Hibrit Cüzdanlar

Mustafa Sakalsız - T2 Yazılım
Dr. Kamer Kaya - Sabancı Üniversitesi

Blockchain - Projeler

BBN Projesi

Dijital Kimlik
Kripto Para (Keklik)
Pazar Yeri
Mobil Light Wallet

B*** Projesi

Zero Knowledge Proof
Cüzdan

Blockchain - Hackathon

BNP PARIBAS

alBaraka

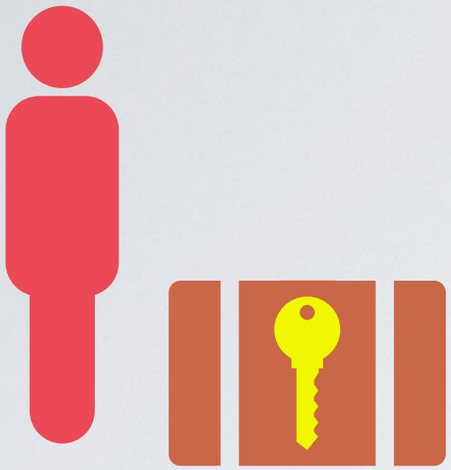
Bondchain

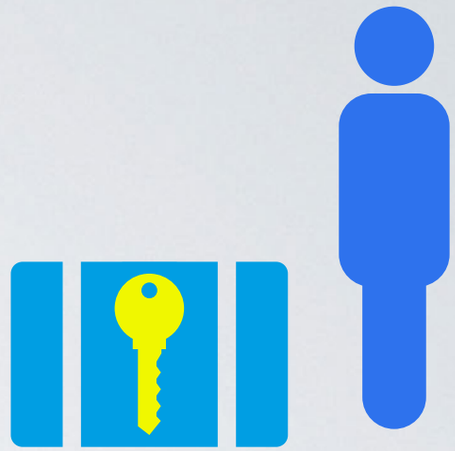
Dijital Çek-Senet
3.'lük Derecesi
Jüri Özel Ödülü

