Mevcut yöntemimizde belge oluşturma yetkisi doğrudan bizim tarafımızdan veriliyor.

Bu inisiyatif bir şekilde ele geçirilebilir, ya da bizim tarafımızdan kötü niyetle kullanılabilir.

Buna çözüm amacıyla geliştirilmiş yöntemler var. Biz de bunlardan bir tanesini kullanıyoruz.

Tanımlar

Contract Deployer: Biz. Ethereum zincirine kontrat ekleme yetkisi sadece bizde var. Bu kontratın içinde her diplomanın nerde olduğu bilgisi var.

Issuer: Okullar. Kontrata yeni diploma adresi eklemek için sadece onlardan gelen bilgiye güveniliyor. Contract Deployer tarafından issuer yetkisi tanımlanmamış herhangi bir kullanıcı, yeni bir diploma ekleyemez.

Öğrenci: Diploma yazma yetkisi olmayan kullanıcı hesabı. Issuer bir diploma ile bir öğrenci hesabını ilişkilendirilir.

Verification:

1)      diploma sahibi olduğunu iddia eden kişi, diplomaya ulaşmayı sağlayacak tek kişi. O private key’e sahip olması diplomanın gerçekten o kullanıcı için düzenlendiğini garantiliyor (matematiksel olarak garantilemiyor, buraları muhtemelen biliyorsunuzdur).

2)      Ulaşılabilir bir diplomanın varlığı, yetkilendirilmiş kişilerce oluşturulduğunu garantiliyor.

Fakat diplomayı oluşturan issuer sahte bir diplomayı herhangi bir kullanıcı adına düzenleyebilir.

O zaman en kritik aşama issuerların yapacağı işlemlerin güvenilirliği sorunu.

Diplomaların doğruluğu için 3 yöntem:

0)      Doğru diplomanın kriterleri belirlenmeli.

1)      PoW: proof of work: İşlemlerin doğruluğu her miner tarafından kontrol edilir. Bizim örneğimizde contratın geçerliliğini kontrol eden minerlar bu yöntemi kullanıyorlar. Ama bu kontratın geçerliliği. Diplomanın değil. Biz aynı yöntemi diploma için uygularsak

·         Üniler miner olurlar. Hepsi birden diplomaların gerçek olup olmadıklarını, önceden belirlenmiş kriterlere göre kontrol ederler.

·         Belirlediğimiz başkaları miner olurlar. Bu işe işlemci adayacak herkesi belirlediğimiz kriterlerin kontrolü için seçebiliriz.

2)      PoS: proof of stack: Oylama. Minerlar eşit oy hakkına, ya da başka bir parametreyle değişen (bir kripto para için bu, minerın sahip olduğu o türden kripto para olabilir) oy hakkına sahipler. %51 ya da başka bir oranı yeterli kabul edebiliriz. Minerların kim olacağı yine bize kalmış.

3)      PoA: proof of authority: Burada miner yok. Validator var. Yeni bir işlem tek kişi tarafından onaylanıyor. Bu onaylama yetkisini contract deployer verir. En maliyetsiz teknoloji budur. Fakat bu yöntem en merkezi de yöntem. PoA tabanlı networklerin Blockchain protokollerini kullanıyor olmaları eleştiriliyor. Böylesi merkezi bir veritabanı yönetimi, neden blockchaini de kullanıyor? Sadece ek maliyet yaratıyor.

Bizim örneğimizde, diploma issuerları biz belirlediğimiz için, diploma verisini de biz tutabilirdik. Ama o veriyi, bir tek yine bizim onayımızda değiştirilebilir bir yer olan ethereum ortamına adres olarak koyuyor ve bunun için bir de para ödüyoruz. Hem işlemler uzun sürüyor, masraflı oluyor hem de merkez ve issuerlar aracılığıyla kötüye kullanımının önüne geçilemiyor.

Burada PoA’cıların çözüm yöntemi ise şöyle. Validatorlar (örneğin bizim için belki Issuerlar olacak) gerçek ve public kişiler. Yani adı sanı herkese açık ve onayladığı işlem (belge) herkes tarafından görünüyor. Ama projenin ilk aşamasında bununla ilgili herhangi bir yöntem yok çünkü validator belirlemedik. Validator olma kriterleri, yöntemi de belirlemedik.

Validatorları aynı minerlar gibi istersek issuerlar olarak seçebiliriz, ister başkaları, yeter ki bu validasyon işlemine işlemci adasın. Ve tabiki validasyon için gerekli kriterler belirlenmiş olsun.

PoA bu validatorlerin, kimlikleri açık olduğundan, isimlerini temiz tutmak ve suçlanmamak adına, validasyon yetkilerini kaybetmemek adına vs, sahte işlem – diploma vs yapmayacağını öne sürüyor. Yapsa bile bir kere iki kere yapar, sahteciliği ortaya çıkınca da validatör özelliğini kaybedeceğinden bütün sistemi çökertemez diyorlar.

Yine de bu durum, geleneksel diploma sisteminin ötesinde bir güvenlik sağlamıyor.

