[**Özet 3**](#_Toc520793748)

[**Arka Plan 4**](#_Toc520793749)

[Kimliğin Kökenleri 4](#_Toc520793750)

[Ulusal Vatandaşlık Numaraları 5](#_Toc520793751)

[Kimlik Karaborsası 5](#_Toc520793752)

[Kimlik Hırsızlığı ve E-Ticaret 6](#_Toc520793753)

[Mevcut Kimlik Formları 6](#_Toc520793754)

[Standart Olmayan Belgeleme 7](#_Toc520793755)

[Devlet Blockchain Girişimleri 8](#_Toc520793756)

[**Snowflake’e Giriş** 9](#_Toc520793757)

[Tokenize Bir Kimlik 9](#_Toc520793758)

[Kimlik Doğrulama 10](#_Toc520793759)

[Snowflake Metadata 10](#_Toc520793760)

[Snowflake’de Hydro Tokenlar 12](#_Toc520793761)

[Açık Yapı/Çerçeve 13](#_Toc520793762)

[**Snowflake: Teknik Detaylar** 13](#_Toc520793763)

[Kullanıcılar 13](#_Toc520793764)

[Çözücüler 13](#_Toc520793765)

[Doğrulayıcılar 13](#_Toc520793766)

[Ticari İşletmeler 14](#_Toc520793767)

[Snowflake Akıllı Sözleşmeleri 14](#_Toc520793768)

[Snowflake API ve Hydro Mobil App 16](#_Toc520793769)

[ERC-721 Kontrat Standard’ına Ayna Tutmak 16](#_Toc520793770)

[**Finansal Hizmetlerdeki Yansımaları** 17](#_Toc520793771)

[Evrensel Hesap Katılımı [Universal Account Onboarding] 17](#_Toc520793772)

[Doğrulayıcı Derecelendirme Sistemi 18](#_Toc520793773)

[Makine Öğrenimi Doğrulama Standardı 18](#_Toc520793774)

[Belge ve Sözleşme Doğrulama Standardı 18](#_Toc520793775)

[Ödeme Doğrulama Standardı 18](#_Toc520793776)

[Sahtecilikle Mücadele POS dApp’leri 18](#_Toc520793777)

[Küresel Kredi Puanlaması 19](#_Toc520793778)

[**Riskler** 19](#_Toc520793779)

[**Sonuç** 20](#_Toc520793780)

[**Kaynakça** 21](#_Toc520793781)

# **Özet**

***İngilizceden Çeviren: M. Talha ALTINKAYA***

Hydro’nun misyonu finansal hizmetler için kamuya açık bir merkez olmak ve merkezi olmayan [decentralized] yeni bir küresel ekonomiyi güçlendirmektir. Bu ekosistem, API'larla bağlantılı finansal uygulamalar tarafından kullanılabilecek standart akıllı sözleşmelerden oluşmaktadır. Bu standartlaştırılmış akıllı sözleşmeler ve API bağlantıları, firmaların blockchain geliştiricilerini işe alım gereksinimini azaltır ve mevcut sistemlere merkeziyetsizlik eklemelerine izin verir.

Mali ekosistemin çekirdek bileşenlerinden biri, kimlik ve kimlik yönetimi nosyonudur. Hesap açma, işlemler, ödemeler ve trilyonlarca dolarlık global finansal faaliyet için güvenlik yaratmak hayati önem taşımaktadır. Dijital ticaretin büyümesiyle, kimlik yönetimi gelecekteki ekonomi için daha da önemli hale gelir.

Bu whitepaper’da, finansal hizmetlerdeki kimlikler için Snowflake adını verdiğimiz kamusal ve merkeziyetsiz blockchain ile güçlendirilmiş yeni bir paradigma öneriyoruz. Kullanıcılar Snowflake kimliğine sahip olarak, değişmezler[immutable] ve doğrulanabilirler. Her bir Snowflake kimliği, kullanıcının mobil cihazında bulunan ve blok zincirindeki benzersiz bir ID'ye bağlı olan kartografiye bağlıdır, yerleştirilmiştir. Bu kimlik, kullanıcının takdirine bağlı olarak üçüncü taraflarla paylaşılabilir ve Hydro’nun gelecekteki gizlilik yönetimi protokolü için temel oluşturur.

Bu önerilen kimlik platformu, birden çok sorunu çözmeye yardımcı olabilir:

1. Kağıt esaslı kimlik yönetimi şu anda pahalıdır ve hırsızlık ile hacklenmeye eğilimlidir.
2. Dark web çalınmış kimlikler için artan bir karlılığa sahiptir.
3. Kimlik yönetimi için küresel açık standartlar yoktur ve özel blockchain girişimleri sorunu daha da kötüleştirmektedir.
4. E-ticaret ve dijital bankacılık giderek artan bir şekilde şirketlerin kullanıcılarının kimliklerini doğrulamasını zorlaştırmaktadır.
5. Gelişmekte olan ekonomiler, cep telefonlarının artan kullanımının kimlik oluşturma ve yönetimindeki avantajlarından yararlanamamıştır.

Hydro’nun yarattığı Snowflake, özel ve bağımsız KYC standartlarına uyan, milyarlarca insanın sahip olduğu kişisel kimliklere sahip olmak ve onları güvence altına almak için küresel bir standart oluşturabilir. Bu anlık hesap bütünleştirme durumu, küresel kimlikler, pasaportlar ve Hydro Raindrop ile kombine edildiğinde, kredi kartı ve banka dolandırıcılığı sıfıra yakın olacaktır.

# **Arka Plan**

## **Kimliğin Kökenleri**

İlk Whitepaper’ımızda, bir teknoloji ekosistemindeki kullanıcıların kurallara uygun kimlik doğrulaması ihtiyacını incelemiştik. Fakat kimlik doğrulaması yapmak için tanımlanabilir hiçbir şey yoksa, kimlik doğrulama yeterli değildir. Bu whitepaper’da finansal hizmetlere uygulanabilecek daha iyi bir kimlik yönetimi yapısı için acil olan bir ihtiyacı inceleyeceğiz. Kamusal bir blockchain’in kimliği değişmez/sabit ve standart hale getirerek bu puzzle’daki kaybolmuş parçayı nasıl sağlayabileceğini keşfetmeden önce daha temel bir soruyu ele alalım: Kimlik nedir ve nereden geliyor?

Bilim adamları en temel kimlik biçimleri olan isimlerin, belki de insanlar konuşma yeteneği kazanır kazanmaz başladığından yola çıkarak yazılı kelimelerden daha önce olduğuna inanmaktadır. Yunuslar gibi diğer memeli hayvanların da bir varlığın diğerine karşı isimlendirme aracı olarak işaret ıslıklarını kullanarak “kimlikler” oluşturduğuna dair bile ikna edici kanıtlar vardır. Tıpkı insanlarda olduğu gibi, bu kimlikler memeliler arasındaki sıkı komünal ilişkilerin kurulmasına yardımcı olur.

Hükümetlerin isimleri resmi olarak doğum belgeleri yoluyla takip etmesi görece modern bir plandır. Yıllar boyunca doğumlar ve isimlendirme çoğu batılı toplumda kilisenin yerine getirdiği bir şeydi. 1800’lerde ABD’ye 30 milyon göçmenin geldiği göç dalgası sırasında reformcular ABD hükümetine nüfus sayımında doğumları ve ölümleri resmi olarak izlemesi için baskı yaptılar ancak ikinci dünyasına savaşına kadar ABD’de nerede doğduğunuzu ve isminizin ne olduğu gösteren standart doğum belgeleri zorunlu hale gelmemişti.