Goldchain

Uluslararası Dijital Altın Hesabı
4.'lük Derecesi

Genel Bir Cüzdan Yapısı

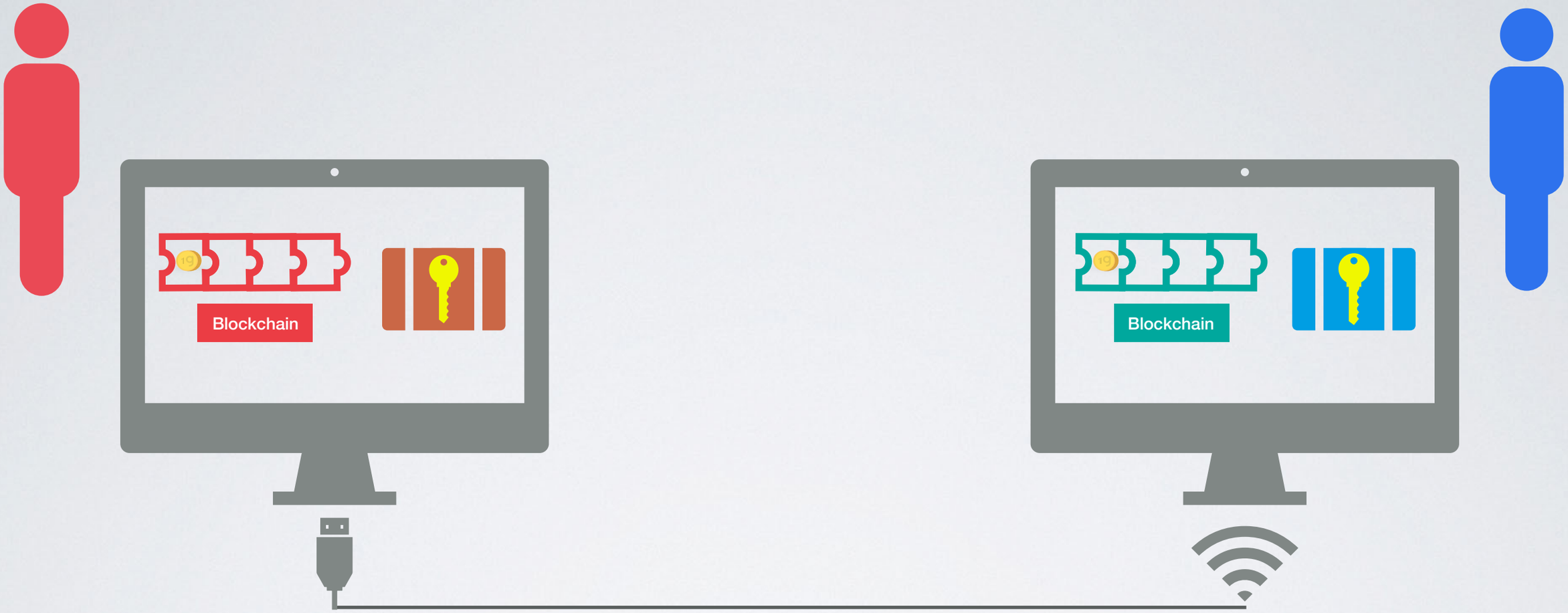




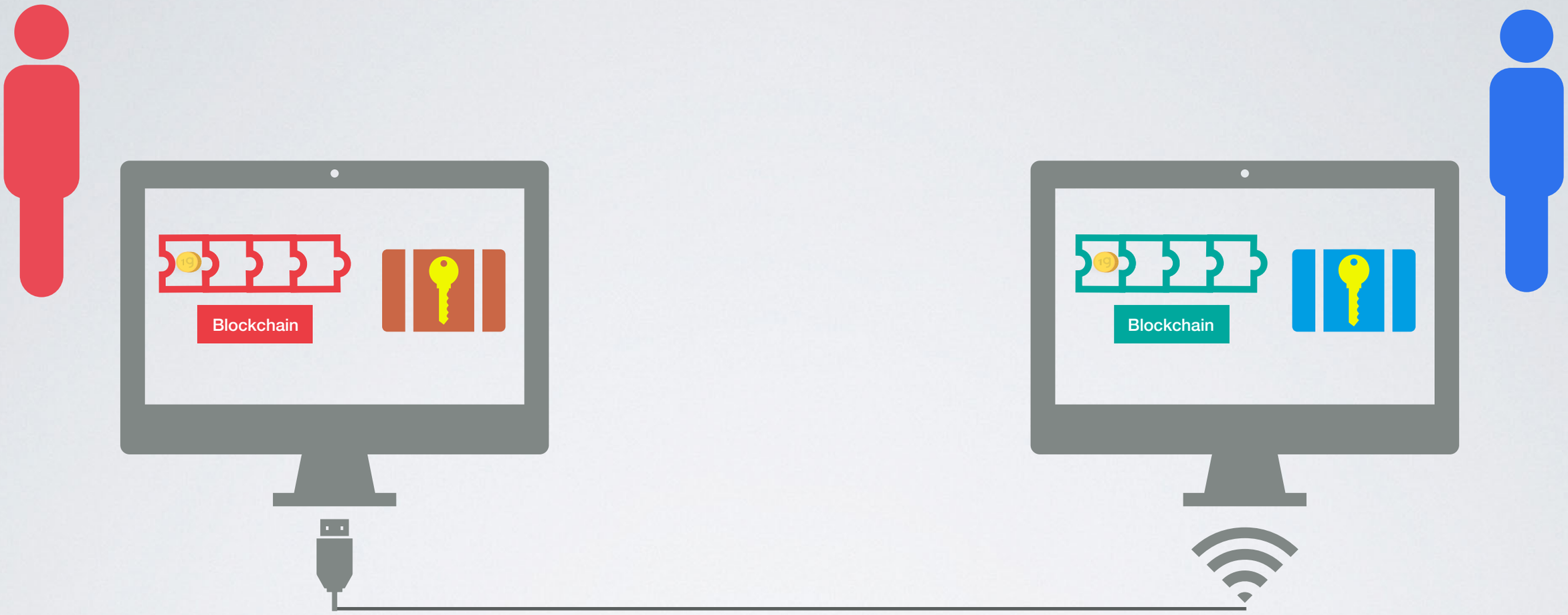
Genel Bir Cüzdan Yapısı

Genel Bir Cüzdan Yapısı

Cüzdanın Çalışması

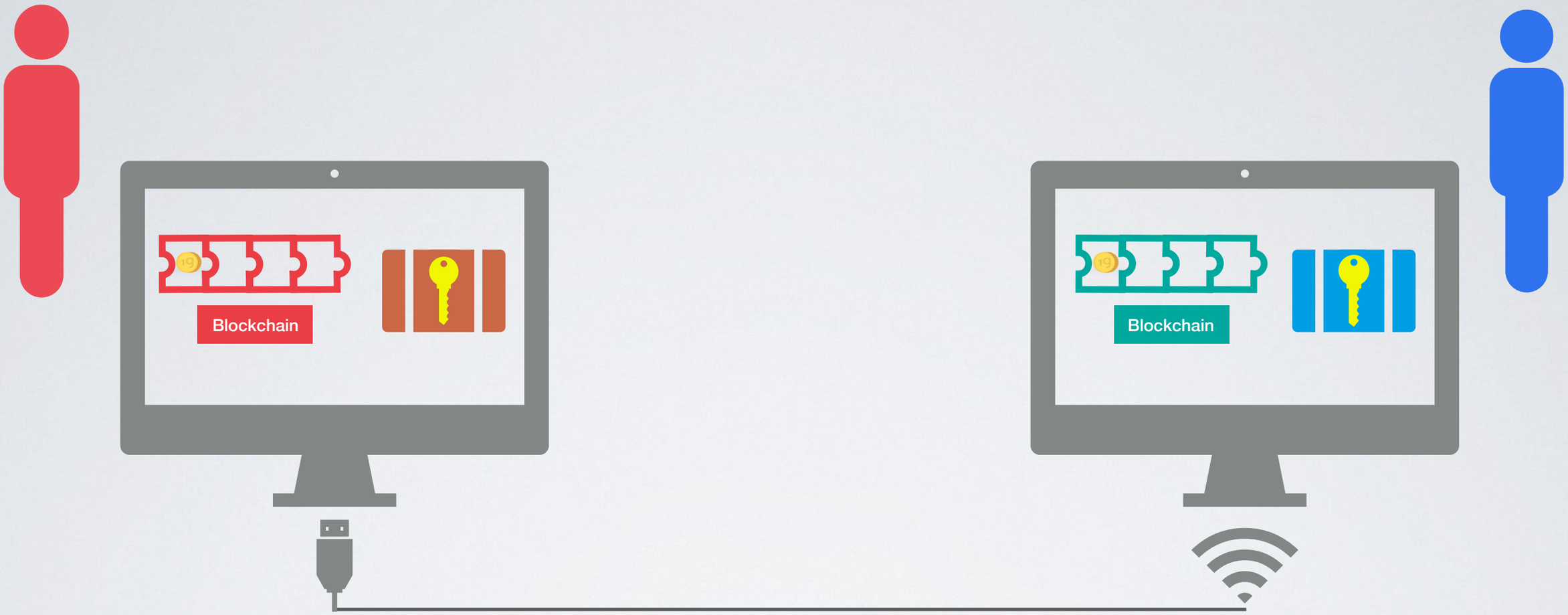


Cüzdanın Çalışması

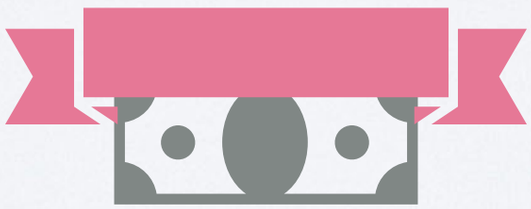


İşlemi Oluşturma

Cüzdanın Çalışması

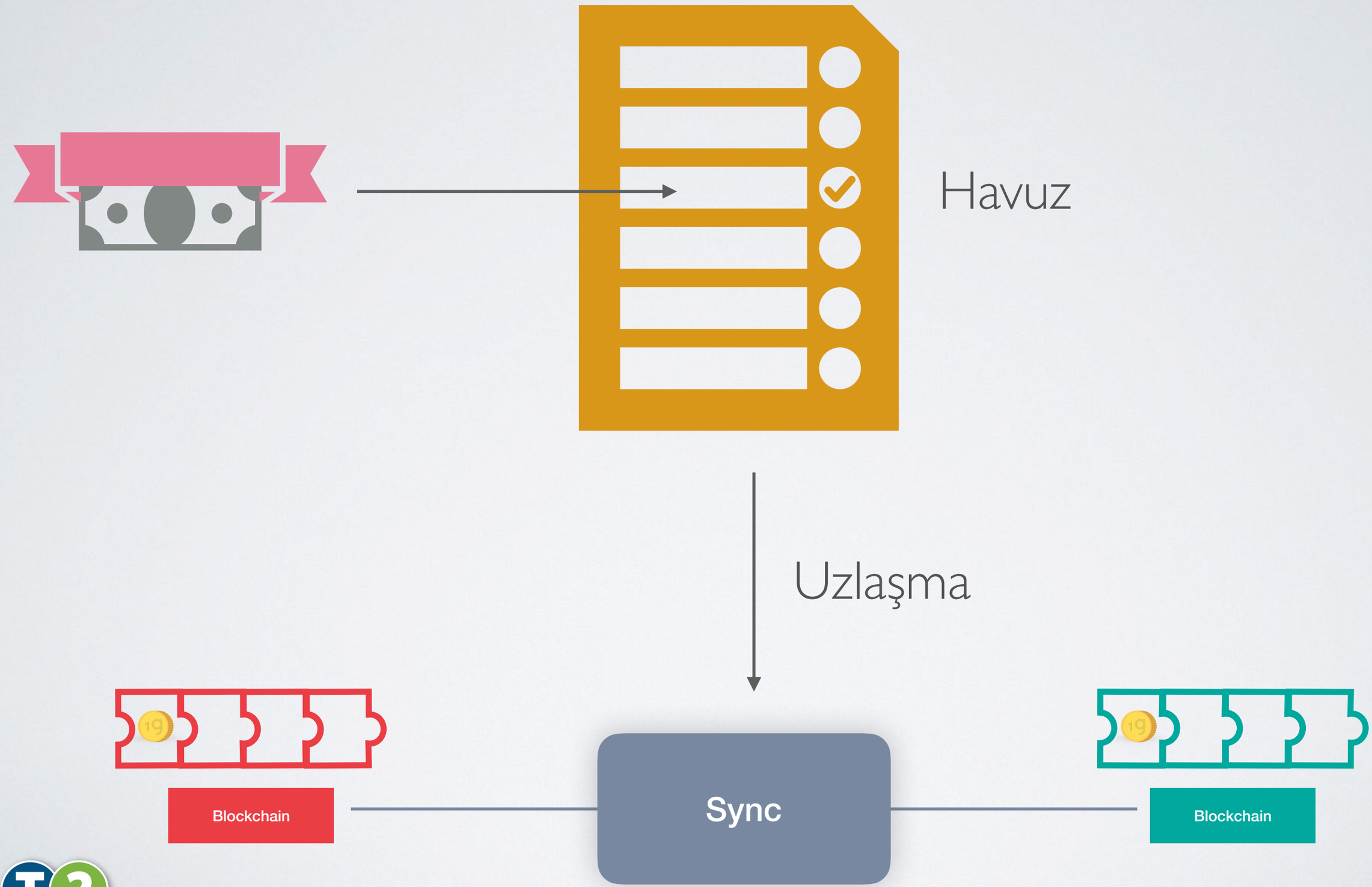


İmzalama

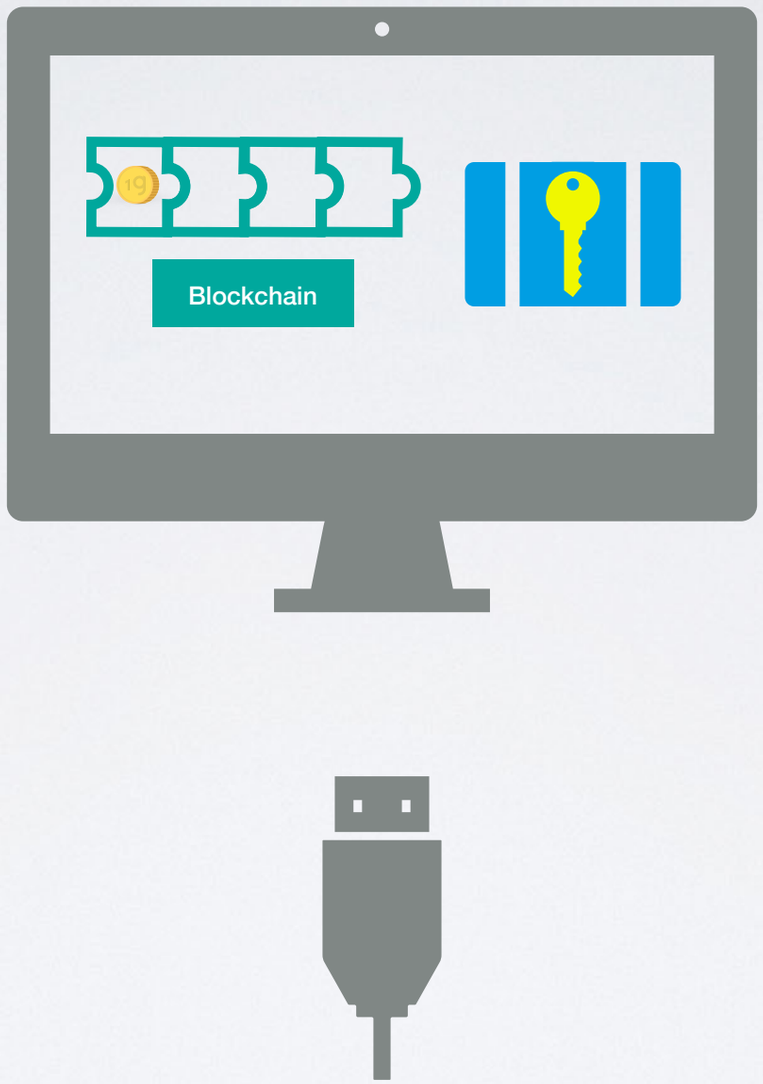


Cüzdanın Çalışması

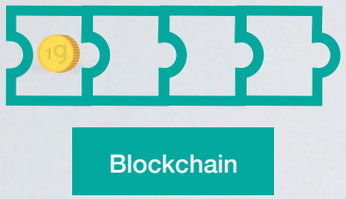
Genel Bir Cüzdan Yapısı



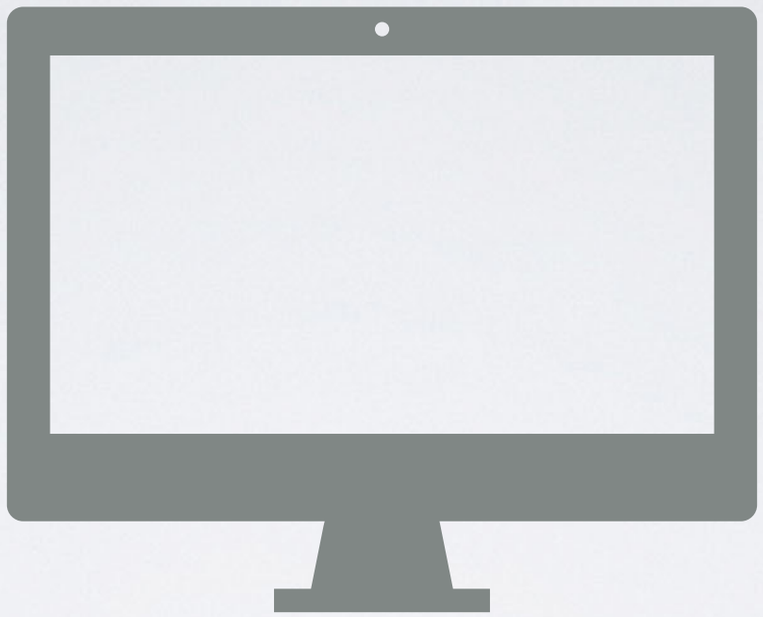
Genel Bir Cüzdan Yapısı



Genel Bir Cüzdan Yapısı



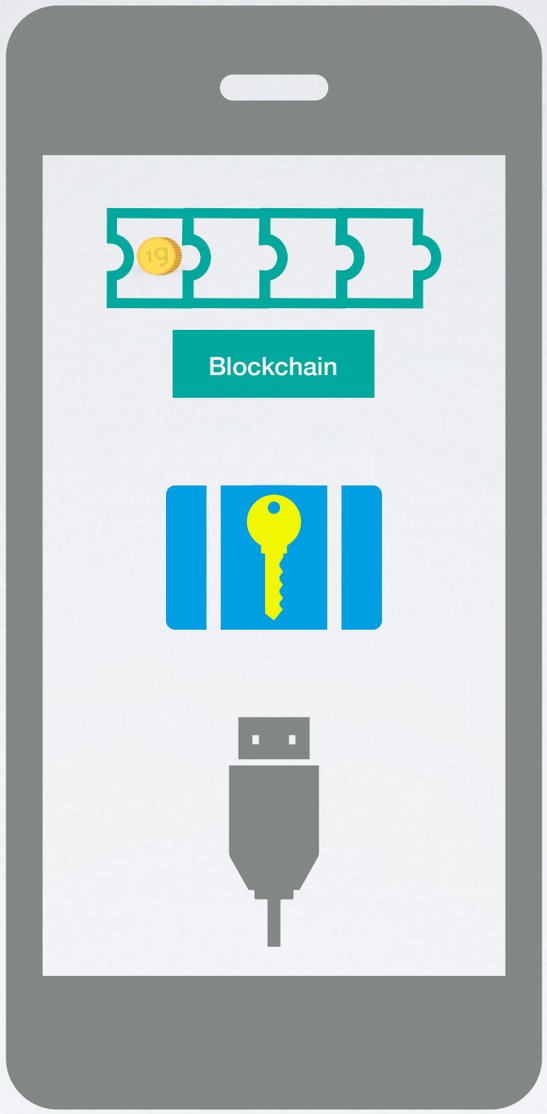
Tüm Geçmiş



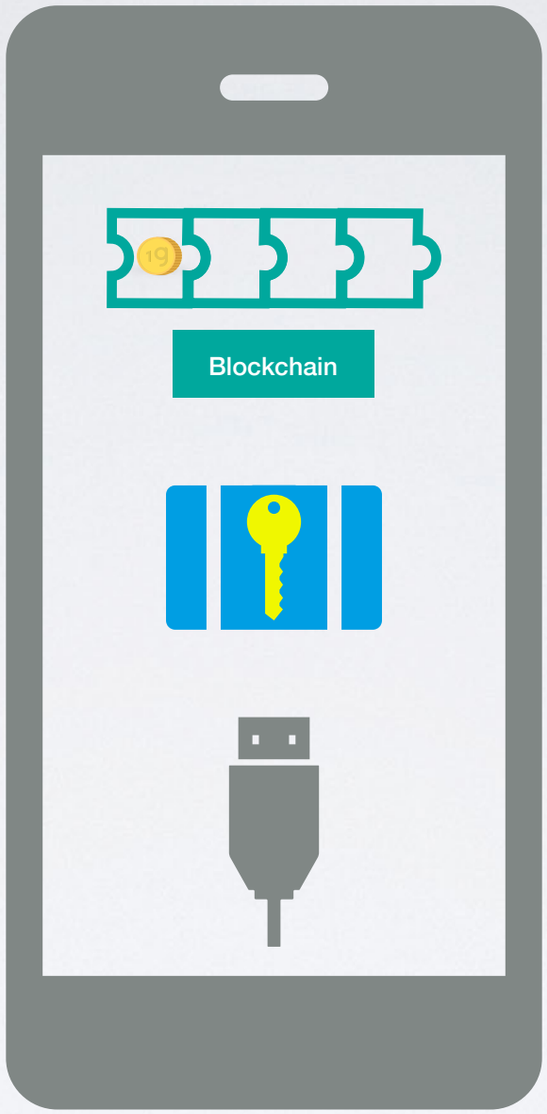
