., Proofpoint, 2020.

[11] Risk Based Security, “2020 Q3 Report - Data Breach QuickView,” techreport, Risk Based Security, 2020.

[12] digitalguardian, “Whats cost data breach.” https://digitalguardian.com/blog/ whats-cost-data-breach-2019, December 2019. Last checked July 9, 2021.

[13] S. Dram´e-Maign´e, “Unikname did specification,” tech. rep., Space Elephant, 2021.

[14] S. Dram´e-Maign´e, “uns.network did method specification,” tech. rep., Space Ele phant, 2020.

[15] K. Hamilton-Duffy, R. Grant, and A. Gropper, “Use cases and requirements for de centralized identifiers.” https://www.w3.org/TR/did-use-cases/, Mar. 2021. Last checked July 9, 2021.

[16] O. Foundation, “Welcome to openid connect.” https://openid.net/connect/, 2021. Last checked July 9, 2021.

[17] D. A. W. Group, “Authentication working group.” https://identity.foundation/ working-groups/authentication.html, 2021. Last checked July 9, 2021.

[18] DIF, “Wallet and credential interactions.” https://identity.foundation/ wallet-and-credential-interactions/, 2021. Last checked July 9, 2021.

[19] DIF, “Using openid connect with decentralized iden tifiers.” https://medium.com/decentralized-identity/ using-openid-connect-with-decentralized-identifiers-24733f6fa636, May 2019. Last checked July 9, 2021.

[20] Unikname, “Uniknames authentication protocol au dited with success.” https://www.unikname.com/en/ uniknames-authentication-protocol-audited-with-success/, 2021. Last checked July 9, 2021.

[21] Unikname, “Uns released as open-source.” https://www.unikname.network/ uns-released-as-open-source/. Last checked July 9, 2021.

[22] ARK.io, “The simplest way to blockchain.” https://ark.io. Last checked July 9, 2021.

[23] IBM, “Institute for business value 2017,” 2017.

[24] IBM, “Security, cost of a data breach report 2020,” 2020.

[25] Unikname, “My unikname app.” my.unikname.app, 2021. Last checked July 9, 2021.

[26] Baymard, “44 cart abandonment rate statistics.” https://baymard.com/lists/cart-abandonment-rate, 2021. Last checked July 9, 2021.

[27] Unikname, “Unikname website.” unikname.com. Last checked July 9, 2021.

[28] Unikname, “Unikname integrations.” https://help.unikname.com/, 2021. Last checked July 9, 2021.

[29] D. Lewis, “Why many countries failed at covid contact-tracing — but some got it right,” June 2021. Last checked July 9, 2021.

[30] U. of Manchester, “Digital distrust: Skepticism towards covid-19 contact tracing apps,” May 2020. Last checked July 9, 2021.

[31] W. Simon N, C. J. Armitage, T. Tampe, and K. Dienes, “Public attitudes towards covid-19 contact tracing apps: A uk-based focus group study,” May 2020. Last checked July 9, 2021.

[32] R. C. Merkle, “Protocols for public key cryptosystems,” in *IEEE Symposium on Security and privacy*, vol. 122, 1980.

[33] S. Dram´e-Maign´e, “An introduction to ... merkle trees.” https://forum.unikname.com/t/an-introduction-to-merkle-trees/747, 2020.

[34] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. B¨ohme, “Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency,” in *The economics of information security and privacy*, pp. 135–156, Springer, 2013.

[35] E. Y. Yilmaz, S. Richards, A. Gontijo, and R. Cordell, “ERC-20 Token Standard.” https://ethereum.org/en/developers/docs/standards/tokens/erc-20/, Apr. 2021. Last Checked: August 24th, 2021.

[36] U. Team, “Unikname newtork explorer.” https://explorer.unikname.network/. Last checked July 9, 2021.

[37] U. Team, “Unikname network github repository.” https://github.com/unik-name/typescript-sdk/. Last checked July 9, 2021.