Fakat yine de bu temel bilgi parçalarını biçimsel olarak oluşturmak, benzersiz bir kimlik oluşturmak için yeterli değildir. En eski zamandan beri soyadınız ne iş yaptığınızı veya ailenizin kim olduğunu belirlemek için kullanıldı. Smith soyadı demircilere verilirdi, Robertson “Robert'in oğluydu” ve Bin Ali, “Ali'nin oğlu” idi. Bu anlamda soyadlarının ortaklığı, kimlik yönetimini gün geçtikçe zorlaştırmaktadır. Ancestry.com göre:

*“Bugün kullanılan yaklaşık 100.000 Japon soyadının çoğu, sadece soyadlarının ilk kez verildiği 1868 yılından bugüne kalmadır. Aynı şekilde sadece yüzlerce yaygınlaşmış Çince soyadı vardır ve bunların 20'si nüfusun yarısı tarafından paylaşılmıştır. Yaklaşık 250 Korece soyadı vardır ve bunlardan üçü Kore nüfusunun neredeyse yarısını ve yaklaşık 100 Vietnamlıyı kapsar. Aynı şekilde 3 isim de bu ülkedeki isimlerin %60’ını oluşturur.*

Amerika Birleşik Devletleri’nde 50 eyaletin 40’ında Smith en yaygın soyadıdır. Dünya çapında isimlerin ortak olması nedeniyle, uygun bir kimlik yönetimi düşüncesi hükümetlerin ulusal kimlik numaralarını başlatmasını gerektirdi.

## **Ulusal Vatandaşlık Numaraları**

ABD'de Sosyal Güvenlik numarası (SSN), 1936 yılında Amerikan işçilerinin kazanç geçmişlerini izleme amacıyla, Sosyal Güvenlik Yardımı hakkının belirlenmesinde (Ağustos 1935'te Sosyal Güvenlik Yasası kabul edildikten sonra) ve yardım seviyesini hesaplamada kullanılmak üzere oluşturulmuştur. O dönemde isimler ve adresler parmak izleriyle birlikte değerlendirildi fakat isimler daha önce de belirttiğimiz ortak kullanımlar sebebiyle endişeleri ortaya çıkardı ve 1930’larda parmak izi ABD’de suç faaliyetleri ile fazlasıyla ilişkiliydi.

ABD’de sosyal güvenlik numarasında 9 basamak vardır. İlk üç sayı coğrafi bölge veya posta kodundan yola çıkarak verilir. Ortadaki iki sayı coğrafyayı daha fazla tanımlayan grup sayılarıdır, son dört sayı ise rastgele seri numaralarıdır. Bu anlamda işletmelerin saptama amacıyla kimlik numaralarının sadece son 4 rakamını teyit etmesi yaygındır fakat bu durum bu rakamları hırsızlığa son derece yatkın hale getirir.

Aynı şekilde diğer birçok ülke, kimi zaman Sosyal Sigorta Numarası olarak adlandırılan, Vergi Kimlik Numaraları veya Ulusal Kimlik Numaraları olarak adlandırılan benzer ulusal kimlik numaralarına sahiptir.

## **Kimlik Karaborsası**

Kimlikler sabit/değişmez olmadığından ve aynı şekilde ekosistemde pek çok hükümet ve özel aktör kimlik kayıtlarını oluşturmak veya onaylamak için güvenilir olmadığından, sahte ve taklit belgeler için gelişen bir karaborsa vardır. Örneğin bir Küba doğum sertifikasını ele alalım. Küba’ya ait doğum belgesine sahip olan ABD’deki illegal bir göçmen için o belge sadece 1 yıl içinde vatandaşlığa giden bir yol anlamına gelebilir ki bu yüzden sahte doğum belgeleri 10.000$ ya da daha fazla bir fiyata satılmaktadır.

Amerika Birleşik Devletleri'ndeki pasaport sahtekarlığının % 40'ının Porto Riko'dan gelen sahte veya çalıntı doğum sertifikalarını içerdiği tahmin edilmektedir ve Güvenlik İttifakı 2008'de (aynı yıl) Porto Riko'da 45.622 çocuğun doğduğunu bildirmektedir. Fakat aynı yıl 860.000 adet sertifikalı doğum belgesi basılmıştır. Mevcut hükümetlerin kullandığı kimlik sistemi ciddi biçimde bozulmuş/kırılmıştır ve hem özel sektörde hem de kamu sektöründe kötü aktörleri teşvik etmektedir. Aynı zamanda bu sistem yoksullaşmış nüfusu ek gelir için kimliklerini satmaya teşvik eden bir kara borsa yaratmaktadır.

Bu düşünceyle ile birlikte, adil ve dürüst bir finansal ekosisteme sahip olmayı nasıl bekleyebiliriz? Bankalar, kredi kartı şirketleri ve hatta girişimler kullanıcıların kimliğini doğru bir şekilde tespit etmek için uğraşıyorlar. Fakat yaptıkları zaman bile, acaba kişinin söyledikleri kişi olup olmadığını gerçekten bilmenin bir yolu var mıdır?

## **Kimlik Hırsızlığı ve E-Ticaret**

Raindrop Whitepaper'ımızda incelendiği gibi, kimlik hırsızlığı ABD'de ve dünya çapında büyüyen bir sorundur. Nisan 2017'de Symantec, 2016 yılı boyunca çeşitli kapasitelerde 1,1 milyar adet PII'nin (kişiyi tanımlamak için kullanılan bilgiler) ele geçirildiği tahmin edilen İnternet Güvenliği Tehdit Raporu'nu yayınladı. Ticaret giderek uzaktan yapılmaktadır ve bunun yarattığı kişisel iletişim eksikliği, mali dolandırıcılığın işlenmesini kolaylaştırırken, yetkililerin bu olayları durdurmasını zorlaştırmaktadır. Çevrimiçi işlemlerin büyük çoğunluğu için kimlik saptaması gerekli değildir. Bu sistem bir “güven” sistemine dayanır ve bu sistemde limitten düşülmüş [amorti edilmiş – written off] dolandırıcılık vakaları ve para iadesi (chargeback) vakalarının belirli bir yüzdesi olacaktır. Para iadelerinin ortalama maliyeti tek başına bir tüccarın yıllık gelirinin yaklaşık% 1.47'si kadardır ve false positives sırasında bir satıcının yasal bir müşteriyi bir dolandırıcı olarak yanlış bir şekilde tanımlayarak bir satın alma işlemi yapmasını durdurması durumunda kaybedilen satışlar 118 milyar dolardır. Bunlar, kredi kartı ve e-ticaret işlemleri sırasında kullanılan kamusal blockchain'e bağlanarak değişmez kimliklerle kolayca çözülebilecek şaşırtıcı rakamlardır.

## **Mevcut Kimlik Formları**

Genel olarak kimlik kavramı, Web 3.0'a yaklaştıkça değişmekte ve küresel toplumda daha yapay ve duyarlı bir zekanın ortaya çıkmasıyla zaman içinde gelişmeye devam edecek durumdadır.

Kimlikler şu anda iki ortak biçime sahiptir - özel ve kamusal.

* Özel kimlikler telefon numaraları ve e-posta adresleri gibi şeylerdir.
* Kamusal kimlikler, sivil toplumlarda oluşturulan vergi kimlik numaraları, pasaport numaraları ve diğer kimlik biçimleri gibi şeylerdir.

Giderek artan bir şekilde araştırmalar, özel kimlik biçimlerinin kendimiz hakkında daha çok şey anlatmaya başladıklarını ve kamusal formlardan daha duygusal bağlar oluşturduklarını göstermiştir. Araştırmaların çoğu Amerika Birleşik Devletleri'nde bir cep telefonu numarasının şu anda önem bakımından bir Sosyal Güvenlik Numarası'nın yerini aldığını iddia etmektedir. Statista’ya göre, küresel cep telefonu kullanıcılarının 2019’da akıllı telefon kullanarak % 50’nin üzerinde bir oranla 5 Milyar’a ulaşması beklenmektedir.