Gizli Anahtar

Sürekli Bağlantı

Mobilde Cüzdan

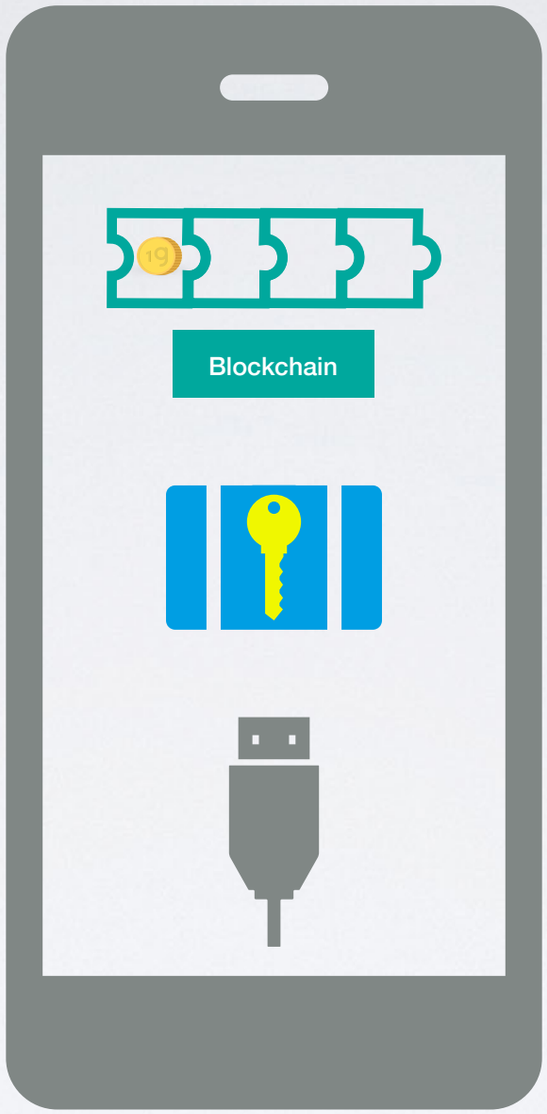


Mobilde Cüzdan



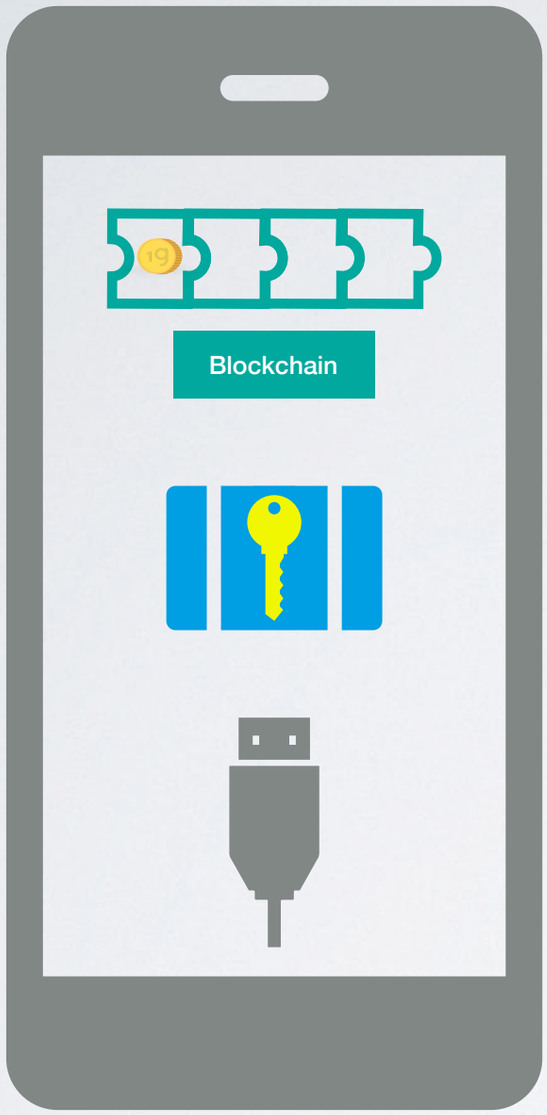
?

Mobilde Cüzdan



Uygun Değil

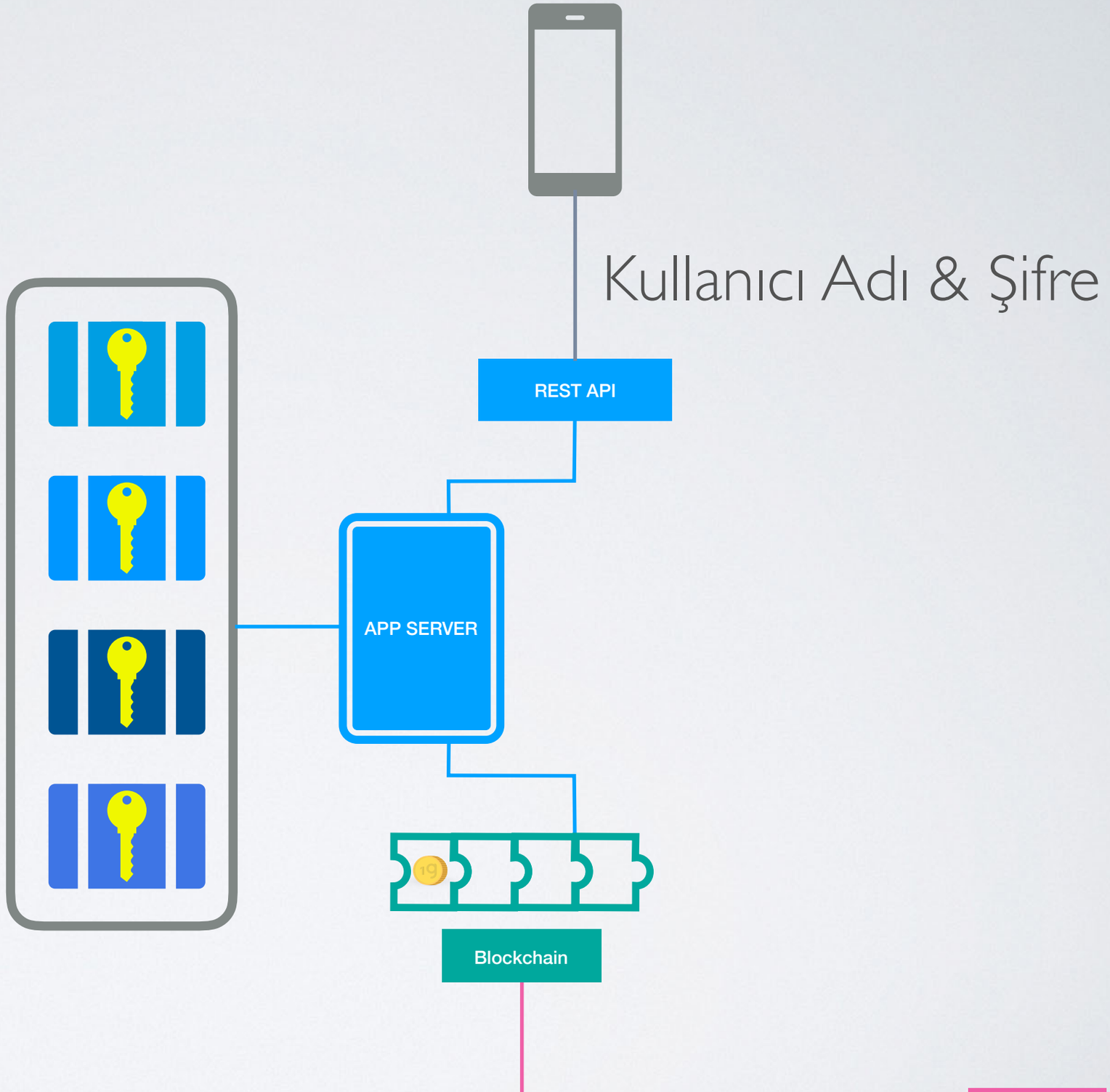
Mobilde Cüzdan



Uygun Değil

- Veri Depolama
- Sürekli Bağlantı
- Private Key Silinmesi/Kaybolması
- Pil Kullanımı

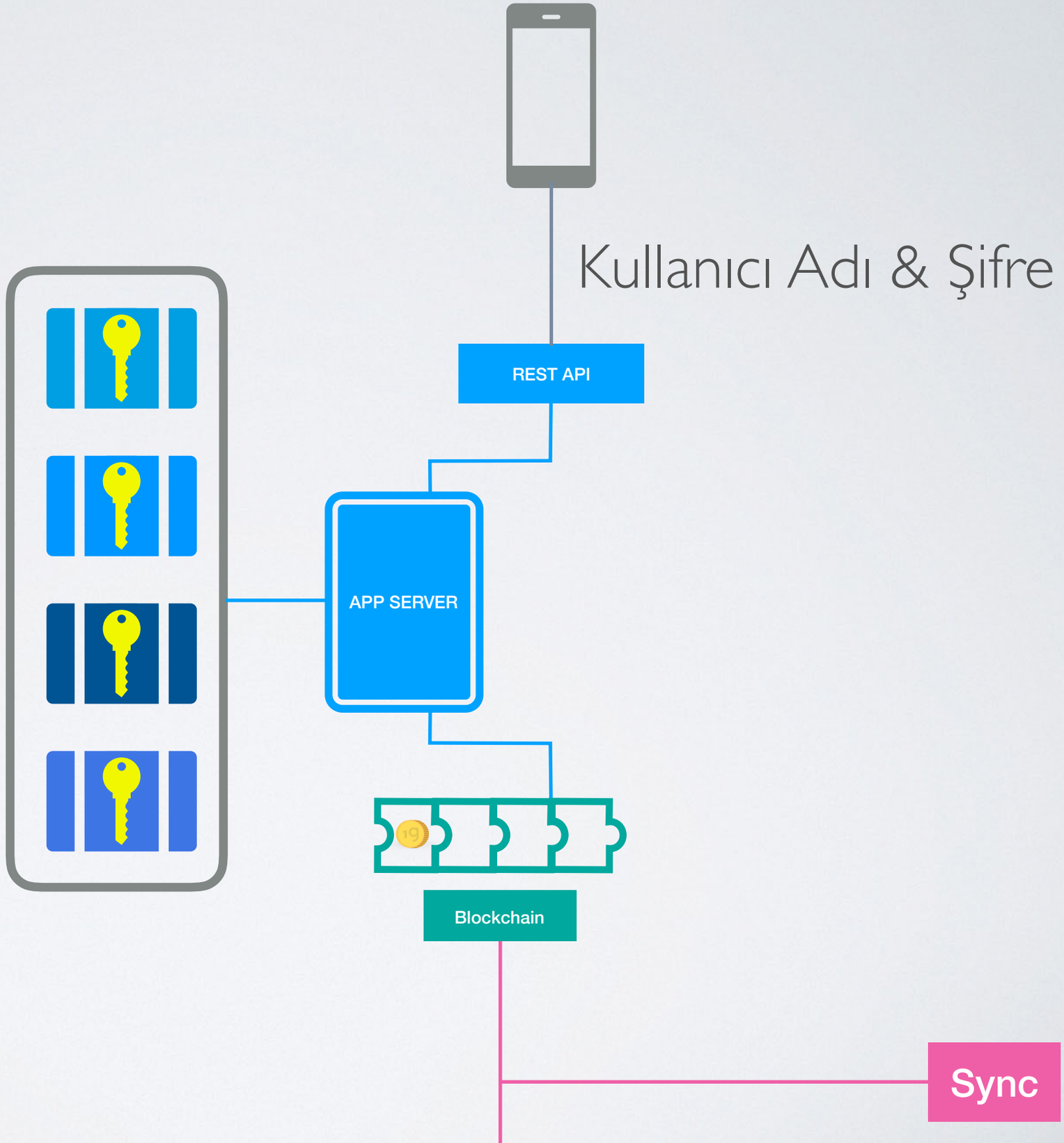
Bulutta Cüzdan Hizmeti



Bulutta Cüzdan Hizmeti

Sorunlar

- Kullanıcı varlıkların gerçek sahibi olmuyor
- Çalınma durumunda tüm anahtarlar beraber çalınıyor



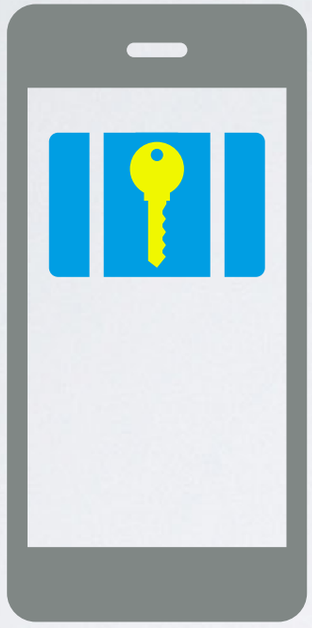
İdeal Senaryo

Varlıkların gerçek sahibi kullanıcı olmalı

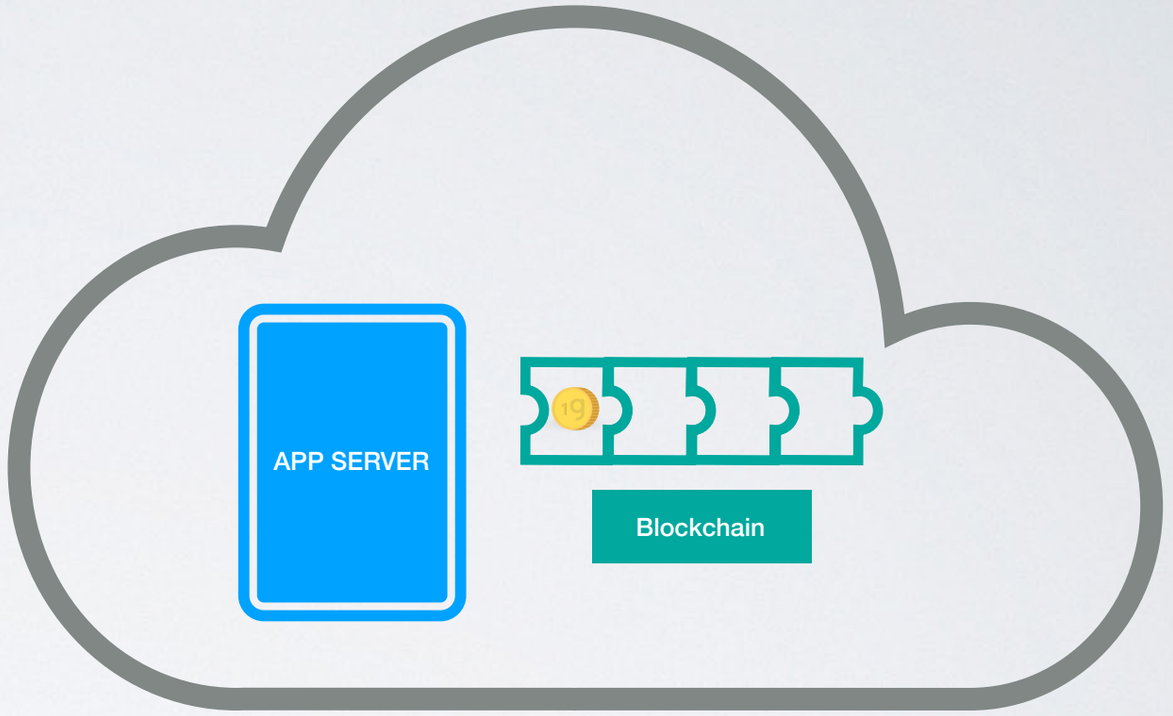
Tarihçe ve büyük veri telefonda tutulmamalı

