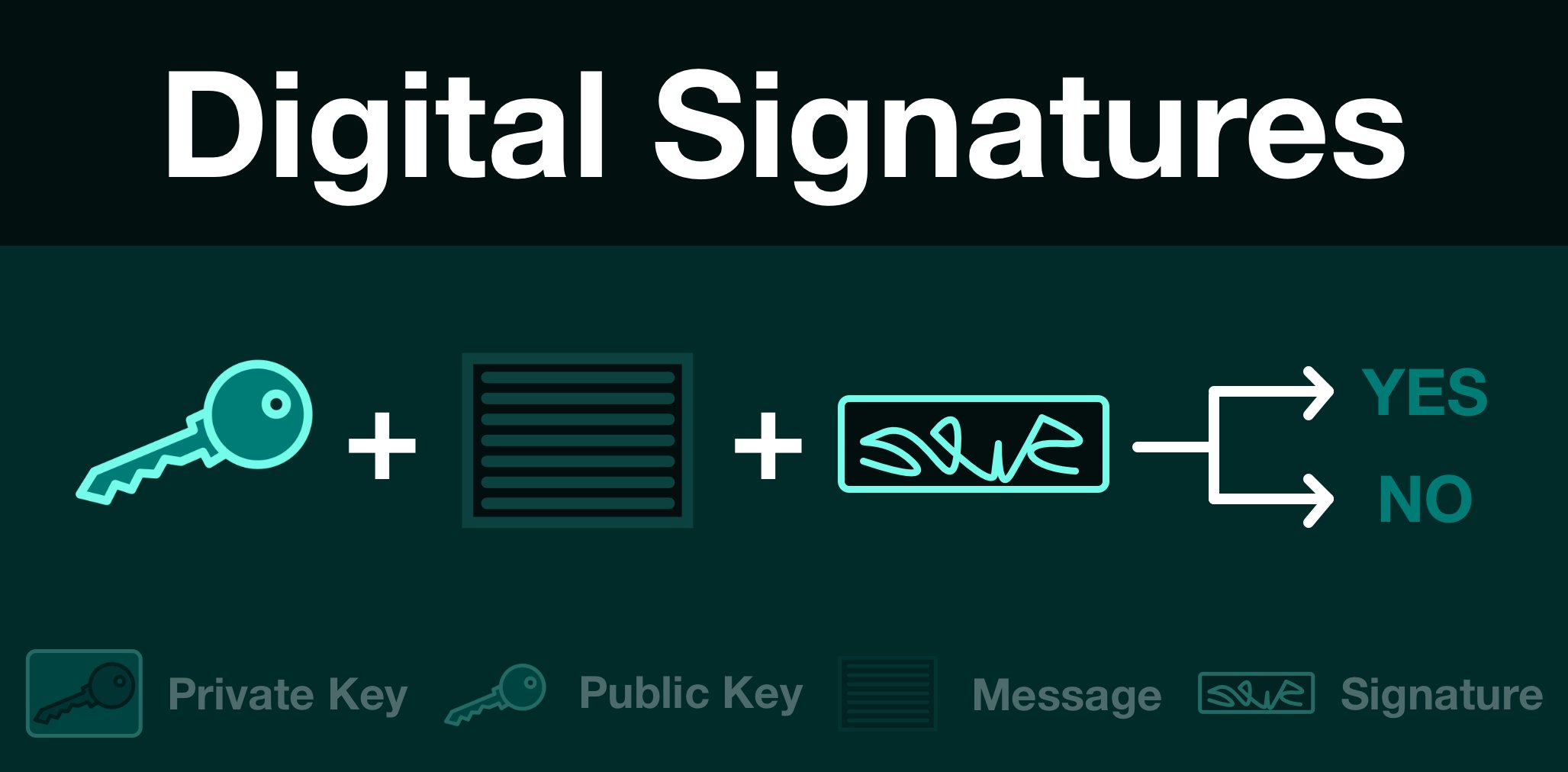
(1/7) Kriptografi 101: Dijital İmzalar

İnternet Vahşi Batı... Bir verinin kime ait olduğunu nereden anlayabiliriz? Verilerin değiştirilmediğinden emin olabilir miyiz? Güvensiz bir ortamda nasıl güven yaratabiliriz?