Cep telefonu numaralarının uzun ömürlülüğü ve kullanışlılığının bir örneği, ABD mobilden mobile bağlantı istatistiklerine bulunabilir. 2003 yılında, ilk yıl verileri toplandı ve ABD mobil portlama veri tabanında sadece 795.000 adet veri tabanı vardı, 2009'a göre bu sayı 40 milyonu aştı [şu anda, yüz milyonlarca kişi olduğunu tahmin edebilir, ancak kamuya açık bir veri yok.]. Artık bu pratiği yaygın kılmak, sıradanlaştırmak için hükümet inisiyatifleri var çünkü yasa yapıcılar telefon numaralarını “önemli tanımlayıcılar” olarak görüyor ve tüketiciler büyük bir çoğunlukla telefon numaralarını tutmayı tercih ediyorlar. Psikolojik araştırmalar, insanların cep telefonları olmadan yüksek düzeyde sıkıntı ve endişe duyduklarını ve şimdi gençler için telefonun oyuncak ayılar gibi benzer bağlanma özelliklerine sahip olduklarını göstermiştir. Kimliğinizin ne olduğu düşüncesi, teknolojinin giderek daha çok kişinin kendi duygusuyla iç içe geçmesi yoluyla değişiyor. Bu anlamda kimlik protokolü oluştururken, sadece kamu kimliğini değil fakat aynı zamanda denklemdeki özel kimliği de içermesi önem arz etmektedir.

## **Standart Olmayan Belgeleme**

İlçe, eyalet, il veya ülke genelinde belgelerin taşınabilirliği ile ilgili artan sorunlar mevcuttur. Tüm kimlik belgeleri aynı şekilde oluşturulmadıkları ve küresel standartlara sahip olmadıkları için terörle mücadele, kara para aklama, uyuşturucu kaçakçılığı ve diğer yasadışı faaliyetler açısından öncelikli sorunlardan biridir.

ABD'yi bir örnek olarak ele alacak olursak, sorun o kadar kötüye gitti ki ABD hükümeti Kentucky, Maine, Minnesota, Missouri, Montana, Oklahoma, Pennsylvania, Güney Carolina ve Washington sakinlerinin tüm yurtiçi seyahatlerde ABD pasaportu kullanmasını zorunlu kıldı. Çünkü bu eyaletler 2005 yılında REAL ID yasasının standartlarını karşılayan bir kimlik çıkarmadılar.

Bu durum sadece merkezi kimlik protokolleriyle ilgili bir sorun değildir. Girişimcilerin açık mimarilerden ziyade özel çözümler üretme arzusu nedeniyle, dağıtılmış veri tabanları üzerinde önerilen veya önerilecek olan pek çok kimlik protokolü aynı sorunlara yol açmaktadır. Tokenların ya da platformların çok etkili olması için bir kimlik protokolüyle okuma, yazma, genişletme, bağla(n)ma ve etkileşim esnekliğine sahip olması gerektiği görüşü, Hydrogen geliştirici ekibinin görüşüdür. Diğer bir ifadeyle denklemin içine kamusal bir blockchain eklemek, yaklaşımdaki temel kusurları değiştirmez. Kimlik yönetimi için protokol düzeyinde özel bir çözüm ortaya koymak, ABD’nin kimlik gereksinimlerini karşılamayan 9 ABD eyaletine benzer. Uyumluluk oluşturmak için yapılması gereken zahmetli değişiklikler vardır ve tam da bu nedenle Hydrogen basit ve standartlaştırılmış bir protokole tamamen bağlıdır.

## **Devlet Blockchain Girişimleri**

Yukarıda sıralanan sorunlardan bazıları kamu sektörünün blockchain teknolojisine daha fazla ilgi göstermesi gibi bariz sonuçlar doğurmuştur. Örneğin, Illinois'deki bir çalışma kolu, devlet tarafından yönetilen/çalıştırılan bir blockchain’de vergi kayıtları, oylama ve sağlık geçmişleri oluşturma planını sundu. Hükümet, insanların kamusal hizmet kimliğinin doğrulanması için veri depolaması sağlayan bir bakıcıdan ziyade bir doğrulayıcı olacaktı. Estonya vatandaşları ve e-konut sakinleri [e-residents] çeşitli kamu hizmetlerine erişim sağlayarak, arka planda blok zinciri altyapısıyla desteklenen, kriptografik olarak güvenli bir dijital kimlik kartı kullanırken, blockchain ID girişimlerini araştıran diğer ülkeler arasında Singapur, Gürcistan, İngiltere ve Dubai bulunmaktadır.

Bununla ilgili sorun iki yönlüdür: 1. Tek doğrulayıcı olarak hareket eden hükümetler merkezileşme ve bozulma yaratır; 2. Her yerel, eyalet ve ulusal hükümet, özel veya yarı özel blockchain yaratırsa, aslında sadece dağıtılmamış olan öncül veri tabanlarının sorunlarını birleştirmiş bir durum yaratılar. Bu anlamda kimlik yönetiminin gerçekten merkezi olmayan ve dağıtılabilir olması için bu alanda çoklu doğrulayıcılar ve standartlaştırılmış protokoller olmalıdır.

Hükümetler yanlış bir şekilde blockchain’i mevcut veri tabanı altyapısının daha dağınık bir hizmete taşınmasının, son vatandaş(?) [end citizen] için sadece marjinal olarak daha iyi olduğu gerçeğini göz ardı ederek her derde deva bir “teknoloji” olarak görebiliyorlar. Daha da kötüsü, bu onların hayatlarını daha zor ve karmaşık hale getirebilir. Yanlış bir bilgiyi, değişmez bir veri tabanına koymak, ilk etapta herhangi bir bilgiye sahip olmamaktan daha kötü olabilir. Kapalı mimariye sahip ve standartlaştırılmamış sistemler oluşturmak, küresel pasaportlar ve sınır güvenliği ile görülen mevcut sorunları bir araya getirip sorunlar yaratabilir.

# **Snowflake’e Giriş**

Şimdiye kadar sözü edilen sorunları çözmek için, Hydrogen takımı Hydro Snowflake’i [kar tanesi] kamusal blockchain tarafından desteklenen benzersiz bir kimlik olarak ortaya koyar. Neden buna snowflake [kartanesi] diyoruz? Kar taneleri doğadaki en güzel, rastgele ve bireysel fenomenlerden biridir. Bilim adamları onların sadece 35 farklı türde olduklarına inanmakla kalmaz, aynı zamanda su moleküllerini oluşturan atomların atom yapısındaki farklılıklar olduğuna ve bunun her bir Kar Tanesi'ni benzersiz kıldığına inanır. Snowflake kimlikleri basılmış/yaratılmış [minted] olmalıdır. Her bir basılmış Snowflake, hem değişmez hem de değişebilir verilerden oluşur ve etkileşime girebilen ve genişleyebilen bir temel kimlik katmanı olarak işlev görür.

## **Tokenize[[1]](#footnote-1) Bir Kimlik**

Her uygulama, ister web ister mobil olsun, kimliğin bazı formlarını tüketir. Sonuç olarak, kullanıcılar aynı verileri birden fazla uygulamaya tekrar tekrar sağlamak zorunda ya da söz konusu bilgileri aktarmak için merkezi taraflara güvenmek zorunda kalırlar. Bu merkezi taraflar kullanıcı verilerini yanlış kullanırsa, kullanıcılar kimlik hırsızlığına karşı kaçınılmaz olarak savunmasız durumda kalırlar. Ayrıca uygulamalar, anlamlı kullanıcı profilleri oluşturmak için sağlanan kullanıcı bilgilerinin geçerli olduğunu doğrulamakla uğraşmak durumundadır.