Telefonun sürekli bağlı olmaya ihtiyacı olmamalı

Hibrit Cüzdan

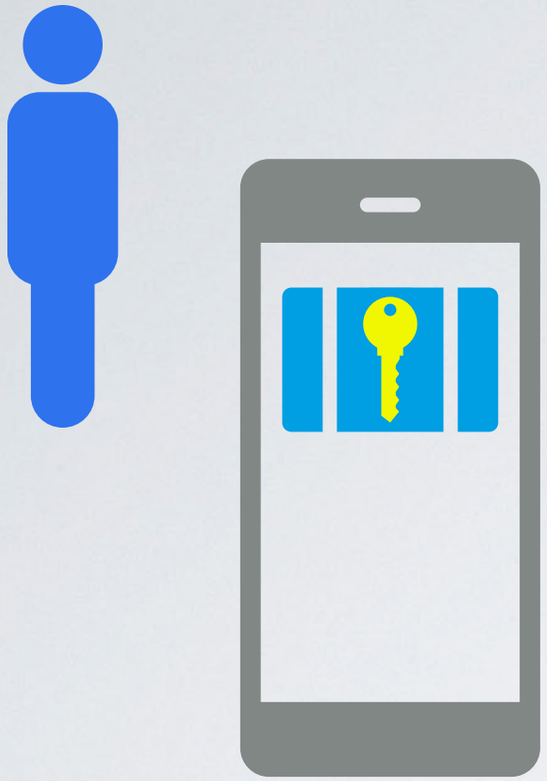


İmzalama

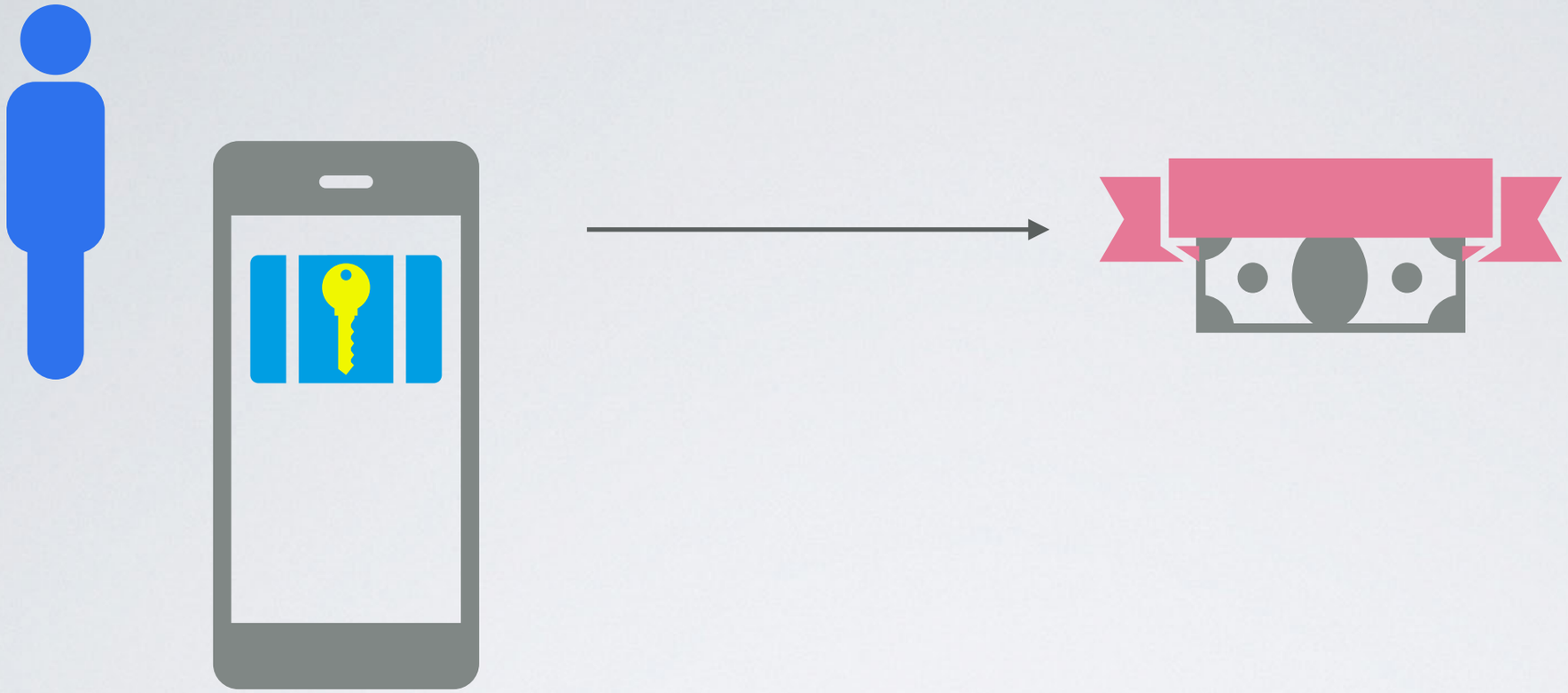


Diğer İşlemler (Sandbox)

