Blokzincir Tabanlı Sayısal Kimlikler Üzerinden Kimlik Doğrulama, Kayıt Tasdik ve Bilgi Paylaşım Sistemi

www.huawei.com

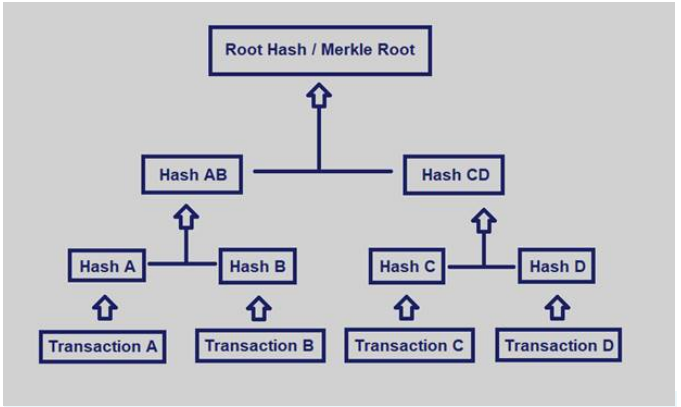
Author/ Email: Mehmet Aydar
Salih Cemil Çetin
Serkan Ayvaz

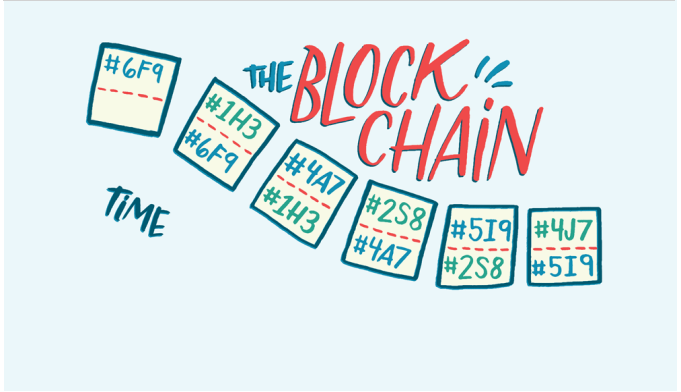
Version: V1.0(20190921)

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Blokzincir nedir?





- **Blokzincir** dağıtık, değiştirilemeyen ve üzerinde sadece ekleme yapılabilen bir veritabanıdır (dağıtık defter.)

- İki farklı kayıt: **hareketler** (transaction) ve **bloklar** (blocks).
- Blokzincir saydamlık ve güven getirir
  - Her katılımcının bir sayısal kimliği vardır
  - Kayıtları merkezileştirmek yerine dağıtık tutar
  - Süreçleri akıllı sözleşmelerle otomatikleştirir

Geleneksel kimlik sistemlerindeki zorluklar

- **Güvenlik**
- **Mahremiyet**
- **Kullanılabilirlik**
- **Globalleşme**
- **Regulasyonlara uyum sağlamak:**
  - Avrupa birliği veri koruma regulasyonu (GDPR)
  - Kişisel verilerin korunma kanunu (KVKK)
- **Verimli ve otomotize edilmiş iş akışı:**
  - Kimlik ve belgelerin dijitalleşme gereksinimi
  - Müşterini tanı (KYC) gereksinimi

Hedef kimlik modeli:

Veri koruma regulasyonları ile uyumlu,

kimlik sahiplerinin kendi bilgilerine **bütünüyle sahip olduğu**,

kimlik sahipleri hakkındaki bilgilerin **standart** bir şekilde tanımlanabildiği,

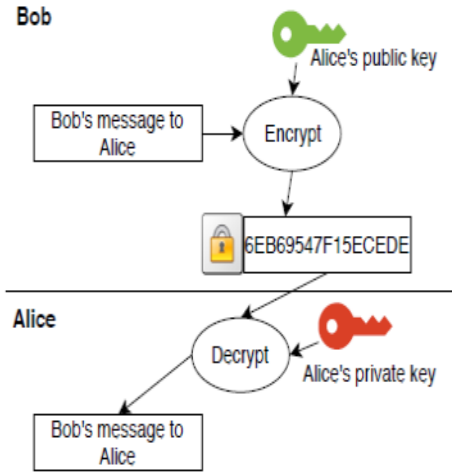
güvenli veri alışverişinin yapılabildiği ve standard bir şekilde **doğrulanabildiği,**

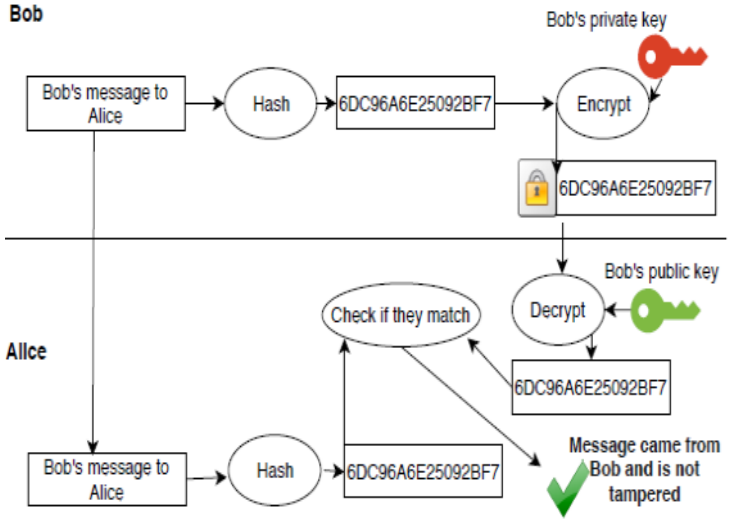
ve daha **otomatize** edilmiş bir iş akışına olanak sağlayan güvenli bir **dijital kimlik modeli** geliştirilmelidir.