Bu eksiklikleri gidermek için, her bir Snowflake kullanıcısı, benzersiz bir HydroID ile eşlenmiş ve bir mobil cihazda Hydro Client-Side Raindrop aracılığıyla oluşturulan seed’lerle birleşmiş/ilişkilendirilmiş, değiştirilemez [mübadelesi mümkün olmayan – non-fungible çn.] bir token’a sahiptir.

Bu değiştirilemez token, üç tür verinin depolanmasını destekler:

* Immutable Data [değişmez veri]
* Mutable Data [değişken veri]
* Metadata [metaveri]
  + Validations [doğrulamalar, onaylamalar]
  + Resolvers [çözücüler]

Bir kullanıcının Snowflake ile ilişkili her bir veri parçası, bu Snowflake kimliğinin bir "özelliği" olarak kabul edilebilir. Snowflake’in mint edilmesi veya güncellenmesi sırasında, kullanıcılar verilerini bir salt ile hash eder. Kriptografide bir salt, "hashes" verisi, bir şifre veya parola [passphrase] olmak üzere tek yönlü bir fonksiyon için ek bir girdi olarak kullanılan rastgele bir veridir. Bu hash’ın sonucu zincir üzerinde saklanır. Zira bu sistemde sıradan gözlemciye ya da saldırganlara karşı veriler anlamsızdır. Fakat bir kullanıcı saltmetin belgelerini ve salt’ı üçüncü bir tarafla paylaşmayı seçtiğinde, orijinalliği doğrulanabilir.

## **Kimlik Doğrulama**

Doğrulayıcılar, bir Snowflake kimliğine bağlı verilerin geçerliliğini doğrulayabilecek üçüncü taraflardır. Doğrulayıcıların yokluğunda, zincirdeki veri hash’leri anlamsız olurdu çünkü hash tersine çevrilemezdir.

Off-chain [zincir dışındaki] doğrulayıcılar merkezi olmayan bu ekosistemde bireysel aktörler tarafından güvenilen taraflar olarak hareket edebilir. Doğrulama, off-chain olarak gerçekleştiğinde, bir kullanıcının snowflake’i için bir on-chain [zincir-içi] kayıt bağlanır. Hiçbir kimse kendi özel anahtarlarına erişimi olmayan bir doğrulayıcıyı taklit edemediği için, ticari işletmeler konu ile ilgili herhangi bir iş mantığına blockchain’i sorgulayarak zincir onayı [on-chain validation] dahil edebilir. Bir kullanıcı herhangi bir veriyi değiştirirse, önceki onaylarını, ilgili tokenlarıyla birlikte kaybeder.

Örneğin bir kullanıcı, verilerin açık belgesini [plaintext] ve uygun salt’ı ileterek üçüncü bir tarafın verilerini doğrulayabilir. Üçüncü taraf daha sonra verileri toplayabilir ve zincir üzerinde neyin kaydedildiğini karşılaştırabilir. Eğer eşleşirse, bir geçerliliğe sahip/layık demektir.

Doğrulama off-chain olarak yapılabilir; örneğin doğum tarihinin doğrulanması bir devlet kurumu tarafından bizzat yapılabilir. Bu onaylama, bir sinema bileti almak için belirli bir yaşın üzerinde olmanız gerektiğinde veya bir bankada yeni bir hesap açarken anlam taşıyabilir. Alternatif olarak, bir kullanıcı bir e-posta adresi için doğrulama alırsa, e-posta adresini herkese açık olarak bildirmek zorunda kalmadan, bu e-postayı bir e-posta doğrulama işlemi gerektirmeden uygulamalara sağlayabilecek demektir.

## **Snowflake Metadata**

Değişmez ve standart veriler bir kullanıcının temel kimlik bilgileri için güvenli ve küresel bir standart oluşturmasına yardımcı olsa da, Snowflake'in en güçlü yönü, kullanıcıların üçüncü taraf dApp'lerini resolver [çözümleyici] olarak ayarlayarak sınırsız metada dizisini kimlikleriyle bağlamalarına izin vermesidir.

Temel olarak, bir üçüncü taraf veya dApp, bir kullanıcının Snowflake üzerinde belirli bir özelliğini doğrular/onaylar. Bir uygulama, o uygulamaların Snowflake’lerinin özelliklerine ilişkin doğrulamalara dayanan bir kullanıcı için anlam ifade eder. Bu anlamlar ile ne kast edildiğini birkaç örnek bağlamında daha yakından inceleyelim.

Doğrulama, kullanıcının bakış açısından ne anlama gelir? Doğrulamalar, kullanıcının temel verilerine anlam kazandırır. Saygın kaynaklardan gelen doğrulamaları almak, bir kullanıcının sahip olduğu Snowflake bütünlüğünü, ilgili kimlik bilgilerinin sorgulandığı uygulamalara dayanarak artırır.

Doğrulama, bir uygulamanın bakış açısından ne anlama gelir? Doğrulama kendi anlamını off-chain tanımadan [recognition] türetir. Bir uygulama Snowflake'i bir kimlik protokolü olarak tanımlayacak olsaydı, kendi gereksinimlerine uyan doğrulamalar için ne anlama geldiğini yazabilirdi.

* Örnek 1, KYC onayı: Bir devlet (off-chain) kullanıcıların bir oylama onayı için kendi Snowflake’lerini kaydetmelerine izin verebilir. Kullanıcı oy verme işlemini sadece kayıtlı Snowflakeler’den oy toplayan Horizon State gibi üçüncü taraf bir dApp aracılığıyla yapabilir. Bu süreç, her bireyin seçmen dolandırıcılıklarını ortadan kaldırarak bir kez oy kullanmasını ve seçimlerde tam şeffaflık ve çok daha fazla verimlilik sağlamasını sağlar.
* Örnek 2, Sosyal Medya: Sahte hesapların oluşturulmasını önlemek için bir uygulama, kullanıcının Snowflake uygulamasını aplikasyondaki bir hesaba bağlayan bir sistemi yürütebilir. Uygulamanın kullanıcıları tarafından adlarını doğrulayan tüm hesaplar (en azından X kadarı), uygulamanın ara yüzünde "doğrulanmış" onay işareti ile gösterebilir. İlk örnekten farklı olarak bu örnek, büyük kurumlar yerine bireylerden gelen doğrulamaları belirlemektedir. Ayrıca, bu örnek bir çözümleyici yerine standart bir özellik için doğrulamayı izler. Snowflake kimlik yapısının açıklığı, geniş bir kullanım alanına izin verir.

Doğrulama, doğrulayıcının bakış açısından ne anlama geliyor? Doğrulayıcının bir Snowflake'in çeşitli niteliklerini kanıtlamak isteyebileceği birçok neden vardır.

* Örnek 1, Sosyal Medya Tasdiki: Bir kişi bir sosyal medya uygulamasına (örn. LinkedIn) katılabilir ve bir arkadaşının becerilerini veya deneyimlerini kanıtlamak isteyebilir.
* Örnek 2, Devletlerin Sürücü Belgeleri: Bir devlet ya da yerel yönetim, kamusal güvenliğin genel yararına olacak şekilde kişilerin sürüş kabiliyetini doğrulamak isteyebilir. Lisansın test edilmesi ve lisans için ödeme off-chain’den yapılabilir, ancak bu kullanıcının Snowflake'ini gözlemleyen herkes sadece durum tespiti yaptığının [başka bir işlem yapmadığının çn.] farkındadır.