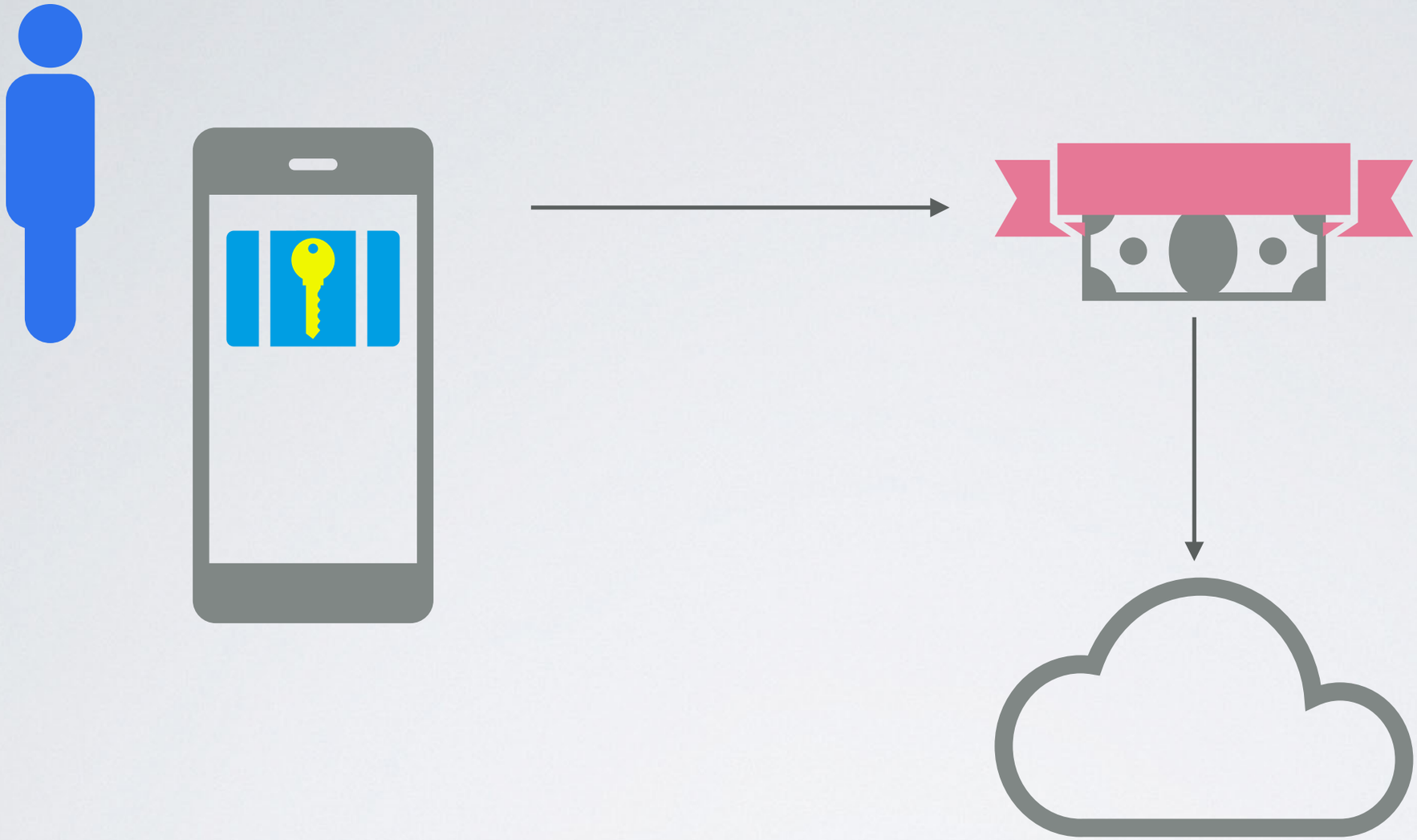
Para Gönderme



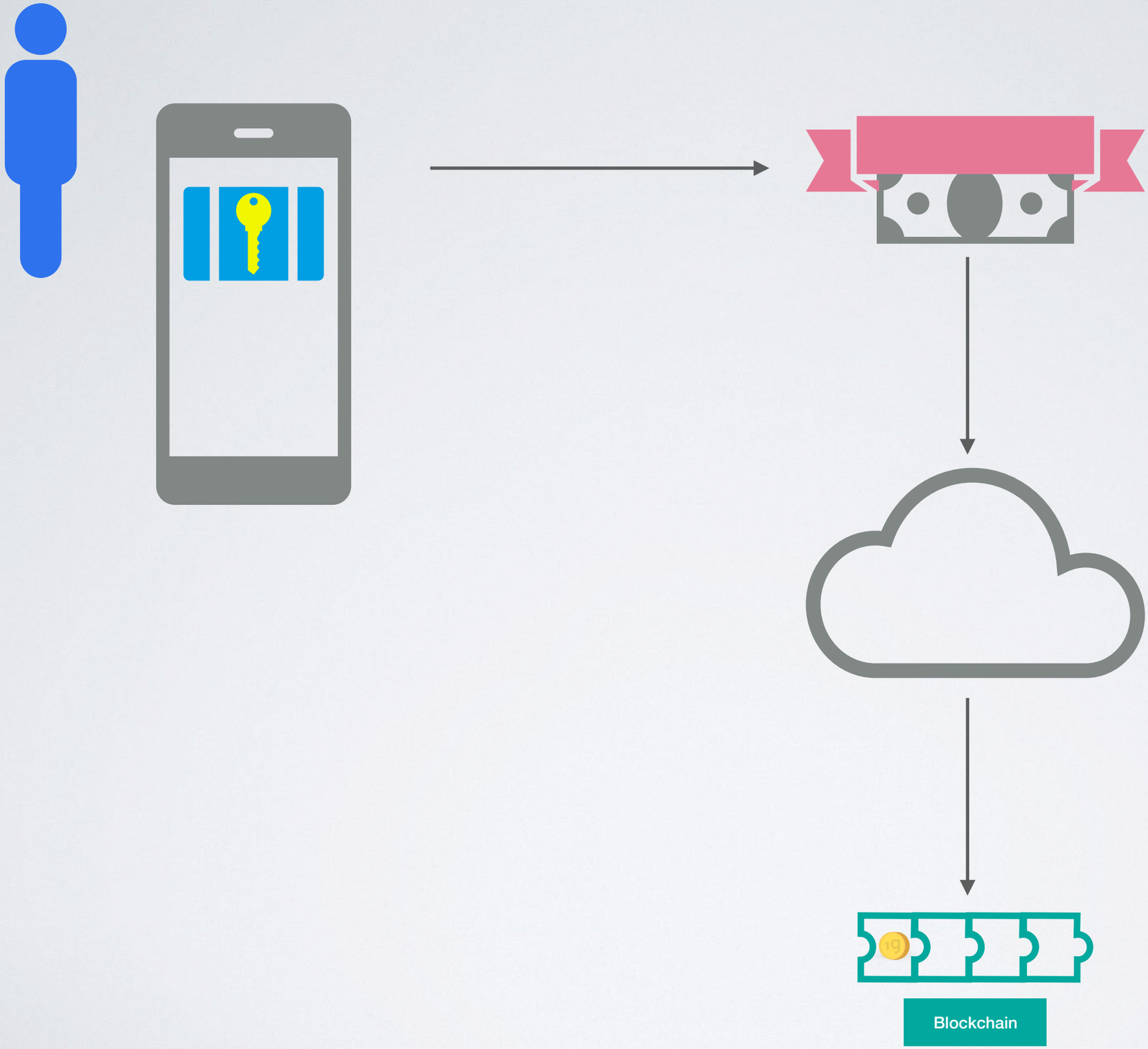
Para Gönderme



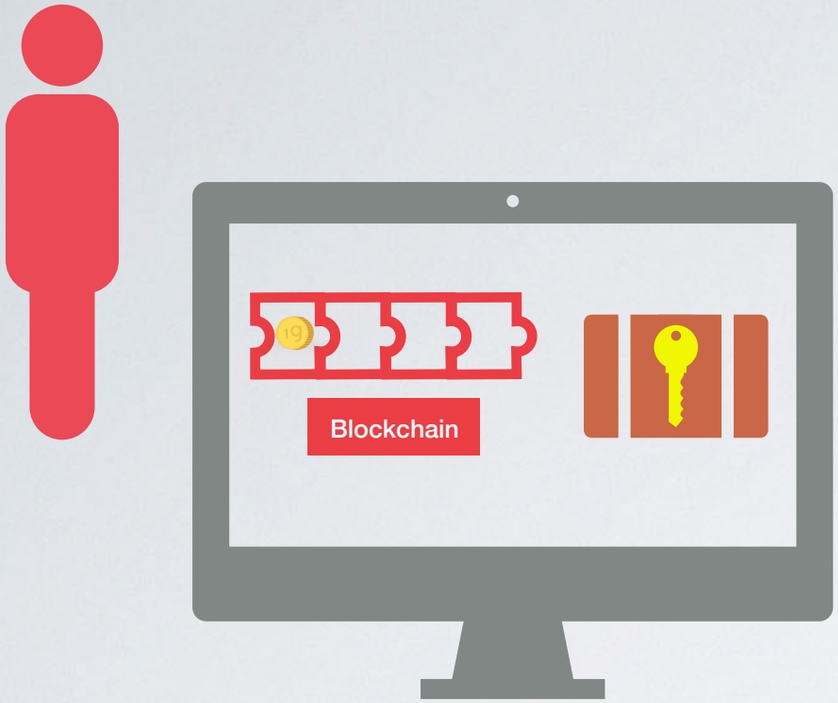
Para Gönderme



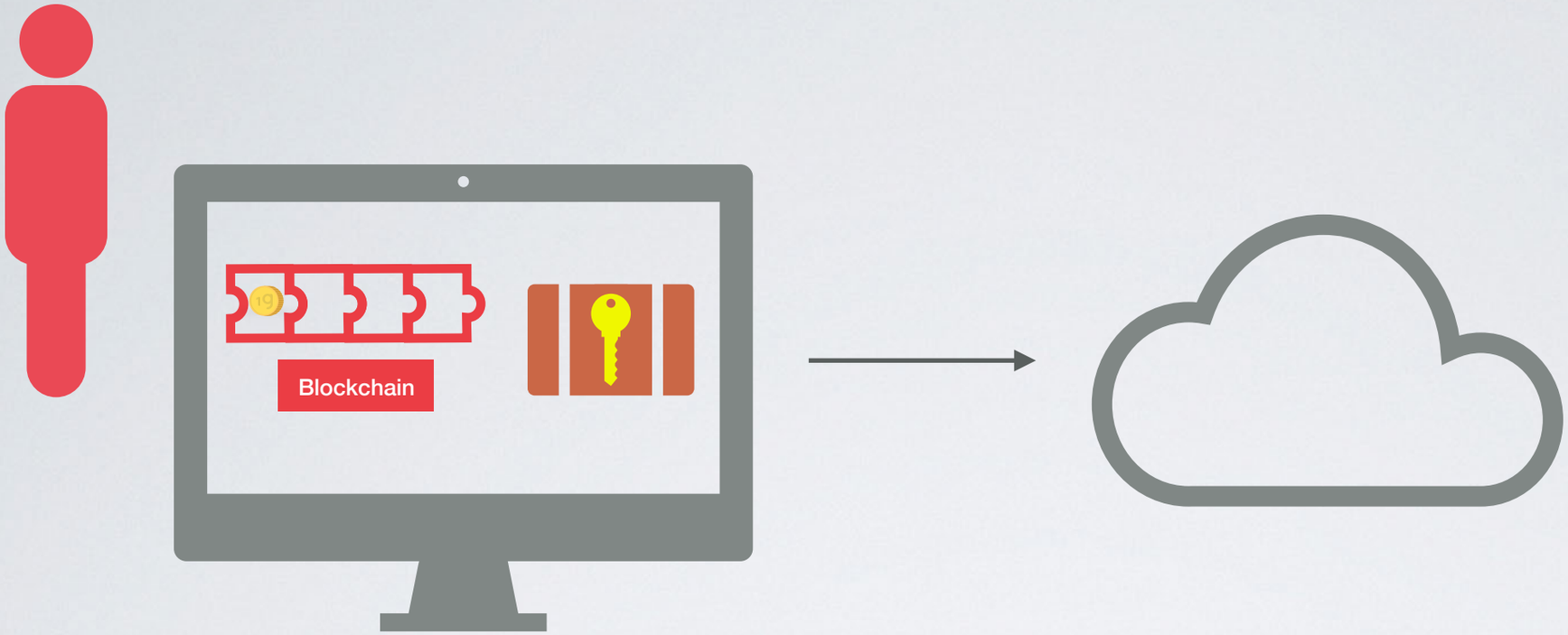
Para Gönderme



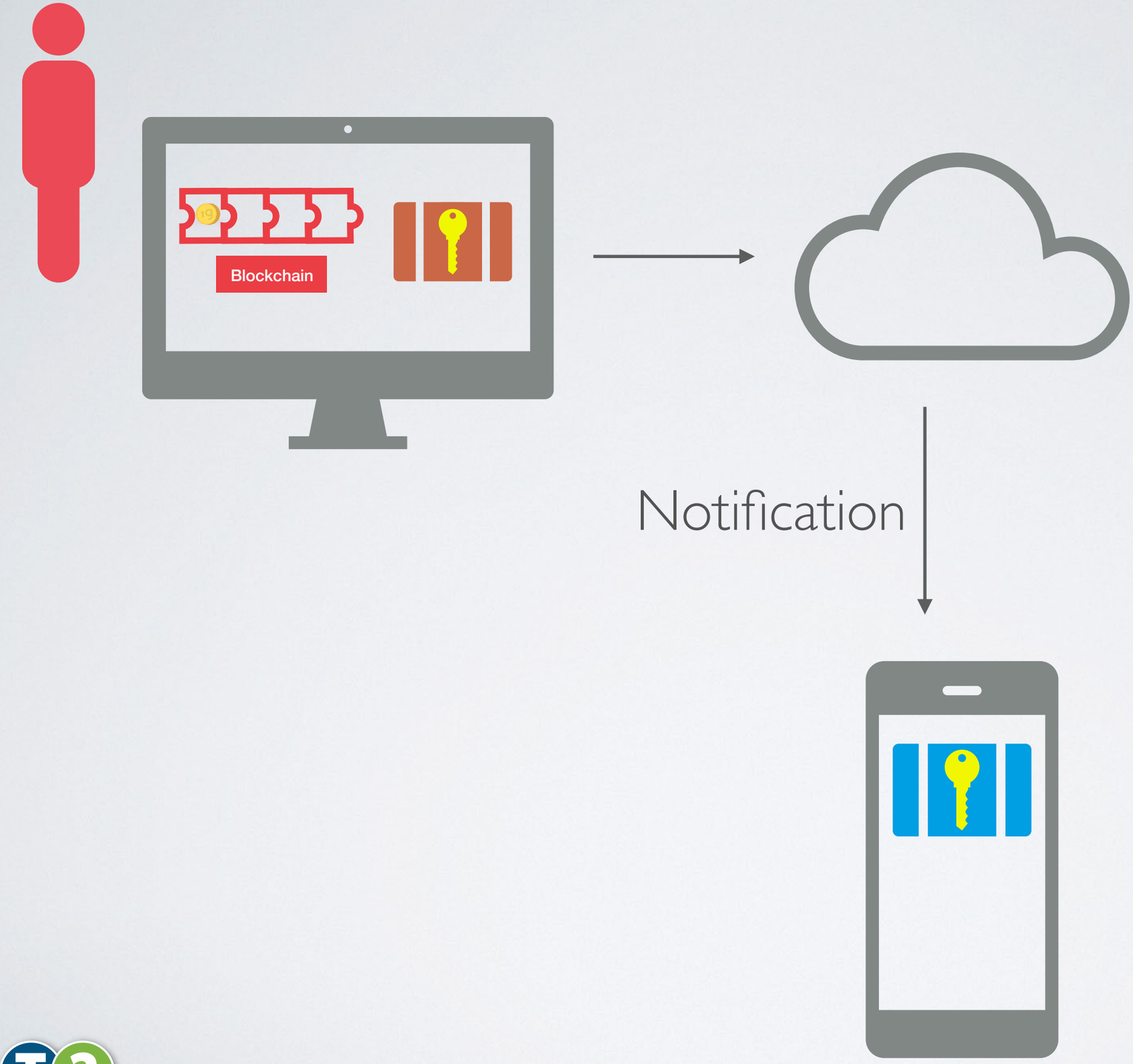
Çift İmza



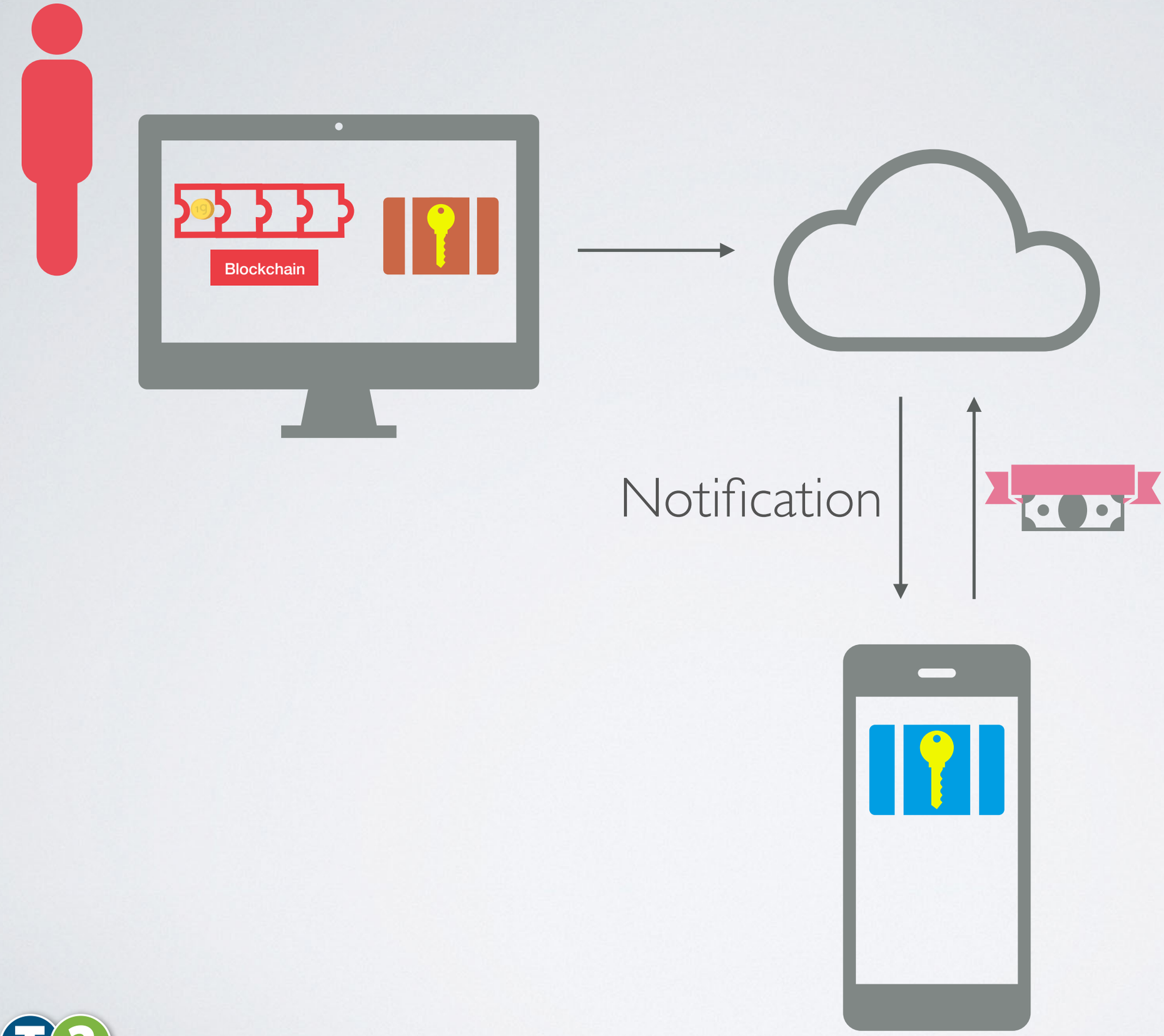
Çift İmza



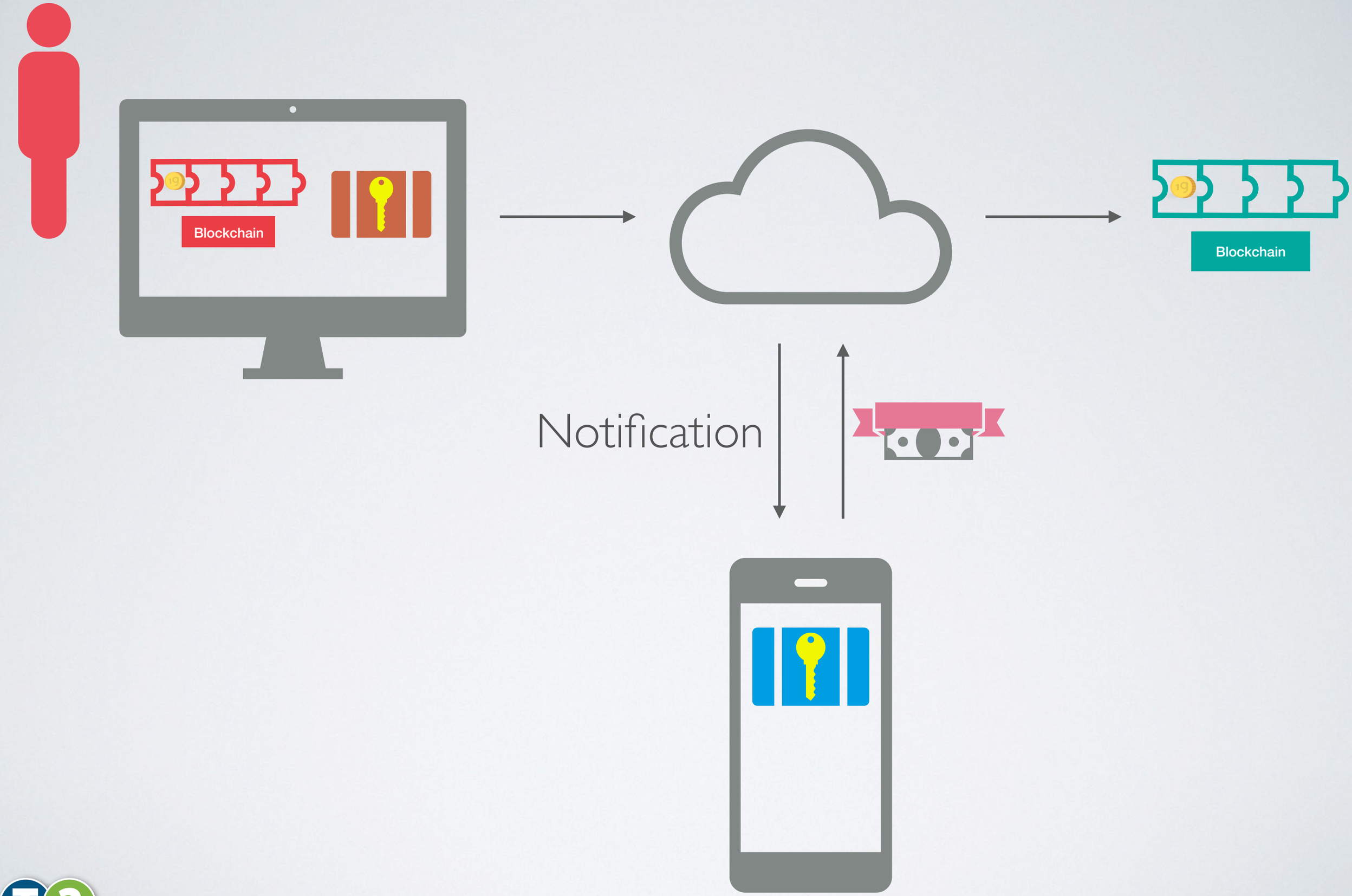