Kimlik sistemlerinde Blokzincir kullanımı

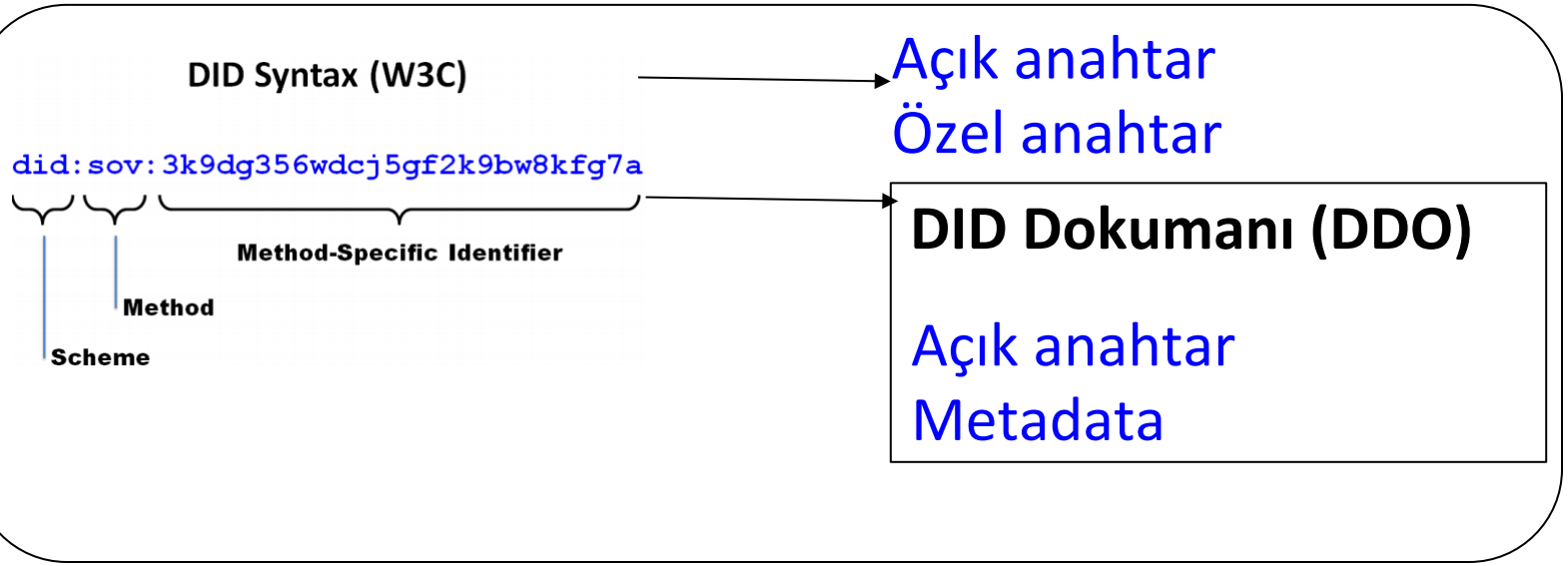
- **Blokzincirinde kullanılan** asimetrik anahtar teknolojisi ve özetleme (hashing);
  - Dijital kimlik sahipliği için genişletilebilir.
  - Kimliğe dayalı kayıtların bütünlüğü ve kökeninin anlaşılmasında kullanılabilir.
  - Dijital noterlik işlemlerinde kullanılabilir.
  - İzine dayalı veri paylaşımını tetikleyebilir.
- **Blokzincirinde kayıtlar değiştirilemez, ve Blokzincirinde tutulan veriler saydamdır.**
- **Tek arıza noktasına (single point of failure) dayanıklıdır.**
- **Ademi merkeziyetçiliği artırır.**
- **Veri paylaşımına teşvik mekanizması getirir.**

Blokzincir + kimlik yönetimi





- Açık ve özel anahtar ikilisi
- **Kimliğin ispatı = Özel anahtarın kontrolünün ispatı**