## **Snowflake’de Hydro Tokenlar**

Doğrulayıcılar ekosisteme katılabilmek için Hydro tokenları stake etmek zorundadır. Tokenlar bir teminatın ticari bir mülk sahibine bağlanması gibi, bir doğrulayıcının benzersiz adresine bağlı bir zincir sözleşmesi üzerinde depolanır. Bu sözleşmeden kaldırılan (veya üçüncü bir tarafa devredilen) tokenlar, doğrulayıcıların ekosisteme erişimini iptal eder. Küresel olarak tüm doğrulayıcıların kötü niyetli davranışlardan kaçınması gerekmektedir. Eğer kötü niyetli davranırlarsa doğrulamaya yarayan off-chain ödemeler için ekosistem söz konusu değildir.

Bu yapı, doğrulayıcı [validatör] olarak hizmet eden bireylerin ve kuruluşların, dürüstlük ve tutarlılık ile doğrulanmaya ilgi duymasını sağlamaktadır. Bu doğrulamaları sorgulayan bir uygulama, verilmiş bir Snowflake için tatmin edici kabul edilen herhangi bir niteliği veya doğrulama seviyesini tanımlayabilir. Örneğin bir uygulama kullanıcının Snowflake’i belirli güvenilir adresler listesindeyse veya bilinen doğrulayıcılar tarafından doğrulanmışsa yalnızca belirli özelliklere kullanıcı erişimi verebilir.

HYDRO token, sadece Snowflake'in üzerine inşa edilebilen dApps ekosistemine bir ağ geçidi olarak değil, aynı zamanda tüm çözücüler [resolverler] için uygun olan programatik transferler için de en önemli öğe olmayı amaçlamaktadır. Snowflake aracılığıyla, kullanıcılar çözücülere HYDRO'yu withdraw etmeleri için belirli ödenekler ayarlayabilirler. Kullanıcı, hali hazırda üçüncü taraf finans kurumları tarafından yönetilmekte olan user-facing modellerin çoğalmasını kolaylaştırarak, her bir çözümleyici temelinde izin verilen para çekme limitlerini belirler. Snowflake'in programatik token transferleri ile yarattığı esneklik, işletmelerin, bir ürün için indirimli abonelikler sunmak amacıyla belirli bir gruptaki üyeliği doğrulamak gibi tekrarlayan işlemler için iş mantığına rasgele bir dizi kriteri kodlamalarına bile olanak tanır.

Daha sonra tartışacağımız gibi, Snowflake üzerine inşa edilen uygulamalar[apps], dApps’ler, ürünler veya platformlar da HYDRO tokenları kendi süreçlerine dahil edebilirler. Örneğin bazı tür doğrulamalar veya eylemler, zincir üzerinde [on-chain] kullanıcıların HYDRO bakiyelerini korumak veya aktarmak için lazım olacak HYDRO token işlemlerini gerektirebilir.

## **Açık Yapı/Çerçeve**

Önerilen yapının kimlik yönetimi için açık bir protokol olduğunu belirtmek önemlidir. Diğer blockchain ürünlerinden farklı olarak, ispatların veya doğrulamaların veya bunları sağlayanların gücünün veya özgünlüğünün üzerinde merkezi bir karar olmayacaktır. Bu ekosistemde kötü niyetli aktörleri belirlemek ve cezalandırmak küresel topluluğa bağlı olacaktır. Daha sonra bu makalede ekosistemin etkinliğini arttırmak için Snowflake'e ya da onun üzerine entegre edilebilecek potansiyel uygulamaları, dApp'leri ve platformları inceleyeceğiz.

# **Snowflake: Teknik Detaylar**

Snowflake’e müdahil olan dört varlık vardır: kullanıcılar, doğrulayıcılar, çözücüler [resolver] ve ticari işletmeler.

## **Kullanıcılar**

Kullanıcılar kendi kimliklerini sunmak/belirtmek için Snowflake’lerini kullanırlar/icat ederler. Snowflake’lerine veri eklerler ve herhangi bir metadata formunu temel Snowflake kimlikleriyle bağlamak için çözücüleri yerleştirirler. Kullanıcılar ayrıca Snowflake’ler içerisinde HYDRO bakiyelerini de koruyabilir ve herhangi bir dApp'in bir kullanıcının Snowflake'i ile etkileşimde bulunabildiği anlaşılması ve kullanılması kolay mekanizmalar oluşturabilirler. Kullanıcı verileri ya sadece sahibi veya onaylanmış doğrulayıcı tarafından saklanabilen, isim ve doğum tarihi gibi standart değişmez verilerdir ya da sahibi tarafından onaylanmış herhangi bir adres veya sahibi tarafından bir dizi veya tamsayı olarak saklanabilen telefon numaraları ve adresler gibi standart olmayan değiştirilebilir verilerdir.

## **Çözücüler**

Doğrulayıcılar Doğrulama'yı bir Snowflake’e eklerken, çözücüler kullanıcıların kendileri tarafından belirlenir. Çözücüler, bir kullanıcı hakkında metadata içeren dApp'lardır. Anlaşılması ve kullanılması kolay bir örnek CryptoKitties'tir- bir çözümleyici olarak CryptoKitties'in ayarlanması, belirli kitty’lerin sahipliğini, kullanıcının Snowflake kimliğine geri bağlayabilir. Bu ayarın saygın/tanınmış doğrulayıcılar tarafından doğrulanması gerekirse, bu adresin ortaya çıkmasına veya aktarılmasına gerek kalmadan CryptoKitties'e ait belirli bir adresin sahipliğini kanıtlamalarını sağlar.

## **Doğrulayıcılar**

Doğrulayıcılar çekirdek Snowflake protokolüne dahil edilmese de, onlar dApp seviyesinde kullanıldığında App’e önemli bir değer eklerler. Snowflake üzerine kurulan doğrulayıcılar, herhangi bir doğrulama kriteri aralığı kodlayabilir. En basit seviye, güvenilir bir KYC sağlayıcısının bir Snowflake'in gerçek bir kişiye ait olup olmadığını teyit ettiği bir doğrulama dApp’i olacaktır. Herhangi bir Snowflake sahibi, güvenilir taraflar aracılığıyla KYC'yi tamamlayabilir, doğrulama dApp'ini Snowflakeler için bir çözümleyici olarak ayarlayabilir ve KYC partisine hiç katılmadan (aynı zamanda hiç görüşülmemiş) herkese var olduğunu kanıtlayabilir. Pratikte dApp'ler, çeşitli endüstrilerde off-chain reputation’dan ya da kendi yerel on-chain reputation protokollerinden türetilen amaçlarla çok daha geniş kapsamlı etkilere sahip, bilişsel olmayan doğrulama yapıları oluşturabilirler.

## **Ticari İşletmeler**

Ticari işletmeler bir Snowflake’e bağlı bilgilere dayanan uygulamalara mantık [logic] inşa eden aplikasyonlar ya da dApp’lerdir. Örneğin bir kullanıcı bir veya daha fazla üçüncü taraf dApps aracılığıyla bir Snowflake'e kredi ile ilgili bilgilerini bağladıysa, bir işletme kullanıcının kredi için onaylanıp onaylanmayacağını belirlemek adına bu meta dataları kullanabilir.

## **Snowflake Akıllı Sözleşmeleri**

Çekirdek [core] snowflake akıllı sözleşmeleri, verileri, çözücüleri ve HYDRO bakiyeleri depolar. Bu kullanıcıların tokenları depolamasına, alanlar ayarlamasına ve HYDRO deposit etmesine izin verir. Doğum tarihi ve isim gibi değişmez alanlar değiştirildiğinde kullanıcılar yeni bir tokena sahip olmalıdır. Diğer alanlar değiştirildiğinde, çözücüleri sıfırlanır. Çözücüler, kullanıcıların Snowflake’lerini, ikili olmayan doğrulamalar veya akredite yatırımcı statüsü gibi daha fazla veri barındıran harici akıllı sözleşmelere bağlamasına izin verir. Kullanıcılar, çözücüler veya ilgili herhangi bir taraf, Snowflake akıllı sözleşmesine HYDRO tokenları yatırabilir. Bu yapı geliştikçe Hydro ekosisteme sorunsuz olarak stake etme gerekliliklerini, ödemeleri [payments] ve diğer token işlevlerini entegre etmeyi kolaylaştıracaktır.