Çift İmza



Çift İmza



Çift İmza



Politika Tabanlı İmzalama

Belli koşulları tanımlayabilsin

Koşullar geçerli ise otomatik imzalasın

Kullanıcının gizli anahtarı asla açığa çıkarılamayacak

Politika Tabanlı İmzalama

- Serialized [0,1]*
- Domain Specific Language

Politika

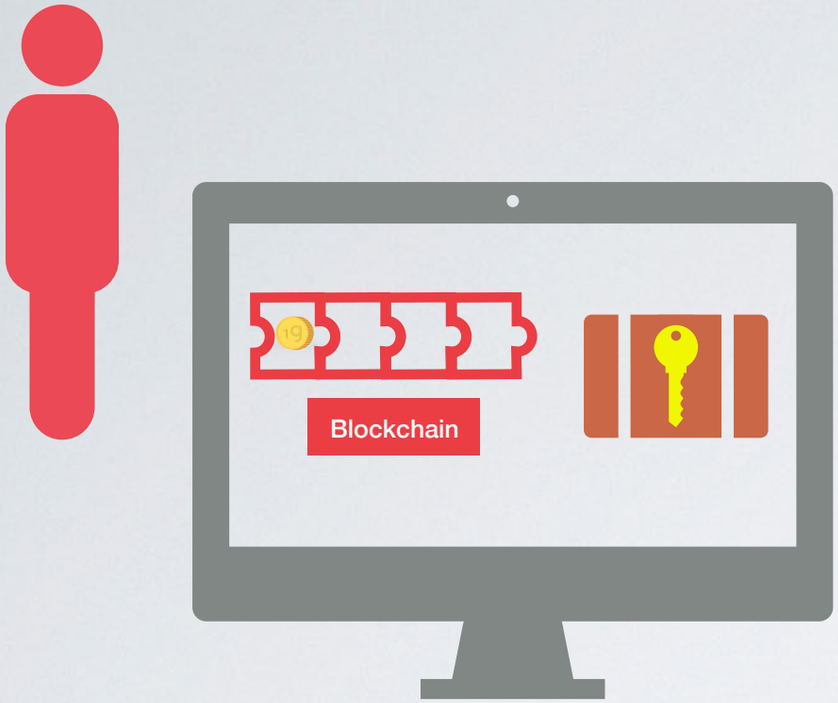
Örnek: Ali'den gelen tüm işlemleri kabul et.