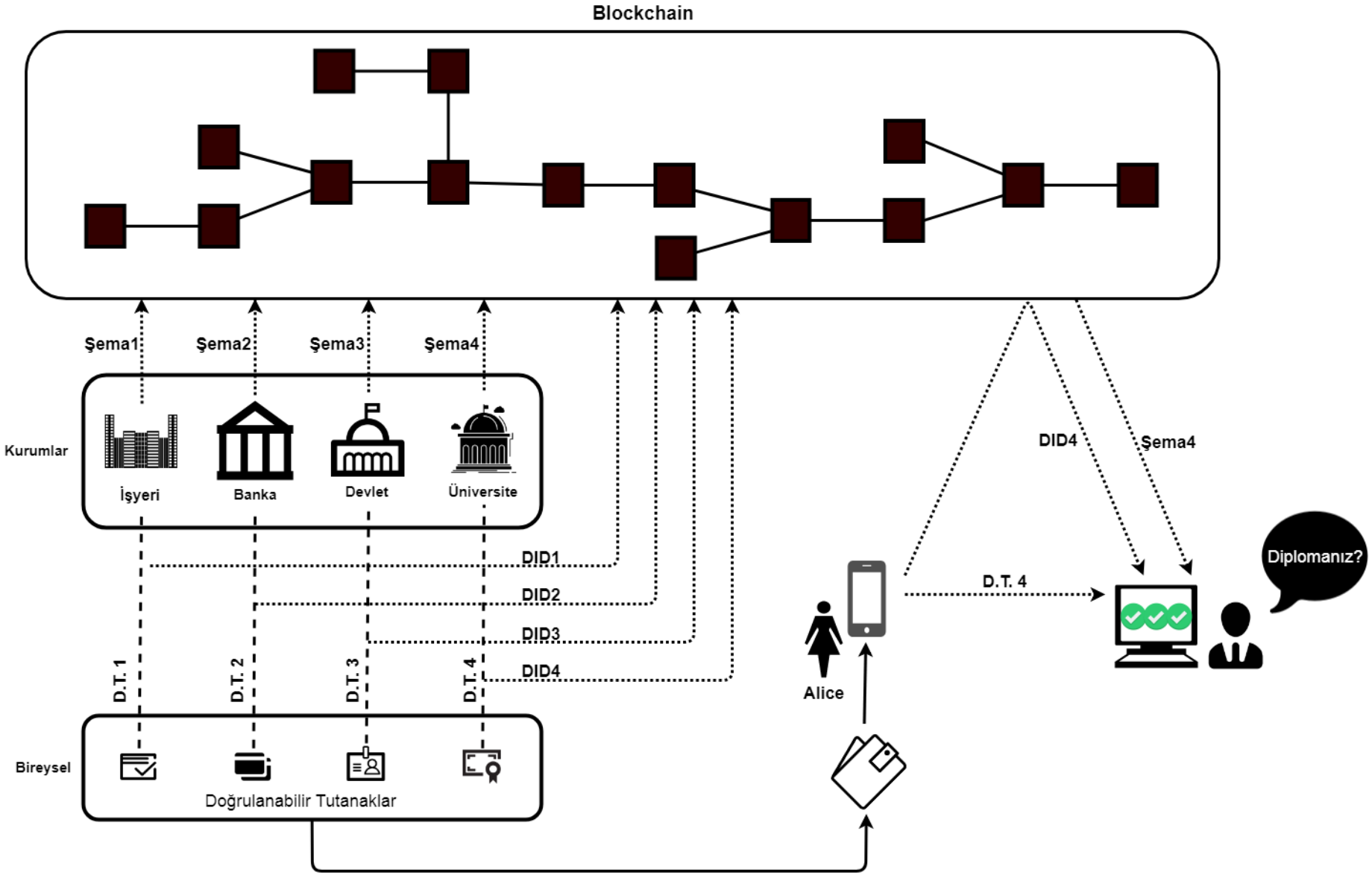


- DID: dağıtık tanıtıcılar
- **Global olarak tek**
- **Merkezi olmayan**
- Standart
- Her DID asimetrik anahtar ikilisi içerir

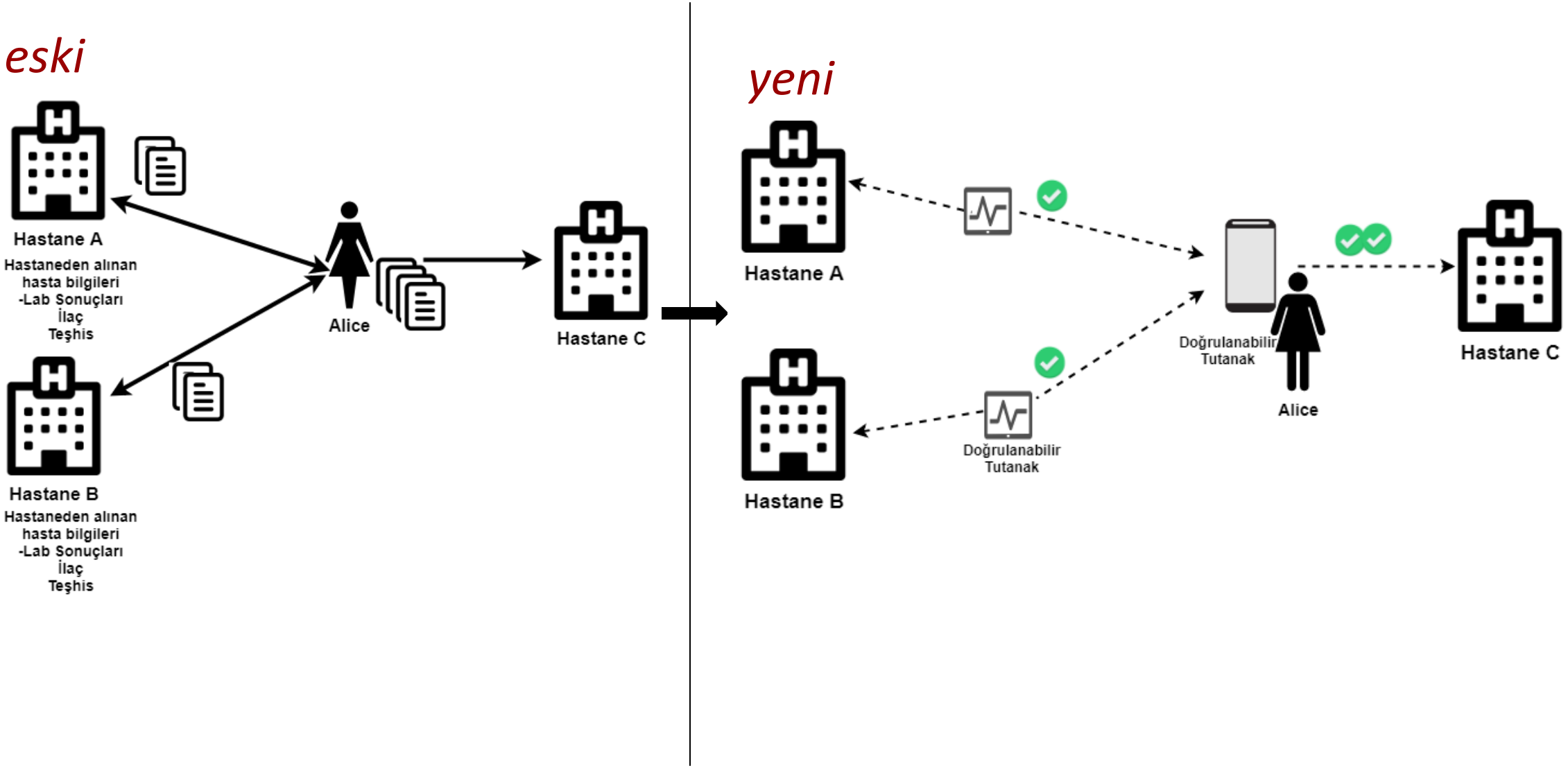
Blokzincir temelli kimlik sistemleri

Teknik Özellikler	Hedef Çözüm	Sovrin	Uport	SecureKey	ShoCard
Blokzincir teknolojisi	Hyperledger Indy	Hyperleder Indy	Ethereum	Hyperledger Fabric	Multiple layers
Blokzincir ağ yönetimi	Public / permission-ed	Public / permissioned	Public	Private	Public or Private
Kişiler için Öz-egemen kimlik	+	+	+	-	+
Öznitelik temelli veri paylaşımı	+	+	+	+	+
Dağıtık tanıtıcılar	+	+	+	-	-
İlişkiler için ayrı ikili dağıtık tanıtıcılar	+	+	-	-	-
Doğrulanabilir referanslar	+	+	+	-	-
Özel anahtarların şifrelenmesi	+	-	-	-	-
Var olan mevcut güvenilir ilişkilerin kullanılması	+	-	-	+	-
Hassas verilerin Blokzincirinde tutulmaması	+	+	+	+	-