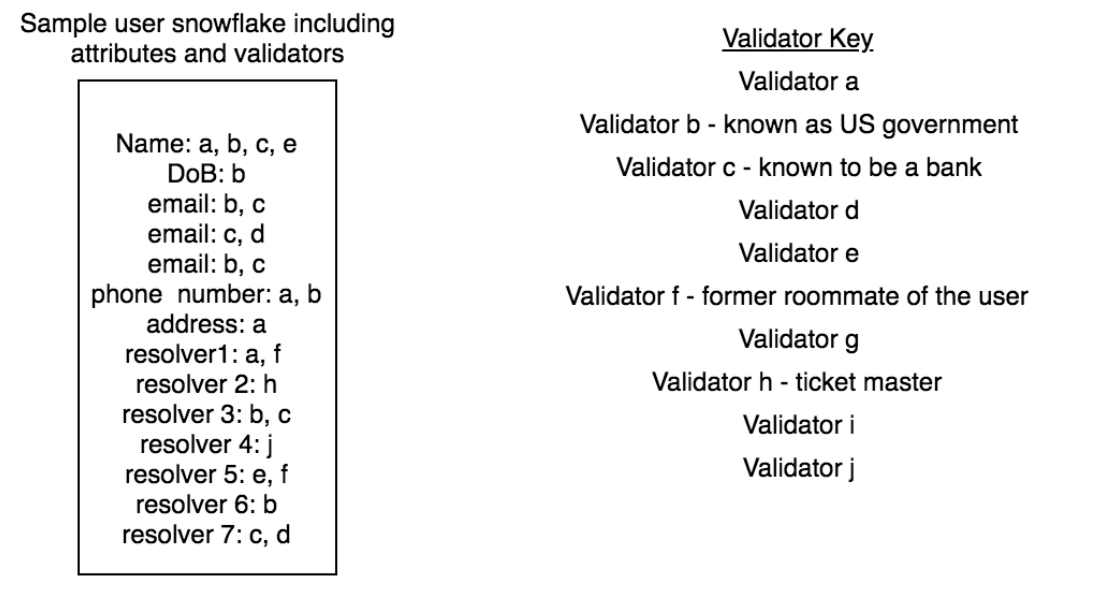
3. taraf dApp’ler:

* Hydrogen, uyumlu üçüncü taraf dApp'lerine bir “ağ geçidi” olan ilk çekirdekli Snowflake veri doğrulama dApp'sini oluşturacaktır (bu uygulamaların nasıl görünmesi gerektiği ile ilgili kurallarımız olacaktır).
* Hydrogen, Hydro için gönderme, stake etme ve ücretlere [fee] izin vermeye yönelik dApp’ler için mantık [logic] yaratacaktır.
* Tüm dApp'ler, kullanıcıların sözleşme adresini çözümleyici olarak belirlemelerini ister.

Temel Snowflake kimliği aşağıdaki şeylerin toplamından oluşur:

* Zincir üzerinde sabit/değişmez olan ve sahibi tarafından bir kez minted edilebilen standart alanlar
  + Ad ve Soyad
  + Doğum Tarihi
* Kimlik sahibi tarafından eklenebilen ve iptal edilebilen standart alanlar
  + İsim öneki/soneki
  + E-Postalar
  + Telefon Numaraları
  + Adresler
* Çözücüler – Token sahipleri tarafından eklenebilir ya da sözleşme sahibi tarafından izin verilirse (eklenebilir)
  + Ethereum Akıllı Sözleşme Adresleri
* Doğrulama - Bir HydroID'e sahip herhangi bir adres, gaz maliyetlerini ödediği sürece herhangi bir Snowflake için herhangi bir özelliği doğrulayabilir.

Bir kullanıcının Snowflake’i, kullanıcının dApp etkileşiminden gelen tüm veriler için bir bağlantı noktası görevi görür. Bir üçüncü taraf uygulaması kullanıcı için hangi alanların doğrulandığını görebilir. Örneğin aşağıdaki resimde çözümleyici 1, bir kullanıcının iyi bir oda arkadaşı olarak doğrulandığını göstermek için bir sosyal inceleme dApp’i olabilir. Bir işletme, eski bir oda arkadaşı olan doğrulayıcı f'nin, sahibinin bilgilerini doğruladığını görebilir. Bu nedenle, kendi iş mantığında, doğrulayıcılar çözümleyicinin platformunun UI'sı hakkında bir inceleme yazmasına izin verilebilir çünkü değerlendirmeleri snowflake sahibi için geçerlidir.



## **Snowflake API ve Hydro Mobil App**

Hydrogen Hydro API'si, Snowflake akıllı sözleşmeleriyle kullanıcı ve ticari işletmelerin etkileşimlerini kolaylaştıracaktır. API, son kullanıcılara HydroID'lerini, Snowflake'lerini önceden gerekli şekilde mint etmek için Hydro mobil uygulamasına Raindrop API entegrasyonu yoluyla kayıt yapma olanağı sağlar. Sonraki yinelemede [iteration] kullanıcılar Hydro API, blockchain ile doğrudan etkileşimi idare ederken [handle], Hydro mobil uygulaması üzerinde HydroID’leriyle ilişkili kendi Snowflake'lerini mint edebilecekler. Onların mobil uygulamasındaki kullanıcı ara yüzü, Hydro API'si tarafından beyaz listeye eklenmiş adreslerden elde ettikleri doğrulamaları gözlemlemelerini sağlayacak. Ayrıca kullanıcılar kendi Snowflake’ine daha geniş bir metadata aralığı eklemek için Hydro mobil uygulaması aracılığıyla çözücüler oluşturabilecekler.

Ticari işletmeler Hydro ekosistemde yer alan bilgiler için Ethereum blockchain'i sorgulamak üzere Hydro API'yi kullanabilecektir. API, blok zinciri geliştiricilerine sahip olmalarını gerektirmeden onların iş mantığına göre kolayca kodlanabilen, hafif formattaki uygulamalara zincir halinde bilgi sağlayacaktır.

## **ERC-721 Kontrat Standard’ına Ayna Tutmak**

HYDRO gibi ERC-20 tokenlar, değiştirilebilirliğin karakteristiğini paylaşır ve bu da her token’in sorunsuz ve eşit olarak birbiriyle değiştirilebilir [fungible] olduğunu gösterir. Bu, ERC-20 standardında her token’in başka bir token ile aynı işlevselliğe sahip olmasından dolayı token’ler için anlam ifade eder. Fakat bir kimlik protokolü için değiştirilemezlik [non-fungible] ona sahip olmanın ardındaki anlamlılığı yönlendirir. Eğer kimliklerimizi kendi aramızda herhangi bir fark olmadan değiştirebilseydik bu kimliklerin herhangi bir gözlemciye karşı değeri kalmazdı. Açımlama 721 için Ethereum talebi ya da ERC-721, 2017'de Dieter Shirley tarafından sunulan bir Ethereum önerisidir. HYDRO token’inin kendisi ERC-20 standardı üzerine kurulu olmasına rağmen, Snowflake protokolünün akıllı sözleşmeleri, ERC-721 tokenlerinde bulunan dinamikleri daha yakından yansıtmaktadır. Bunlar “birleştirilemez/değiştirilemez” jetonlar olarak bilinir.

