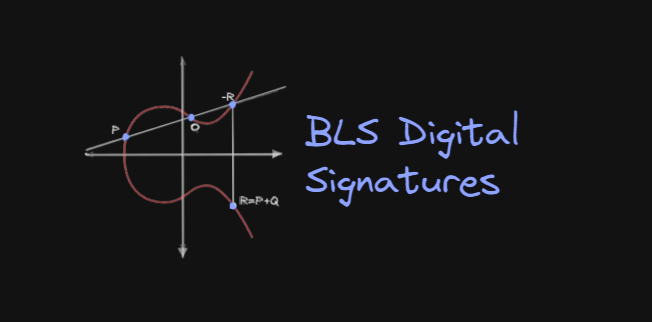
(1/12) Kriptografi 201: BLS Dijital İmzalar

Dijital imzalar, belirli bir kişinin belirli bir mesajı gönderdiğine dair kriptografik güvence sağlar. Blockchain alanının temelinde bulunmalarına rağmen ölçeklenebilirlik sorunu mevcuttur.



(2/12) Boneh-Lynn-Shacham Dijital İmzaları (BLS imzaları) belirli bir dijital imza türüdür.

BLS dijital imzalama, temel imzalama türlerinde bulunan genel yapıyı destekler.

1) Mesaj, mesajı gönderdiğini iddia eden kişiye aittir.

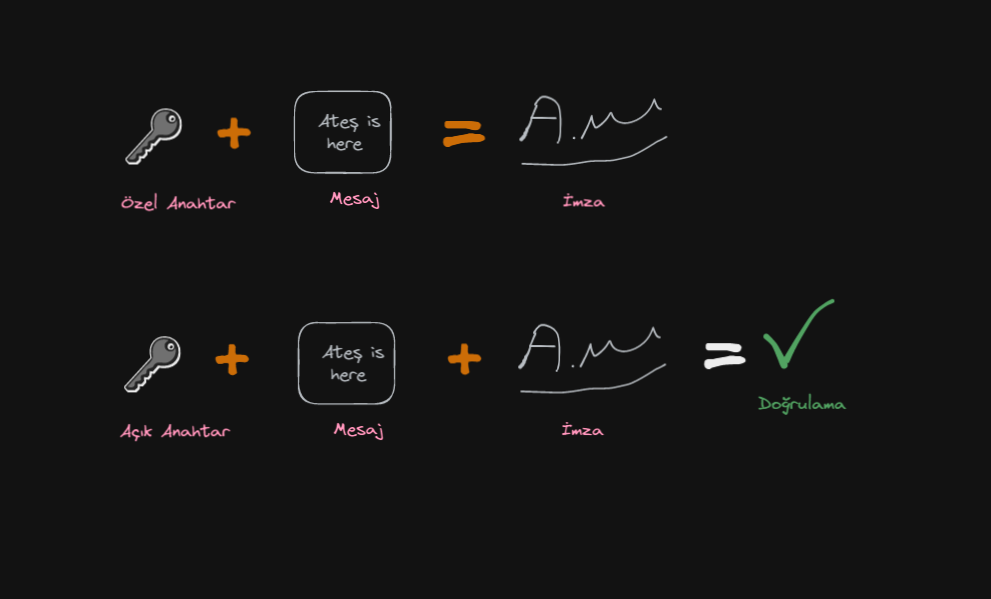
2) Mesaj üzerinde herhangi bir değişiklik yapılmamıştır.

(3/12) Hızlandırılmış dijital imza eğitimi 😊 :

Özel Anahtar + Mesaj = İmza

Açık Anahtar + Mesaj + İmza = Doğrulama

Doğrulama = “Ateş is here” mesajı ATEŞ göndericisi tarafından gönderildi.



(4/12) BLS imzaları standart kriptografik şema olarak (nispeten yavaş olsa da) mükemmel bir şekilde çalışır, ancak asıl sihir birleştirme işleminden gelir.

Birleştirme, tek bir mesaj verildiğinde, birden fazla imzanın tek bir işlemle doğrulanabileceği anlamına gelir.

(5/12) Teknik olarak "imzalar" eliptik eğride belirli bir noktayı temsil eder ve "toplanabilir". Bu (hesaplama açısından) kolay bir işlemdir.

Nihai sonuç eliptik eğride bir noktayı temsil eder ve bu nedenle toplanmamış bir imzadan ayırt edilemez.