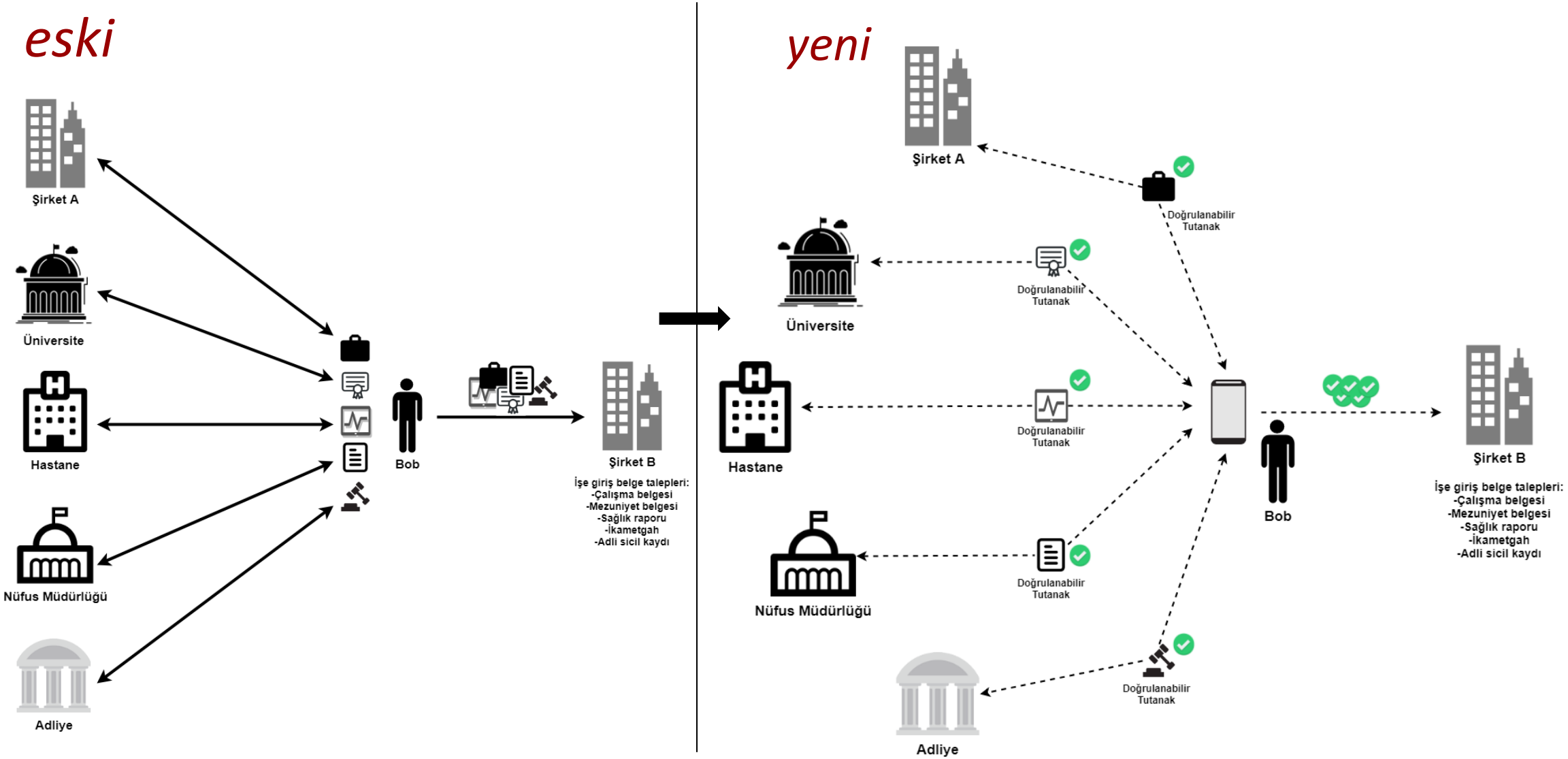
Genel mimarisi



Kullanım senaryosu 1 – hasta bilgileri

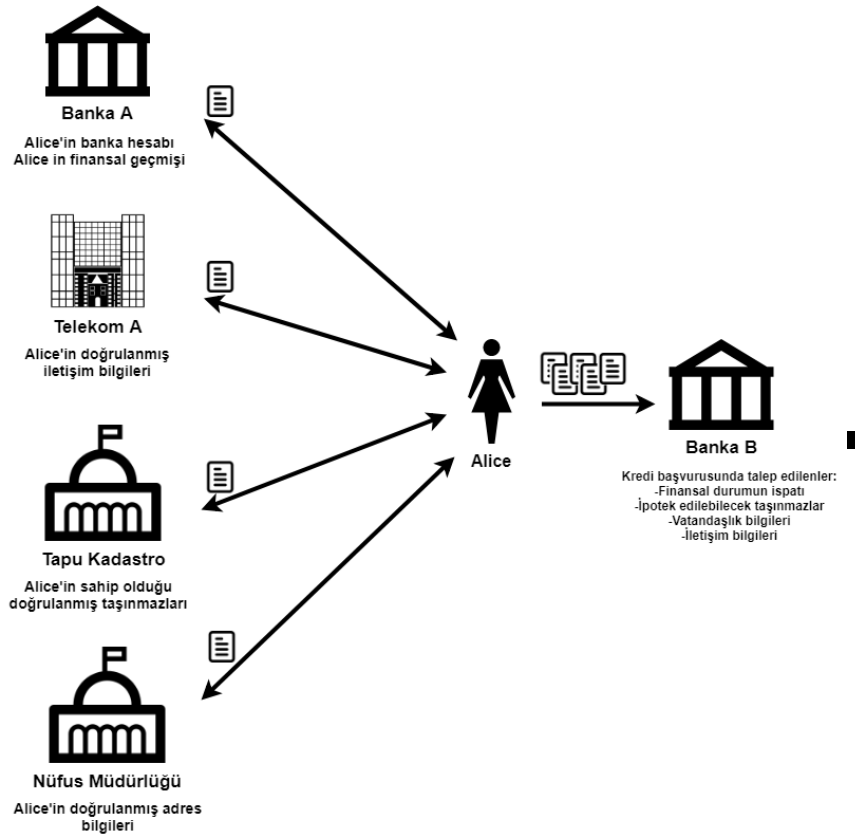


Kullanım senaryosu 2 – yeni işe giriş

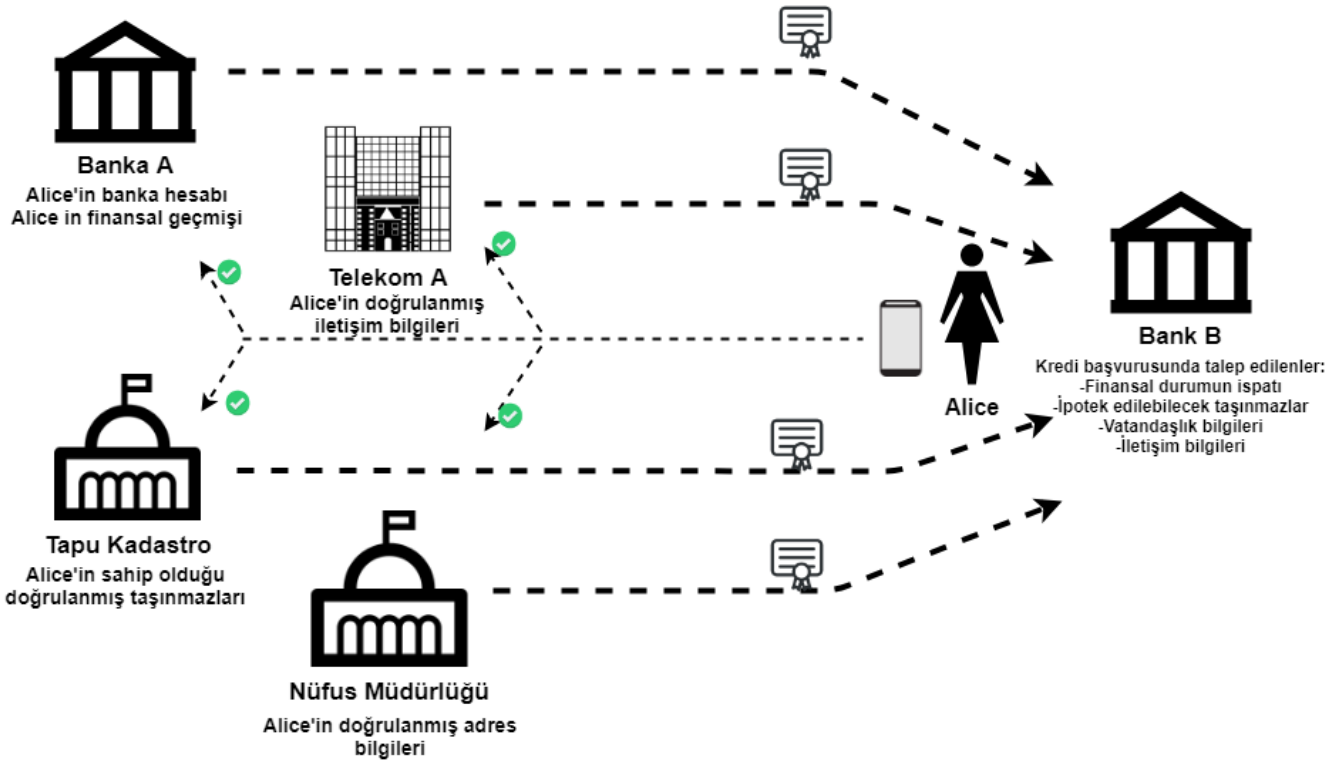


Kullanım senaryosu 3 – kredi başvurusu