Kullanıcıların kimlikleriyle ilişkili bilgilerin sahipliğini kanıtlamalarına izin vermek için, her bir Snowflake’in birbirine değiştirilemez [non-fungible] olması çok önemlidir. Snowflake kimliğinin değeri, bir parasal değer için değiştirilebilememesinden değil, kullanıcının zincir üzerinde kimliğini oluşturan benzersiz özelliklere sahip olmasından gelir. Bunu akılda tutarak, bir kimliğin sahiplik aktarımına izin vermemek için ERC-721 standardından biraz uzaklaştık.

Açık kaynaklardaki ve blockchain topluluklarındaki sürekli endişe, çoklu proje ve standartlardaki geliştirici çabasının parçalanmasıdır. Bu riskin farkındayız ve Snowflake'i bu olasılığın olabildiğince az olmasını sağlayacak şekilde tasarladık. ERC-721'den bu uzaklaşışımız, bu çalışmanın eleştirisi olarak ele alınmamalıdır. Aksine kimliklerin sahiplerine, diğer benzersiz ve tahsil edilebilir tokenlarda olmadığı haliyle bağlanan bir yapıdaki basit bir gerçekliğin yansımasıdır. Bu kısıtlama içerisinde Snowflake, temelde modüler ve açık olacak şekilde tasarlandı. Bu anlamda Snowflake, çok çeşitli kullanım durumlarını esnek bir şekilde birleştirebilecek ve kimlikle ilgili istemlerde bulunmak için ortak bir protokol olarak hizmet edecektir.

# **Finansal Hizmetlerdeki Yansımaları**

Snowflake'in açık yapısı, protokolün uzun vadeli başarısına entegre olan ürünleri, platformları, uygulamaları ve dApp'leri üretecektir. Aşağıda, Hydro topluluğunun destekleyeceği bazı ilk uygulamaları inceleyeceğiz:

## **Evrensel Hesap Katılımı [Universal Account Onboarding]**

Doğrulayıcılar olarak küresel KYC sağlayıcıları ile entegrasyon sayesinde Hydro, günümüz dünyasında var olan geniş KYC standartlarına uyum sağlayabilen standartlarda tek dokunuşlu dijital bir hesap standardı oluşturabilir.

## **Doğrulayıcı Derecelendirme Sistemi**

Bu basit dApp, çoklu kimlik alanlarında doğrulayıcılar için bir destekleme [upvoting] / eksileme [downvoting] sistemi yaratacaktır. İtibar temelli bir puanlama sistemi, oylamada teşvik odaklı bir dürüstlük yaratacaktır. Bu merkezi olmayan itibar oluşturma durumu, bazı doğrulayıcılar için ikili bir süreçten daha büyük bir anlam ifade edebilir.

## **Makine Öğrenimi Doğrulama Standardı**

Hydrogen platformu Ion AutoML API'sini içerir. Küresel olarak yeterli doğrulamalarla, merkezi olmayan ve veriye dayalı bir şekilde doğrulama yapan, doğrulamaları derecelendiren, sıralayan, işaretleyen ve kaldıran AutoML API kullanılarak bir ürün oluşturulabilir. Akıllı sözleşmeler, şeffaflık için AutoML yeteneklerinin üstüne entegre edilebilir.

## **Belge ve Sözleşme Doğrulama Standardı**

Hydro projesinin bir sonraki aşaması ICE olarak adlandırılır ve bu bir belge yönetim protokolüdür. Raindrop ile birlikte Snowflake, Ice’ın ölçeklendirilmesi için integral olacaktır. E-imzalama teknolojileriyle ilgili en büyük sorunlardan birisi, tek faktörlü kullanıcı adları ve şifreler dışında hiçbir zaman bir doğrulama veya kimlik doğrulama yapılmamasıdır. Herhangi bir belge imzası veya sözleşme damgalaması için onaylanmış Snowflake’ler ve çok faktörlü kimlik doğrulama işlemleri, Hydro mobil uygulamasına inşa edilebilir. ICE protokolünün üzerine inşa edilen bazı basit dApps’ler, DocuSign ve Adobe Sign gibi popüler e-imza yazılımlarına da entegre edilebilir

## **Ödeme Doğrulama Standardı**

Hydro projesinin sonraki aşamalarından birisi TIDE olarak adlandırılır; bu bir ödeme ve veri gizliliği protokolüdür. Bu protokol doğrulamaları referans alabilecek ve “levelleri” ya da onaylamanın gücünü yaratabilecek bir dApp oluşturmak için harika bir fırsattır. Bunun bir sonucu, doğrulama düzeyini kontrol eden finansal hizmetlere ait web siteleri için bir eklenti olabilir. En yüksek düzeyde bir doğrulama, ekstra doğrulama veya kimlik doğrulama gerektirmezken, en düşük seviyedeki doğrulamanın ikincil bir ID formunu gerektirmesi gerekebilir.

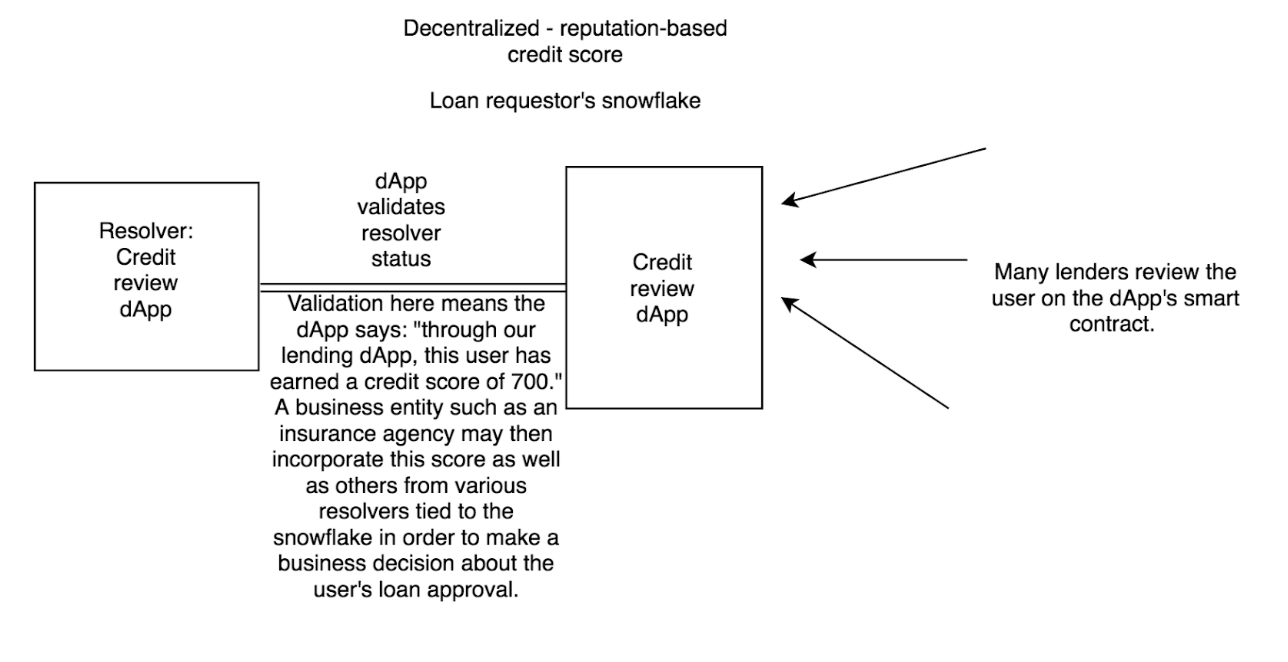
## **Sahtecilikle Mücadele POS dApp’leri**

Satış sistemlerinin çoğu aygıtı, hesap kartı ve kredi kartlarında basit bir kaydırma hareketi veya çip doğrulaması gerektirir. Satış sonrası aldığınız fiş incelendiğinde bu belgede, satış sırasında yapılan hiçbir ek kimlik kontrolü yoktur, o belge sadece satış sonrası için tetkik edilmiştir. Square, Paypal, Braintree ve Stripe gibi firmalar küresel olarak varlıklarını milyar dolarlar seviyelerine taşıdıkça, satış noktalarının işlem protokollerine anında erişebilecekler. Merkezi olmayan bir POS ağı üretmek için Hydro'nun Snowflake, Raindrop, Tide ve Mist aşamalarını entegre edebilecek çok ilginç dApp'ler vardır.