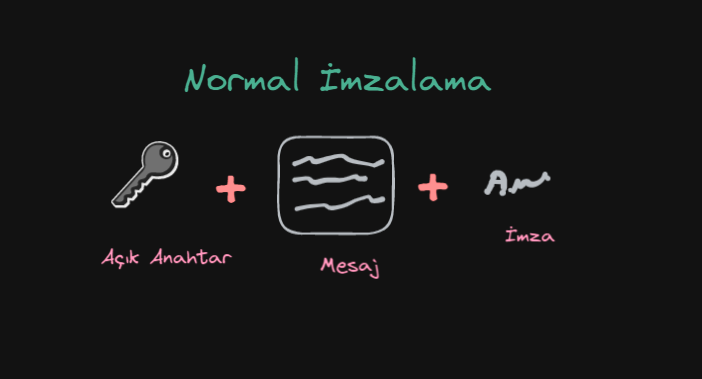
(6/12) İmza gibi "açık anahtar" da eliptik eğri üzerinde bir noktadır ve benzer şekilde "toplanabilir" (hesaplama açısından da kolaydır).

Bir kez daha, toplanmış açık anahtarlar matematiksel olarak toplanmamış açık anahtarlardan ayırt edilemez.



(7/12) Toplu imzalar normal imzalardan ayırt edilemediğinden ve toplu açık anahtarlar normal açık anahtarlardan ayırt edilemediğinden, normal doğrulama algoritmamızı yeniden kullanabiliriz.

Böylece tek bir işlemle çok sayıda imza doğrulanabilir.



(8/12) Daha önce de belirtildiği gibi, BLS imzaları daha standart bir şemayı doğrulamakla karşılaştırıldığında hesaplama açısından pahalıdır - bir büyüklük sırasından daha yavaştır.

Bununla birlikte, her bir doğrulama standart bir şemadan (tek bir doğrulama) ÇOK daha fazla sayılabilir.

(9/12) 100 imzayı doğrulamanız gerektiğini düşünün:

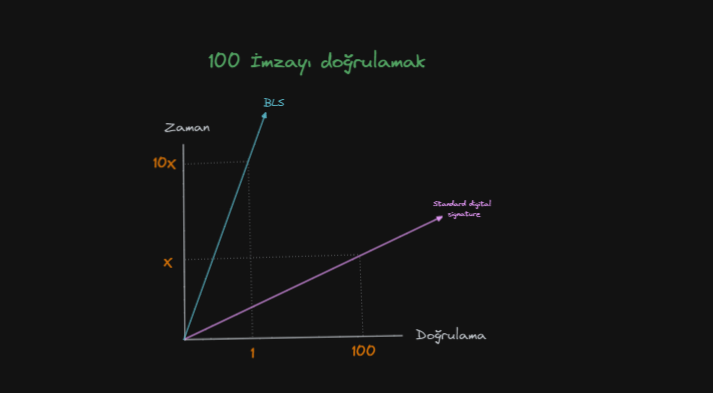
Standart dijital imza:

x zaman/doğrulama \* 100 doğrulama = 100x

BLS dijital imzası:

10x zaman/doğrulama \* 1 doğrulama = 10x

Ne kadar çok imzayı bir araya getirebilirseniz, tasarruf o kadar yüksek olur



(10/12) Ancak doğrulama hızı tek avantaj değildir: BLS imzaları, bir araya getirilmemiş imzalara göre büyük alan tasarrufu sağlar.

Birleştirilmiş imzalar, kaç imzanın bir araya getirildiğine bakılmaksızın tek bir imza ile aynı boyuttadır.

(11/12) 100 imzayı doğrulamanız gerektiğini düşünün:

Standart dijital imza:

x bayt/imza \* 100 imza = 100x

BLS dijital imzası:

x bayt/imza \* 1 imza = x

Daha fazla birleştirme, daha fazla tasarruf anlamına gelir. BLS hızdan daha çok alanla öne geçmeyi hedefler.



(12/12) BLS imzaları, herhangi bir imza ile aynı garantileri sağlayan (özgünlük ve canlılık) ancak büyük imza gruplarını doğrularken büyük ölçeklendirme avantajları sağlayan bir dijital imza türüdür.

Çok sayıda dijital imza kullanan herhangi bir şey düşünebiliyor musunuz?