eski



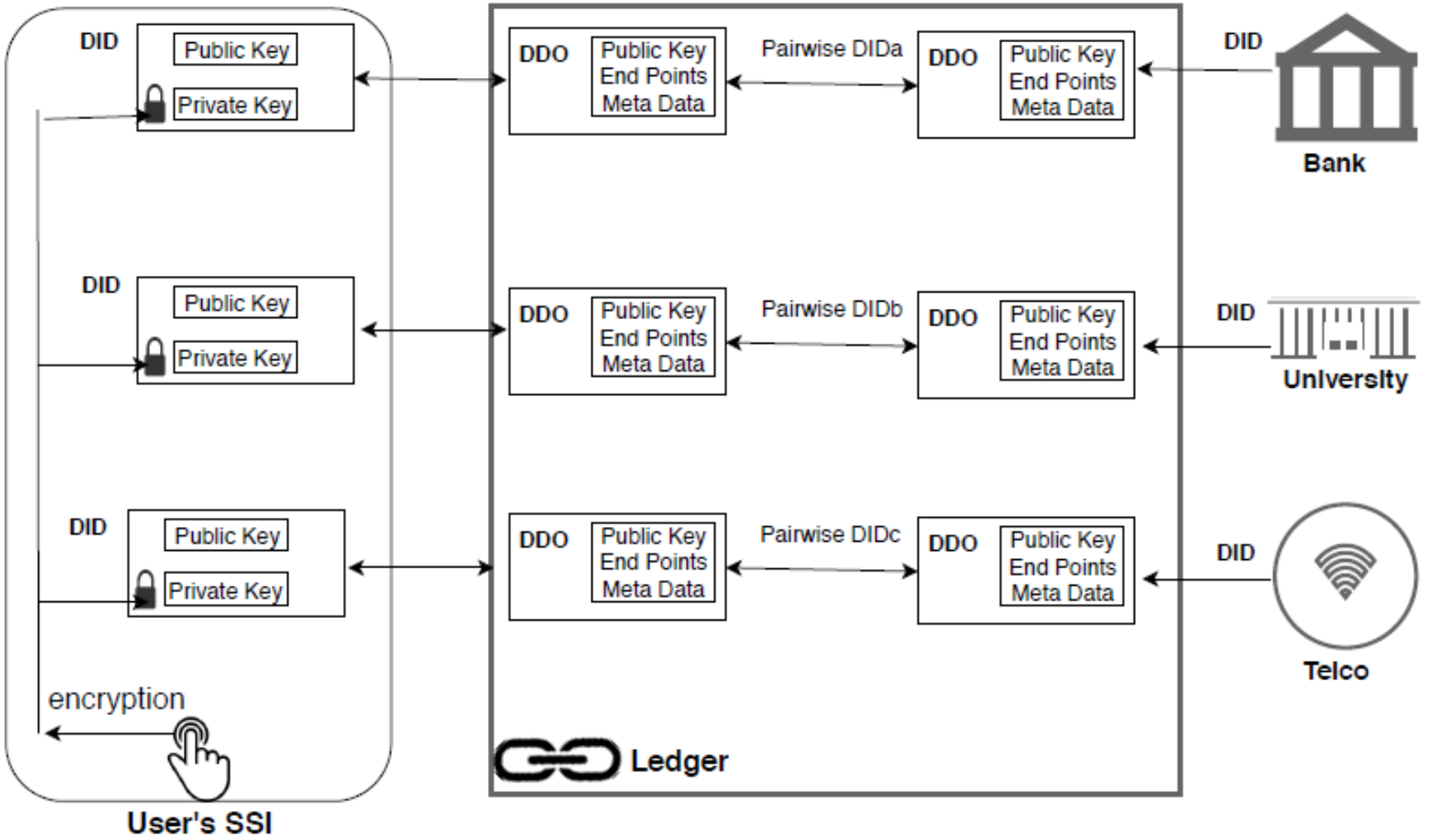
yeni



Gereksinimler

- Kurumlar arası Konsorsiyum
- Akıllı telefon entegrasyonu
- Özel anahtarların şifrelenmesi / kurtarılması
- Hükümetlerin sağladığı kimlik kartları entegrasyonu
- Yasal mevzuatlara uyum sağlanması