Politika Tabanlı İmzalama

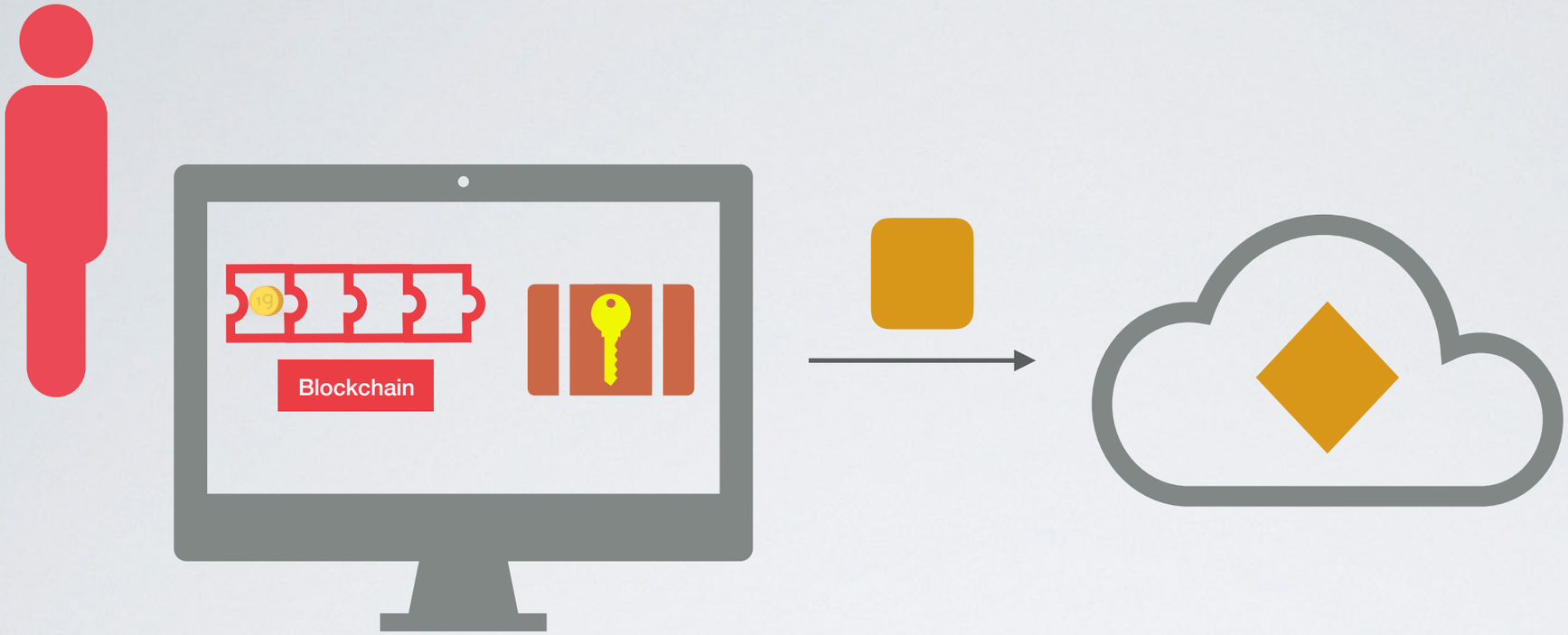
Politika İşlem/İstek İmzalanmış İşlem

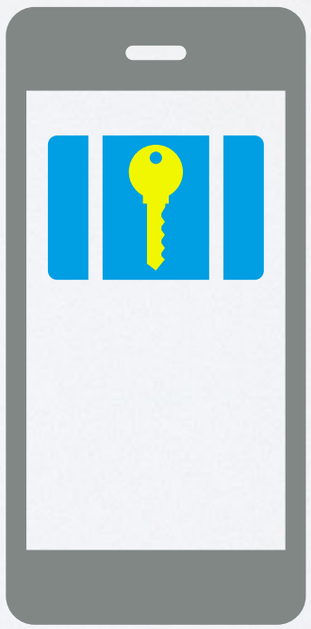
*Non-Interactive Zero Knowledge Proof

Politika Tabanlı İmzalama

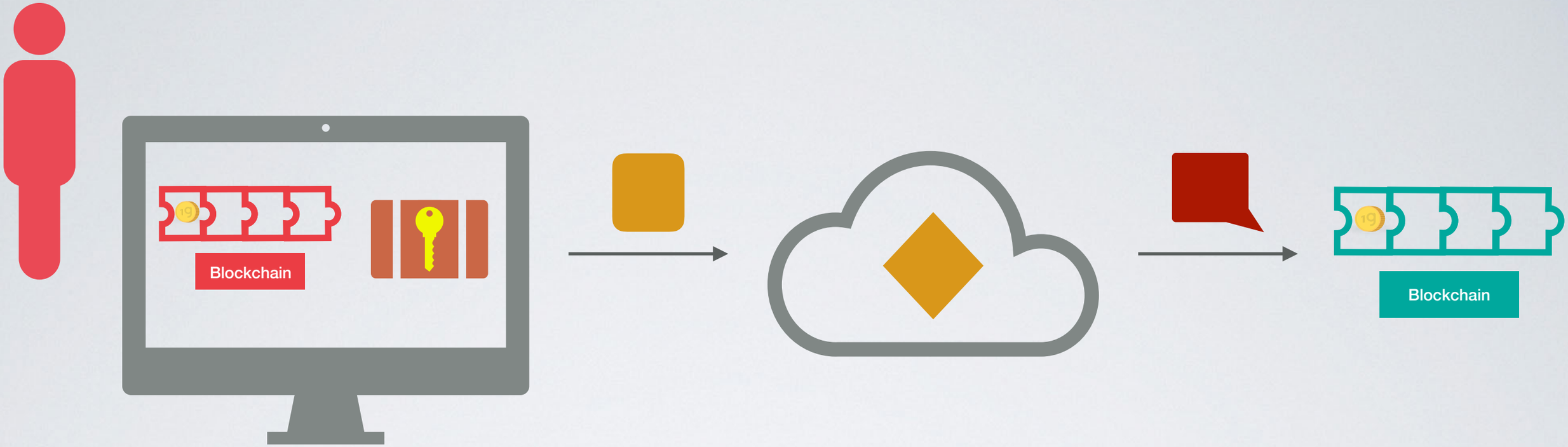


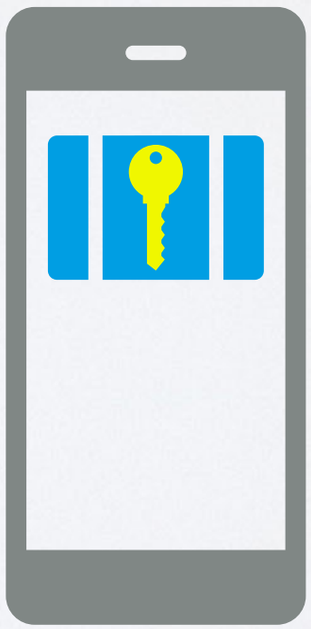
Politika Tabanlı İmzalama



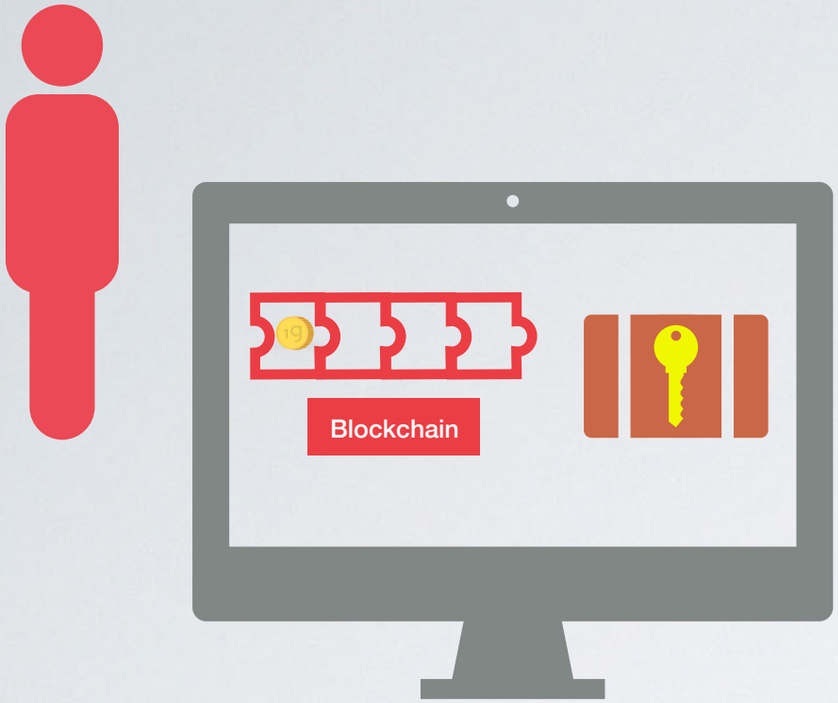


Politika Tabanlı İmzalama

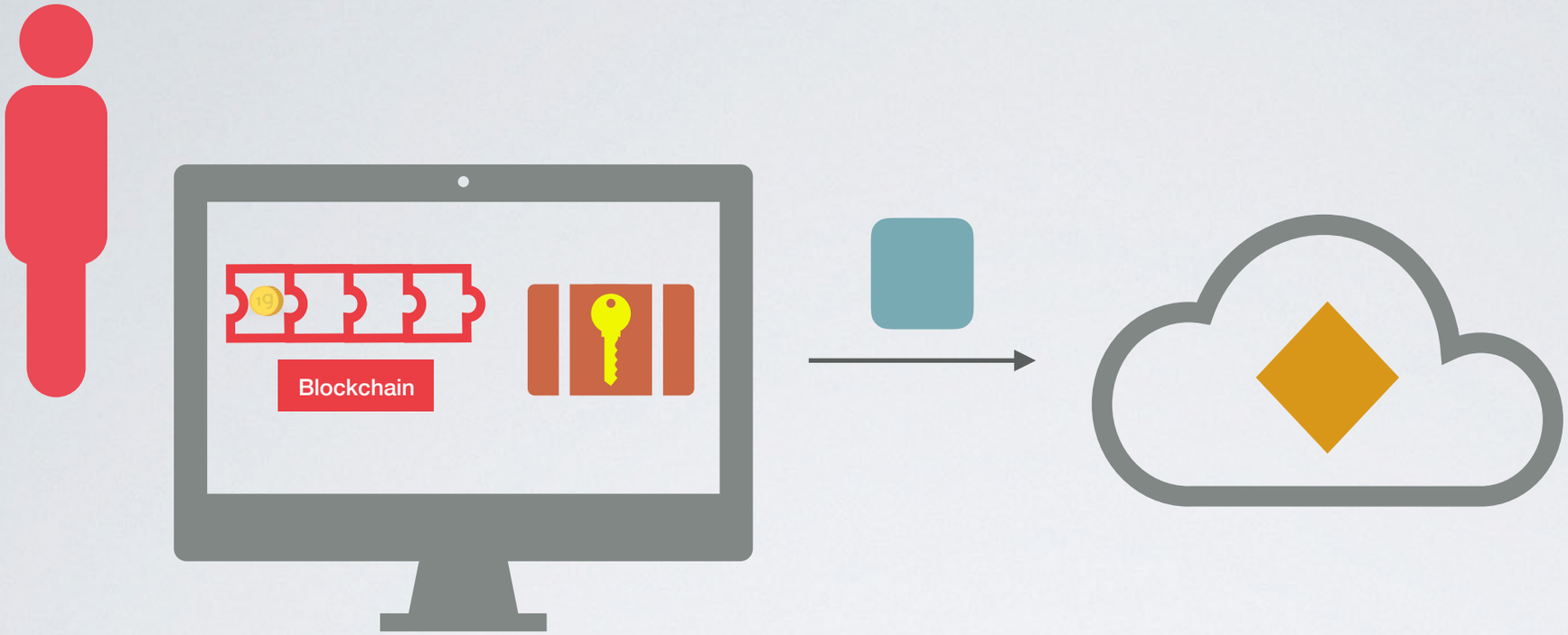


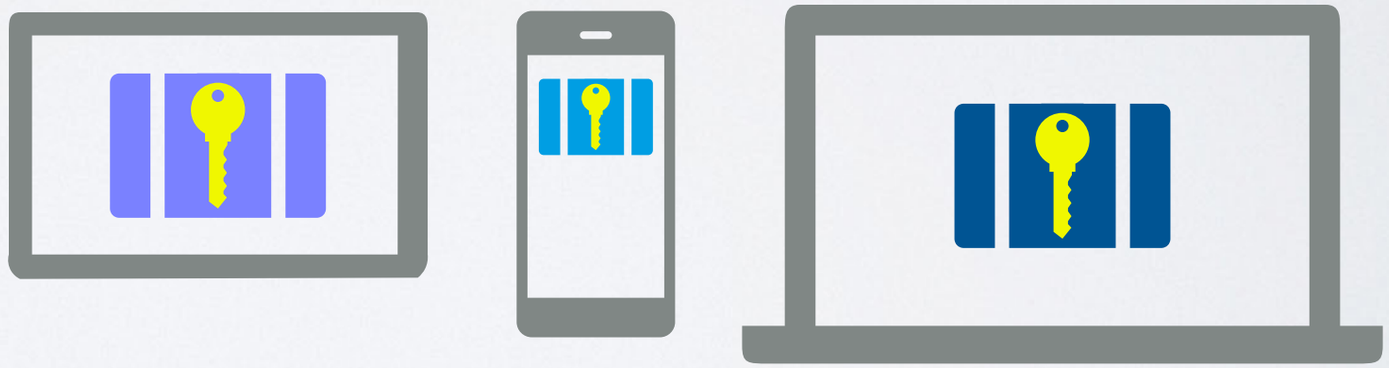


Politika Tabanlı İmzalama