·         Sahte kimlikle imzalamak: geleneksel yöntemde başkaları, yetkili kişilerin imza ve mührünü taklid ederek  (okula kayıdı ösym puanı sınav belgesi vsden ünideki sınav sonuçları için hocaların kurulların imzasına kadar, yökten onay verenlerin imzasına kadar taklit edebildiğimizi düşünün) sahte ama geçerli bir diploma üretilebilir.

·         Bizim yöntemimizde de bunun karşılığı olacak bir validasyon işlemi olmalı. Not kaydı onları girenlerin yetkisi vs ulaşılabilir ve denetlenebilir olmalı. Bu denetleme işini de PoA networküyse kimlikleri belli validatorler yapacak ya da minerlar (PoS we PoW için)

·         Gerçek kimlikle sahte diploma: Bu geleneksel yöntemde Yök yetkileri bir şekilde kötüye kullanılırsa mümkün. Diploma oluşturma yetkisi, haksız şekilde birine verilirse, haksız diplomalar gerçek kişilere verilebilir.

·         Biz PoA kullanır, validator olarak issuerları görevlendirir vesadece kendi diplomalarını valide ettirirsek, bir şekilde bizden issuer yetkisi almış biri istediği gibi sahte diplomalar oluşturabilir. Hacklenmesi geleneksek yöntemden daha kolay. Bu özetle çağının kız arkadaşına diploma oluşturması demek. (yeni oluşturduğu fake üniversite üzerinden)

·         Validatörlerin seçimi: Miner değil validatör kullandığımız durumda, bunların public olmaları yetmez. Kim oldukları, kesin olarak gerçek bir kişiyle ilişkilendirilmeleri gerekir. Bunun için de devletten yardım alınmak zorunda kalıyoruz (noter onaylı belgeler,kimlik kontrolü vs gibi) bu durumda da zaten devletin bildiği kadar bile değil, sadece devletin sunduğu kadar güvenilir bir kimlik verisine sahibiz. Geleneksel sistemin denetçileri idari hukuk ve bir sürü kurum. Denetlenecek şeye özel denetçiler, denetçi olabilmek için farklı ve spesifik kriterler var.

·         PoA networkü istiyorsak, biz de validator seçimi için kriterler belirlemeliyiz. Yökten alınacak üniversite olunduğuna dair bir belge gibi. Sonra bir de validatörlerin valide olmaları için bir yöntem. Bunda da PoA PoS ya da PoW seçilebilir. Yani yeni eklenecek üniversitenin gerçekten üniversite olup olmadığına kim karar verecek? Şu an biz karar veriyoruz. Bir çeşit PoA yöntemi oluyor, tam merkezi. Fakat hiçbir kriterimiz yok henüz. Tamamen keyfimize kalmış. Merkez (Contrat deployer) hacklenirse de dileyen dilediği kişiye dilediği diplomayı yükleyebiliyor, hiçbir kritere ve validasyon sürecine takılmaksızın.

Eğer PoA ile yapabileceğimiz en ileri şeyi yapsak, hem issuer olmak (Üniversite olmanın ispatı) hem de diplomanın gerçekliği adına mükemmel kriterler ve en adil validatör atanması (PoA ile tek kişi valide edeceğinden, kim edeceğin cevabı, random olabilir en yüksek reputasyon olabilir vs) yöntemini de tasarlasak, şöyle bir de sorunumuz var: Bu kriterler herkes için aynı olmak durumunda. Yani Amerika’da bir üni olmanın kriteri ile TR’de bir üni olmanın kriteri +  Türk ve amerikan diplomalarını validasyon kriterleri aynı olmalı. Bu sorun teknik açıdan, bir çeşit kriter maplemesiyle çözülebilir. Sözde aynı kriter uygulanır, gerçekte bambaşka kriterler. Bu da kimi issuerların diğerlerinden daha avantajlı (örneğin sahte diploma oluşturup bunu gizleyebilir) olabilmelerine olanak tanıyabilir. Yani PoA’nin temel prensiplerinden biri çöker (eşit kriterler).

Şu an bizim geldiğimiz aşamada bunlardan tabi hiçbiri yok, buna karar vermek networkün demokratikliği ve güvenilirliği ile ilgili sanırım en mühim şey.

Öneri:

Herkes veri tabanına (IPFS ya da değil) diploma ve not bilgileri atabilsin. Issuer bilgisi de diploma üzerinde olacağı için, o issuerdan gelen belgeleri verileri kabul edip etmemek, yeni aday öğrencisinin diplomasını inceleyen kurumun insiyatifine terk edilsin. Biz sadece veritabanının (issuer ve öğrenci bilgilerinin doğruluğunu kriptografik doğrulama ile güvenlik altına alalım. Silinemez, değiştirilemez herkese açık vs datalar(IPFS hashi ya da JSON text) da ethereum ortamında bulunsun.

Bu durumda veritabanı şeklen tamamen decentralized oluyor. İşleyişte ise geleneksel kurumların zaruri ihtiyaç duydukları merkezi kontrol olanağı mevcut kalıyor (Uygulamamızı kullanan üniversite, kayıt için blockist platformundan diploma kabul ederken  Yök tarafından yayınlanmış onaylı issuerlar listesini baz alarak belgeleri değerlendirmeye alır/almaz vs gibi).