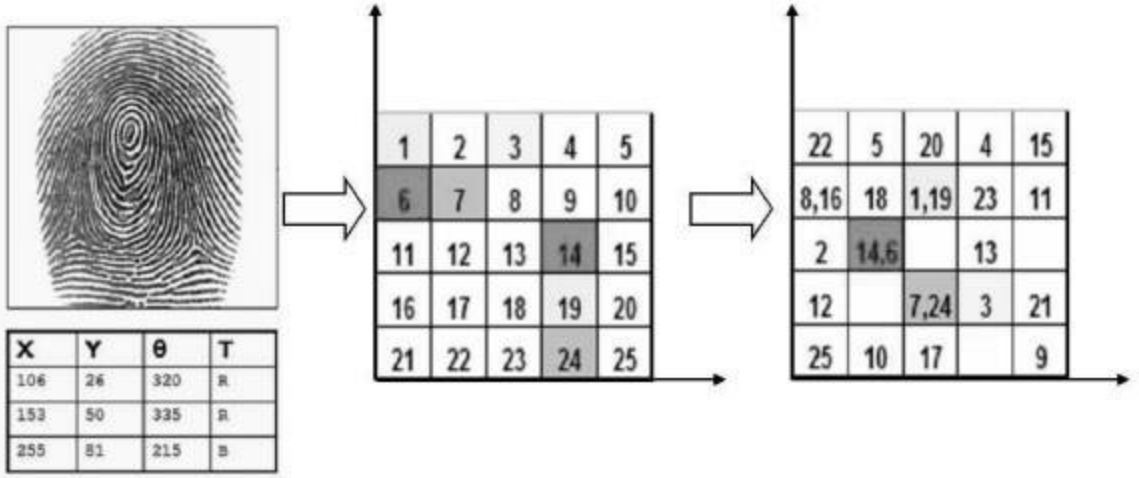
İkili dağıtık tanıtıcılar (DIDs)

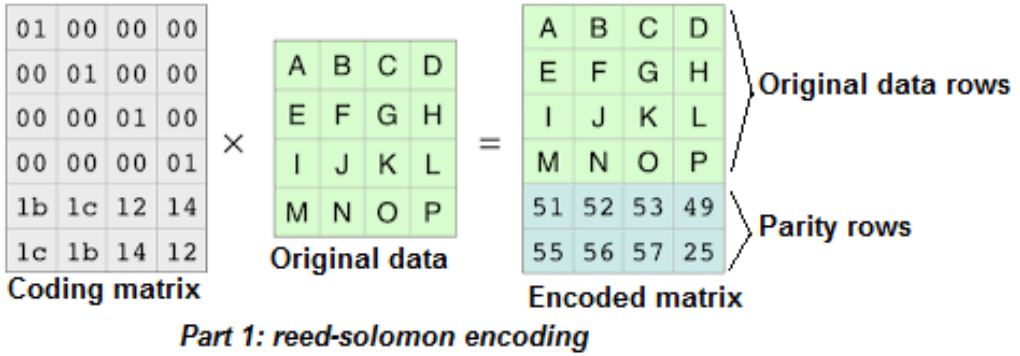


. Akilli **telefonlarin kimlik cuzdani** olarak kullanilmasi

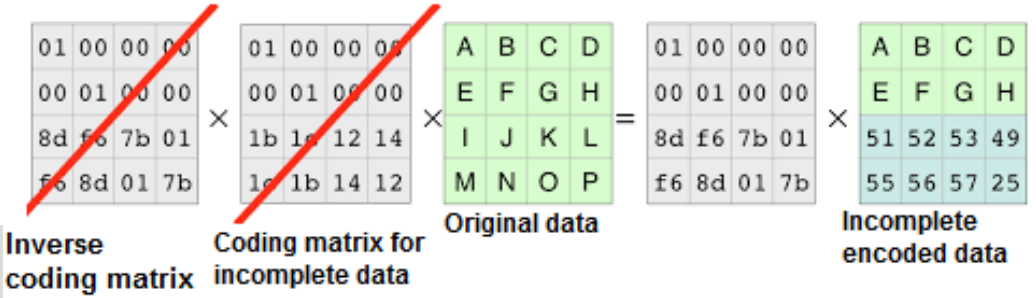
. **Özel anahtarların şifreli** tutulması