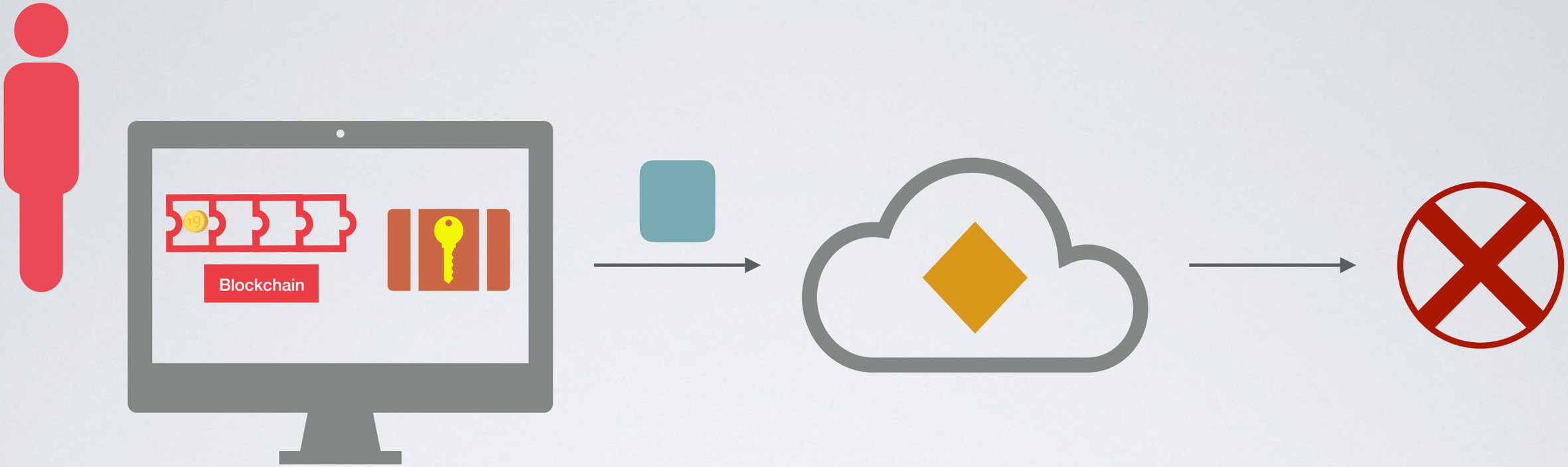


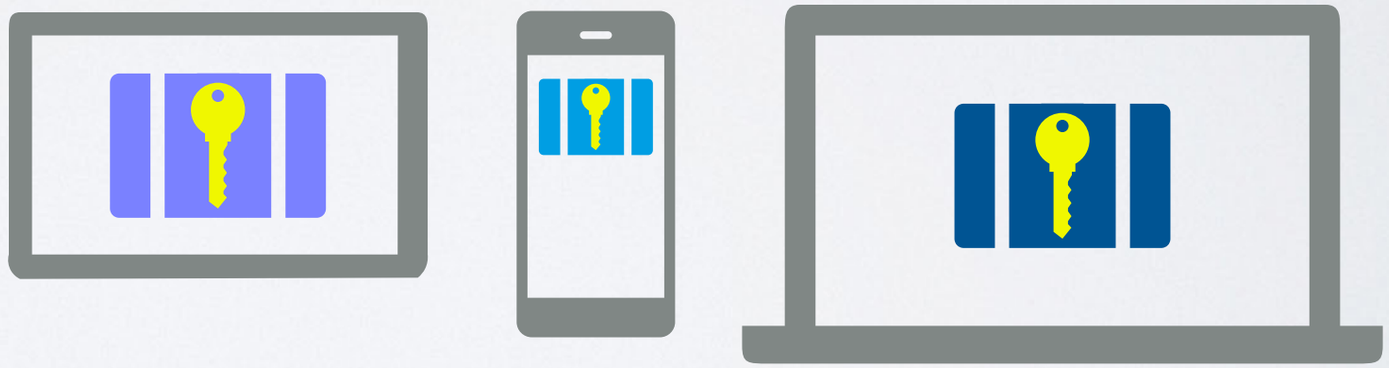
Politika Tabanlı İmzalama



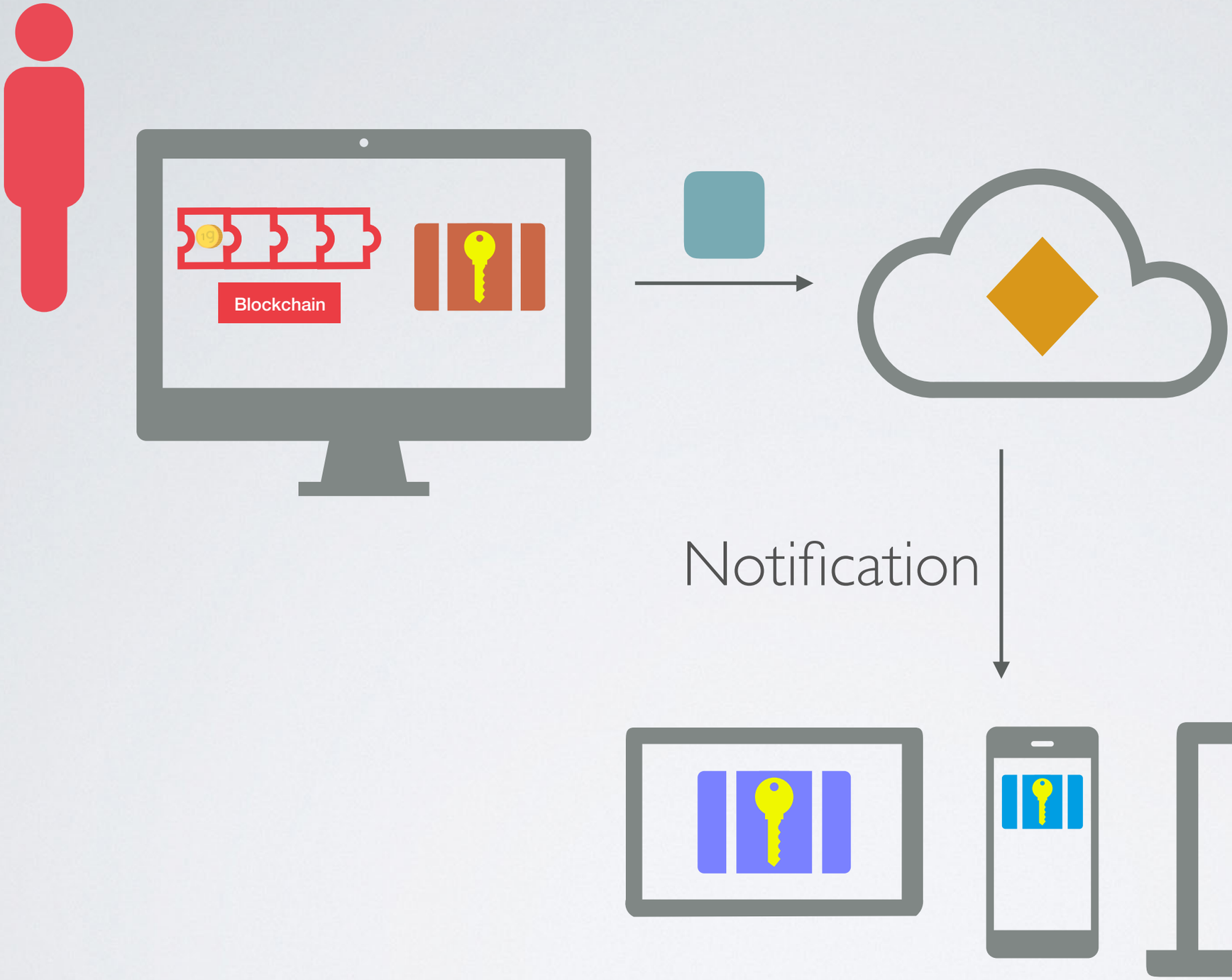


Politika Tabanlı İmzalama



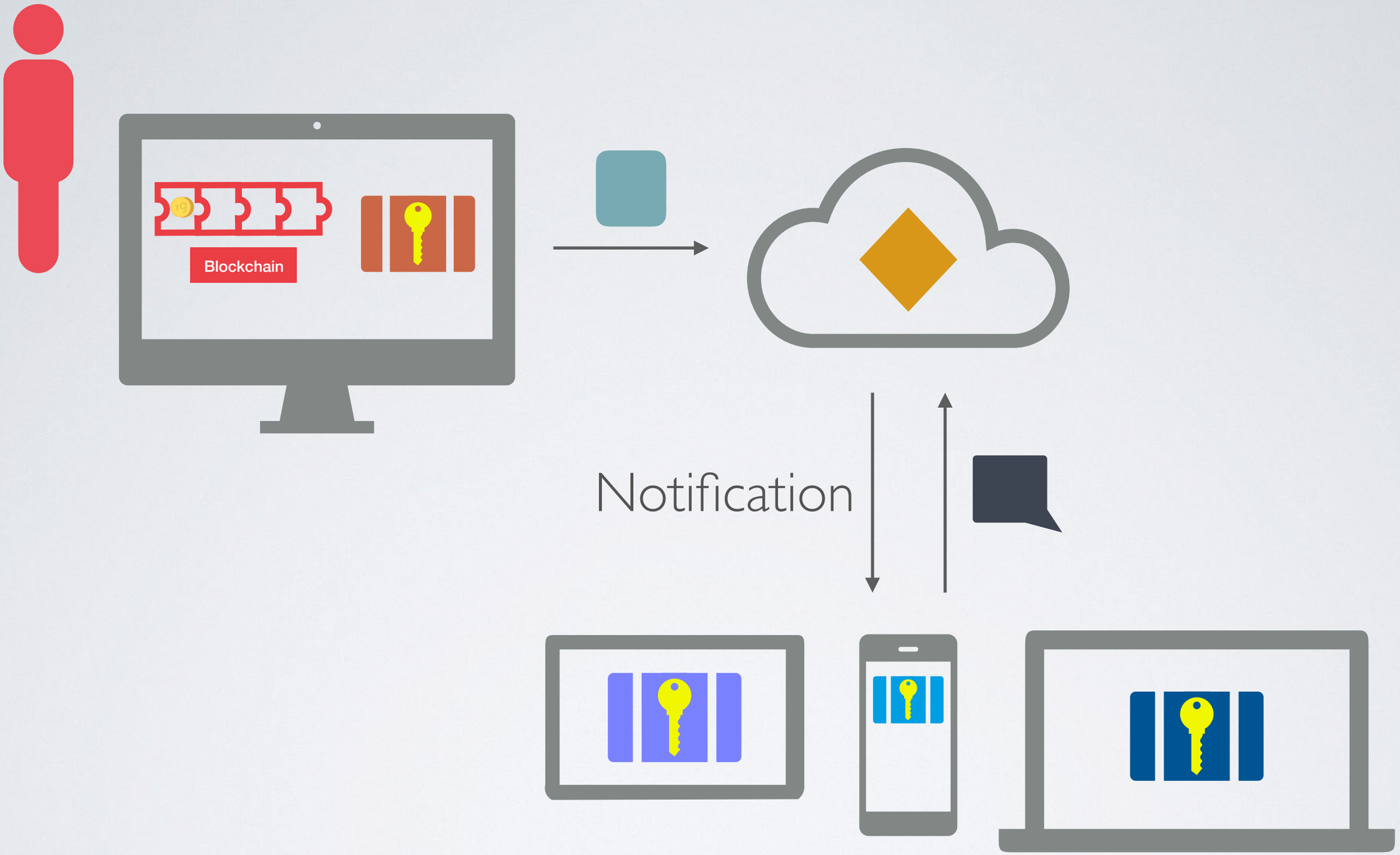


Politika Tabanlı İmzalama



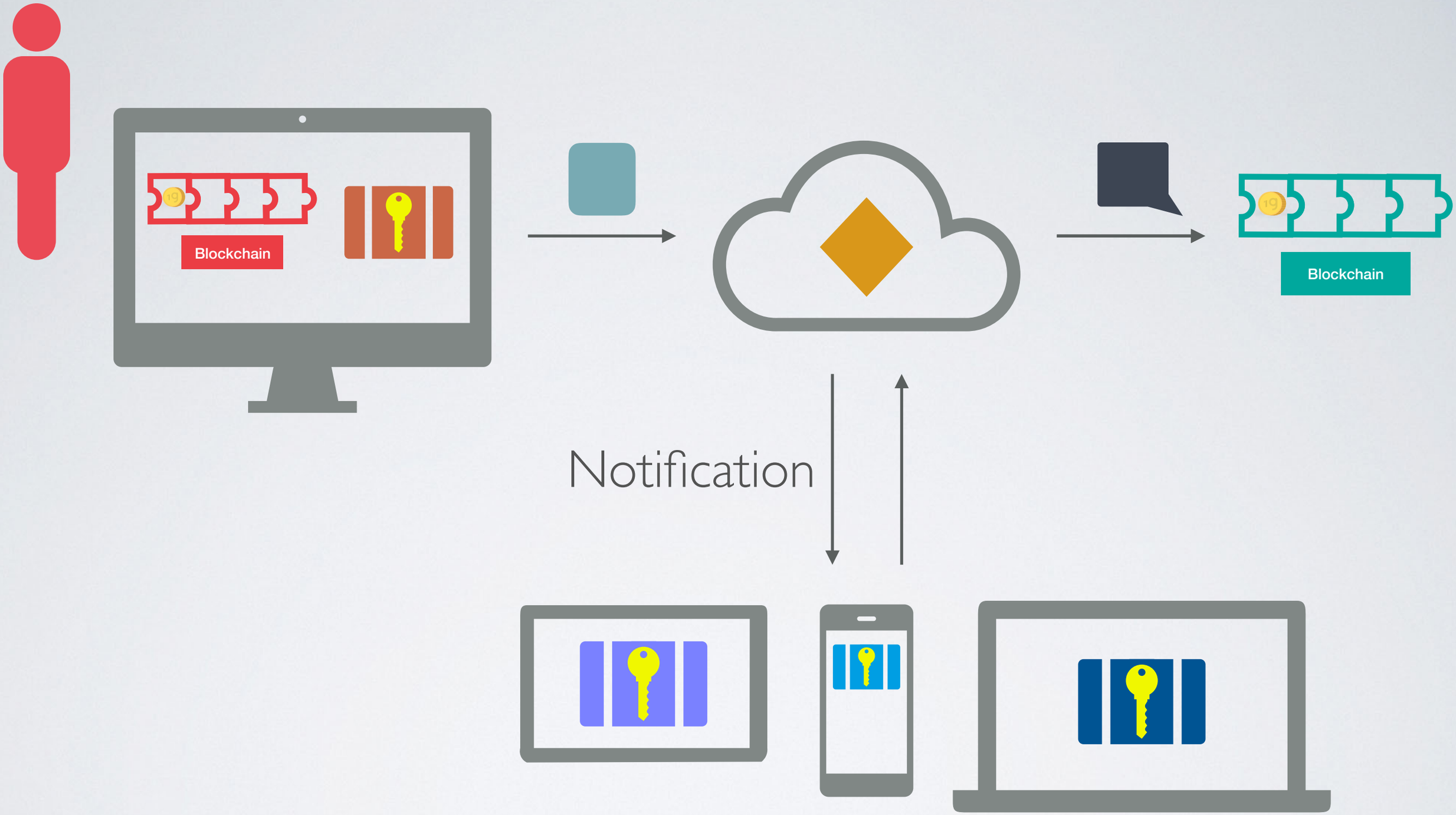
Eşik Kriptografisi

Politika Tabanlı İmzalama



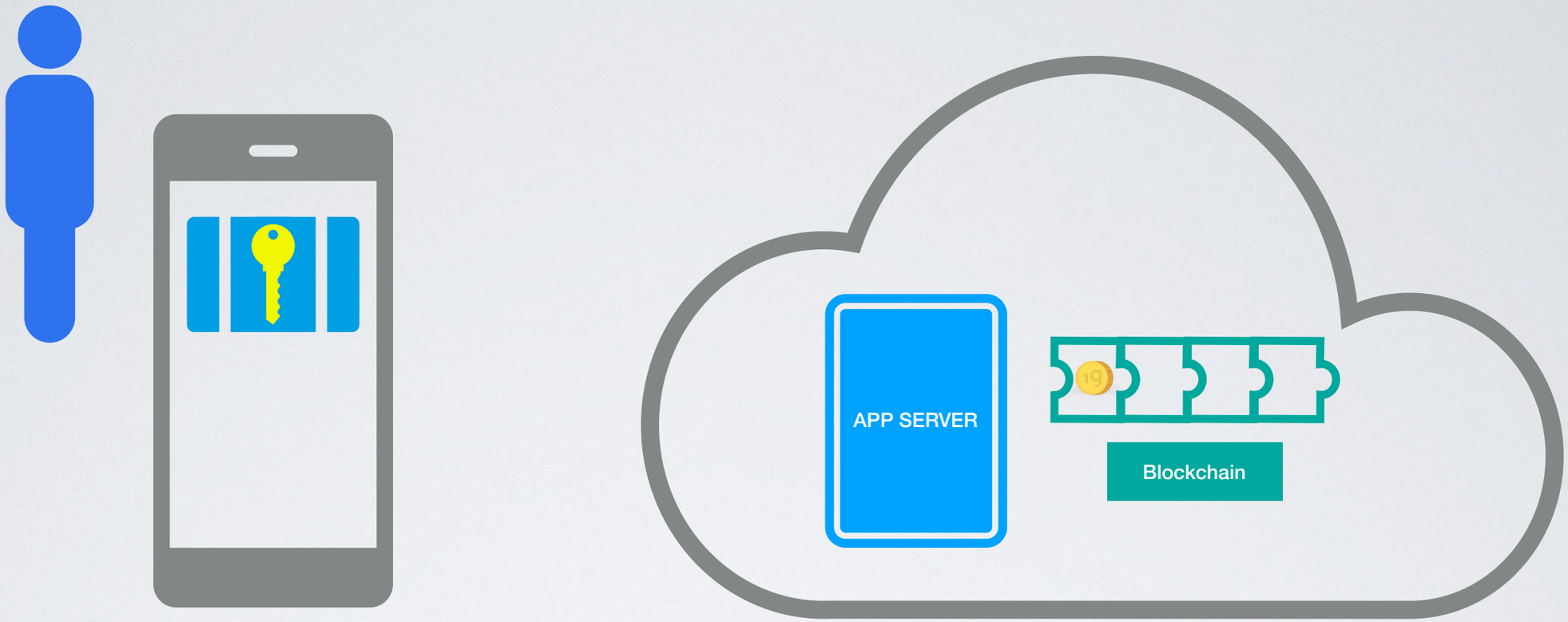
Eşik Kriptografisi

Politika Tabanlı İmzalama



Eşik Kriptografisi

Özet



Politika + İşlem/İstek = İmzalı İşlem