## **Küresel Kredi Puanlaması**

Krediye erişmek muazzam bir küresel sorundur ve 2 milyara yakın kişinin bankalara erişimi olmamaması kitleleri etkileyen en önemli sorunlardan birisidir. Bu problemi önlemek için, ABD'de kredi değerini doğrulamaya yönelik finansal verileri kullanmaya çalışmak için bir FICO puanlama sistemi kurulumu yapılmıştır. Ancak bu sistem, hiçbir “sosyal kanıt” sağlamadığı ve sadece banka hesaplarıyla, kredi kartları ile finansal sistemde olanları hesaba katması sebebiyle temelde kusurludur. Hydro API, hassas kullanıcı verilerini depolamak için merkezi taraflara yaslanmadan, daha sağlam kredi puanlama modelleri oluşturmak için ihtiyaç duydukları bilgileri işletme kuruluşlarına sağlayabilir.

Bir üçüncü taraf işletme tüzel kişiliği, bir kredi teslim etmede iş kararını sürdürebilmek için kullanıcının kredi puanlama verilerine bir çözücü aracılığıyla ulaşarak, o kullanıcının Snowflake’ine bağlı bilgilere güvenebilir.

[](https://github.com/hydrogen-dev/hydro-docs/blob/master/Snowflake/_assets/workflow2.png)

# **Riskler**

Snowflake ekosistemi, en iyi aktörler olarak off-chain doğrulayıcılara ve kötü davranışı/girişimi cezalandıracak küresel bir merkezsiz topluluğa bağlıdır. Örneğin, zincir dışında [off-chain] var olan doğrulama ve belgeleme için aynı “kara borsaları” teşvik etmeyi ve onları zincir haline getirmeyi istemiyoruz, bu nedenle ekosistemin tasarlandığı şekilde çalışması zorunlu kıldık. Tam da bu nedenle HYDRO token ve onun stake edilmesi ekosistemi doğru [honest] tutmak için çok önemlidir.

Ek olarak ekosistemde parçalanma/bölümlenme [fragmantasyon] riski vardır. Bir kullanıcıyı onaylamak için ne kadar doğrulama veya tasdik işleminin kabul edilebilir olduğuna karar vermek bir işletme veya web sitesine bağlı olacaktır. Snowflake bir protokol olduğu ve bir ürün olmadığı için bu tarz bölümlenmelerin kabul edilmesini önlemek için en iyi kullanım durumlarının hızla standartlaştırılması zorunlu olacaktır. Örneğin, onaylanmış bir eyalet sürücü lisansı Amazon'da ödeme için kabul edilebilir ancak Google'da ek bir sosyal onaylama gerekli olabilir. Hydro ekibi bu sorunla mücadele etmek amacıyla çeşitli kullanım durumları için; kullanılabilecek sitelere yönelik en iyi uygulamaları, örnek uygulamaları ve widget'ları sağlamayı amaçlamaktadır.

Ekosistem içinde bir de “eğitimsel” bir risk vardır. Birçok yerleşik blockchain kimlik ekosistemi kapalı bir mimaride veya özel bir şekilde inşa edimiştir. Özel blockchain sağlayıcıları tarafından kamusal blockchain’deki algılanan zayıflıklar üzerine büyük bir dezenformasyon kampanyası yapılmıştır. Fakat Snowflake ekosistemi, kamusal blockchain ve onların akıllı telefonlarındaki şifrelemeye güvenen kullanıcılara bağlıdır.

# **Sonuç**

Kimlik yönetimi dünya çapında bozulmuş, parçalanmış durumdadır ve Web 3.0’ın şafak vakti yaklaştıkça daha da kötüleşmektedir. Kimlik hala merkezi, yolsuzluğa ve hırsızlığa yatkın bir araç durumundadır ve bu sebeple milyarlarca insan finansal hizmet çözümlerinin kısmen de olsa dışarısında bırakılır.

Hydro’nun Snowflake yapısı, kimlik yönetimi sorununun anahtar parçalarını (sorunlarını) çözmek için uygulanmaktadır:

* Zincir üzerinde şifrelenebilecek kişisel bilgileri saklamak için standartlaşmış ve bir merkezi olmayan yapı oluşturulması
* Zincir üzerinde [on-chain] verilere bağlanan bir zincir dışı [off-chain] ispatlama ve doğrulama ağı oluşturulması
* Kolayca entegre edilebilen, standartlaştırılmış uygulamalar, QR kodları, UI widget'ları ve Snowflake protokolünün üstündeki diğer ürünlerin oluşturulması

Hydro ekibi ortaya konan bu yapının/çerçevenin Web 3.0'ın standart kimlik yönetimi protokolü olabileceğine inanmaktadır. Hydro API'nin kullanım kolaylığı nedeniyle hem uygulamalar hem de dApp'ler Snowflake mimarisini hızlı bir şekilde kendi kendilerine uygulayabileceklerdir.

# **Kaynakça**

PNAS.org - <http://www.pnas.org/content/110/32/13216>

Social Security Administration - <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>

History Channel - <https://www.history.com/news/the-history-of-birth-certificates-is-shorter-than-you-might-think>

Ancentry.com - <https://blogs.ancestry.com/cm/what-can-your-surname-tell-you/>

CNN.com - <https://www.cnn.com/2013/01/18/justice/florida-cuban-birth-certificates/index.html>

Watchdog.org - <https://www.watchdog.org/florida/those-with-fake-birth-certificates-find-it-s-easy-to/article_a3935cbf-74b8-5237-9b0a-ae17748f6786.html>

Martin Private Investigators - <http://www.martinpi.com/your-cell-phone-number-is-your-new-social-security-number/>

Statista - <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>;<https://www.statista.com/statistics/188511/mobile-to-mobile-telephone-numbers-in-us-porting-database-since-2003/>

Federal Register - <https://www.federalregister.gov/documents/2017/11/27/2017-25458/nationwide-number-portability-numbering-policies-for-modern-communications>

Psychology Today - <https://www.psychologytoday.com/us/blog/fulfillment-any-age/201609/is-why-we-cant-put-down-our-phones>)

Symantec - <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>

Chargebacks911 - <https://chargebacks911.com/chargeback-stats-2017/>

Travel & Leisure - <http://www.travelandleisure.com/airlines-airports/no-drivers-license-tsa-rule>

Coindesk - <https://www.coindesk.com/illinois-eyes-blockchain-for-ids-and-public-asset-management>

Enterprise Innovation - <https://www.enterpriseinnovation.net/article/how-are-governments-using-blockchain-technology-1122807855>

W3.org - <https://www.w3.org/DesignIssues/Metadata.html>

PSU Meteorology - <http://news.psu.edu/story/141325/2009/02/18/research/probing-question-each-snowflake-really-unique>

Wikipedia Cryptography - <https://en.wikipedia.org/wiki/Salt_(cryptography)>

1. Başlığın kendisi orijinal metinde “A Tokenized Identity”dir. Düz bir Türkçe çeviri ile Jetonlanmış/Jetolaşmış bir kimlik olarak çevrilebilir fakat token üzülerek belirtmek gerekirse dilimizde yer edinmiştir. Örneğin tüm dünya tıpkı economics gibi tokenomics gibi kavramları kullanmaktadır. Bu sebeple bende çeviride kavramı Tokenize olarak bırakmayı doğru buldum. [çn] [↑](#footnote-ref-1)