Özel anahtarların şifrelenmesi





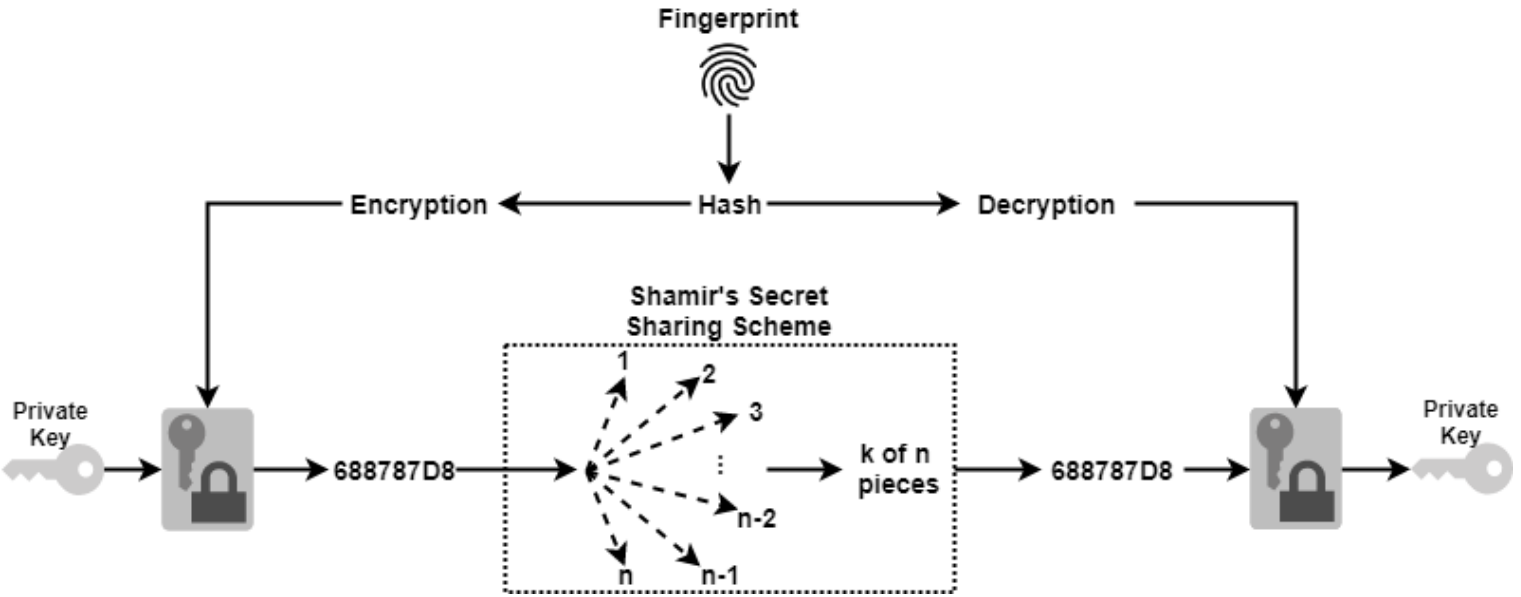
Part 1: reed-solomon encoding



Part 2: reed-solomon decoding

- ***Parmak izi kayit***
  - *On isleme*
  - *Minutiae çıkarımı*
  - *Kartezyen donusturme*
  - *Reed-Solomon kodlama*
  - *Simetrik anahtar olusturma*
- ***Parmak izi eşleme***
  - *Kayıt ve on işleme adımları*
  - *Minutiae eşleme*
  - *Kartezyen geri dönüşüm*
  - *Reed-solomon hata duzeltme*
  - *Simetrik anahtar eşleme*