Dijital özgünlük ve bütünlük üzerine bir başlangıç.



(2/7) Dijital imza, iki şeyi kamuya açık bir şekilde teyit etmek için bir tarafça oluşturulan benzersiz bir bilgi parçasıdır:

1) mesajın gerçekten onu gönderdiğini iddia eden kişi tarafından gönderilmiş olması (özgünlük)

2) mesajın üzerinde herhangi bir değişiklik olmaması (bütünlük)

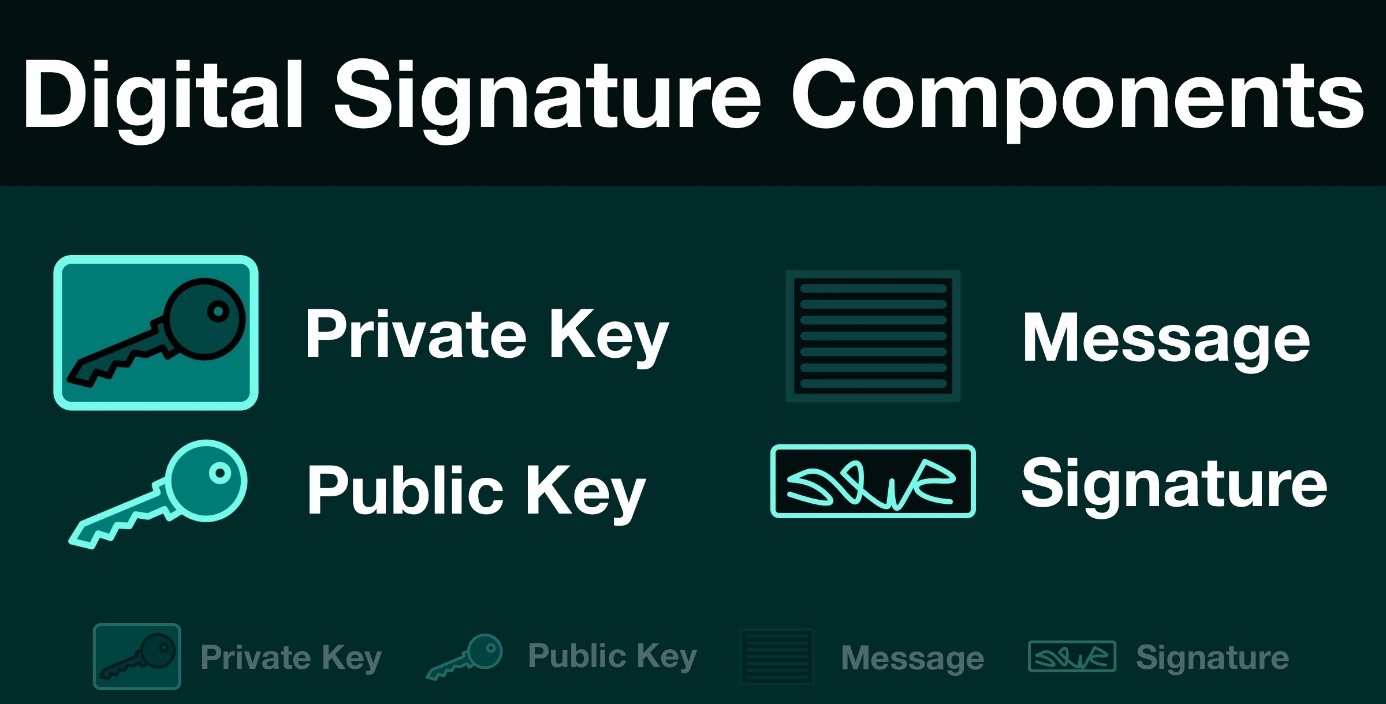
(3/7) Dijital bir imza için 4 gereklilik vardır:

Private Key - imza oluşturmak için kullanılan gizli kod

Public Key - imzaları doğrulamak için kullanılan ortak kod

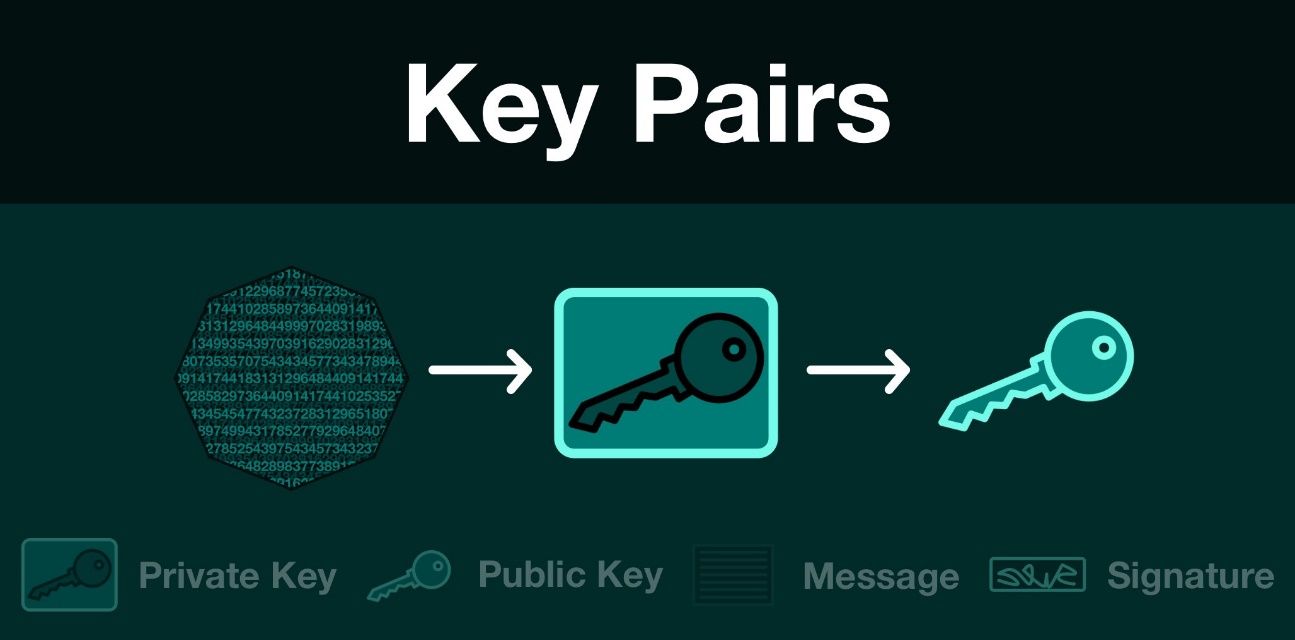
Message - imzanın onayladığı veri

Signature - kriptografik olarak güvenli doğrulama



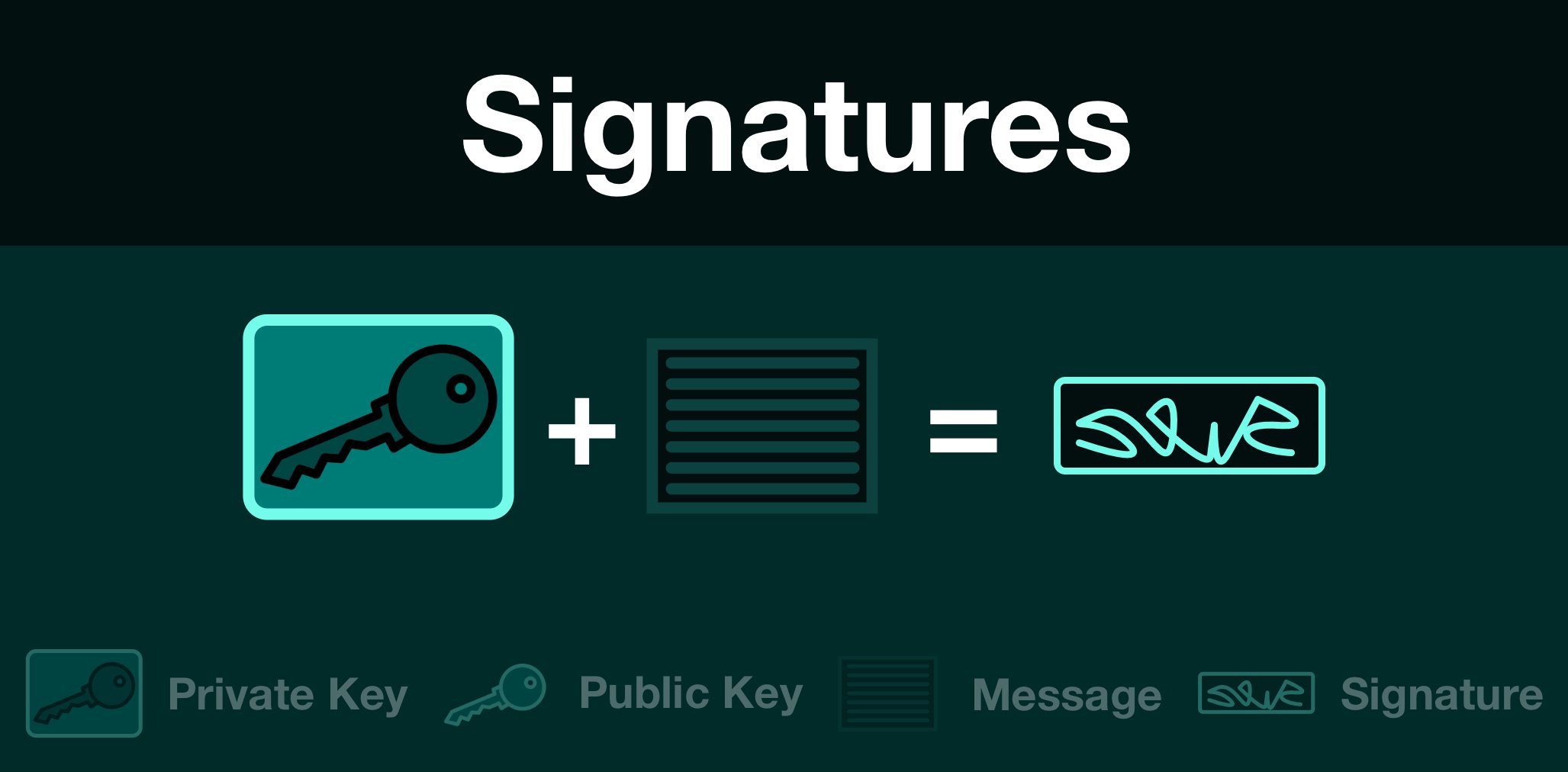
(4/7) Süreç bir özel anahtar (rastgele oluşturulmuş büyük bir sayı) üretilerek başlar.

Eliptik eğri kriptografisi kullanılarak, açık anahtar özel anahtardan türetilir. Bu tek yönlü bir işlemdir; bir kez tamamlandığında, bir özel anahtar bir açık anahtardan ayrılamaz,değiştirelemez



(5/7) Mesaj, rastgele bir veri grubudur. Örneğin metin, kod veya birkaç rakam bu grubu oluşturabilir.

İmzalayan kişi kendi özel anahtarını göndermek istediği mesaja bağlayarak bir imza oluşturur. İmza hem özel anahtar (imzalayan) hem de mesaj için benzersizdir.



(6/7) Bir imza, imzalayanın açık anahtarına, mesaja ve imzaya kriptografik doğrulama uygulanarak doğrulanır.

Bu doğrulama sisteminde bütün veriler doğrulanırsa imza geçerli sayılır. Aksi bir durumda sorun olduğunu anlamamız gerekir. Örneğin mesaj değiştirilmiş ya da imzayı başka biri oluşturmuş olabilir.

(7/7) Bilgisayar bilimlerinde kullanılan birçok farklı türde dijital imza şeması vardır. Farklı şemaların farklı zafiyetleri vardır, ancak hepsinde bazı temel gereksinimler vardır:

Proof of Authenticity- Mesajın bilinen bir gönderici tarafından gönderilmesidir.

Proof of Integrity- Mesajın değiştirilmemiş olmasıdır