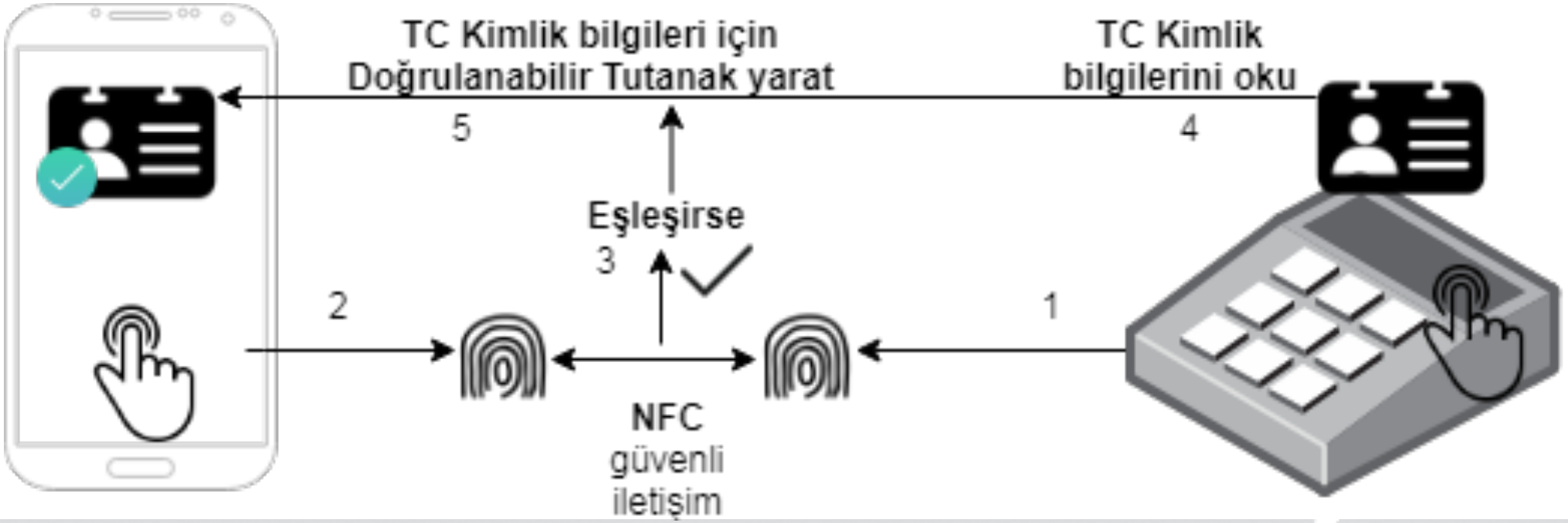
Kaybedilen Anahtarların kurtarılması



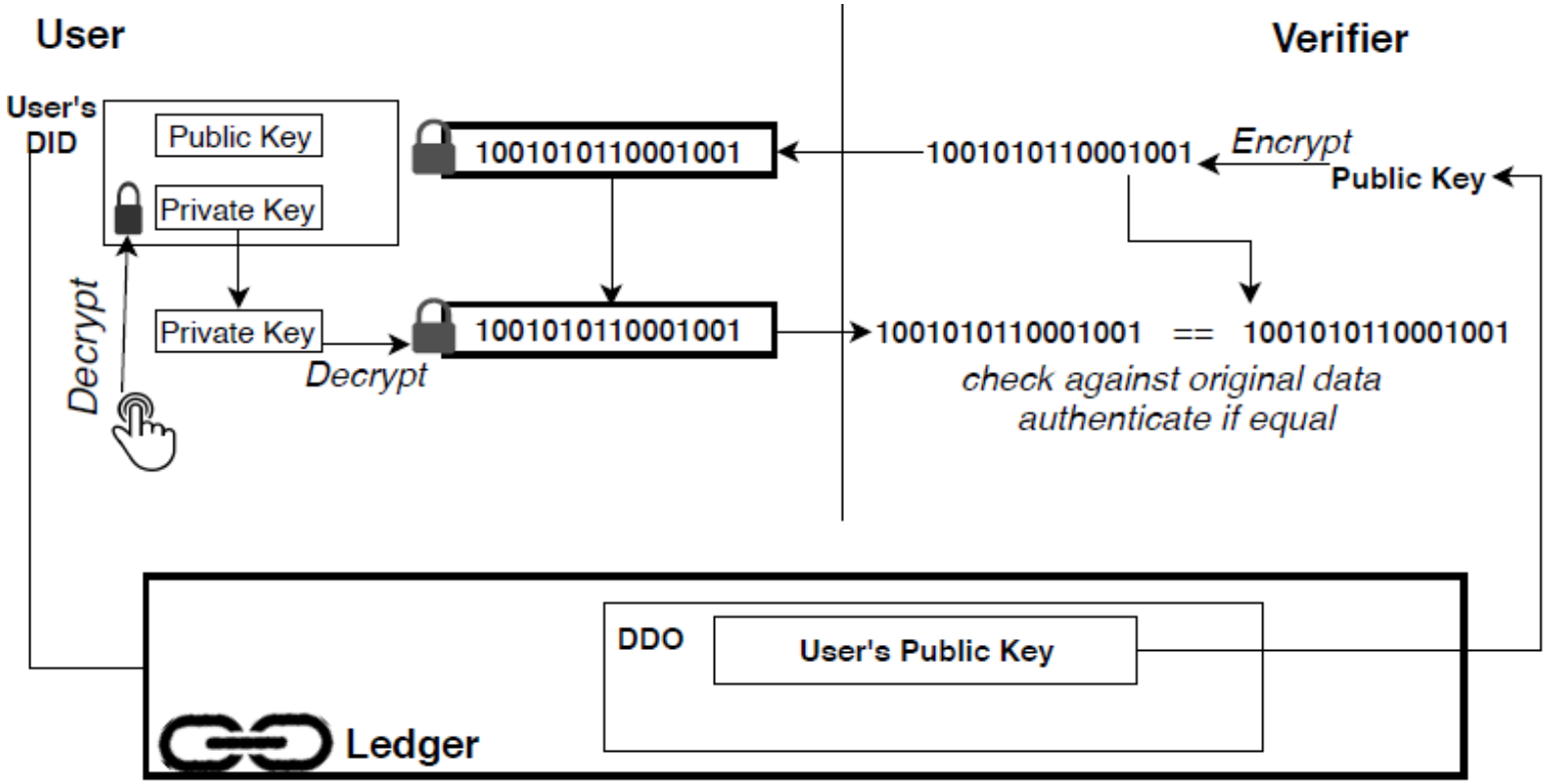
- **secret sharing schema** kullanılabilir
- *Biyometrik("secret")->(k,n)*
- *Biyometrik("secret")* kriptografik olarak parcalanarak ***n*** birime dagitilir.
- Bunlardan ***k*** birim bir araya gelince *Biyometrik("secret")'*i oluştururlar.
- Kimlik sahibi biyometrik özelliğini kullanarak *Biyometrik("secret")'*i açar.

Türkiye Cumhuriyeti Çipli Kimlik Kartı Entegrasyonu

- Kimlik sahipleri dijital cüzdanlarında bulunan “doğrulanabilir referanslar” ile kendini tanıtacaktır.
- Peki sistemin başlangıcında güven mekanizması nasıl sağlanmalıdır?
  - İdeal olan: devletin de bir idari kuruluş olarak sisteme katılması ve vatandaşların kimlik bilgilerini “doğrulanabilir referans” formatında vatandaşa sunması.
  - Gerçekçi yaklaşım: Çipli kimlik kartlarıyla entegrasyon.

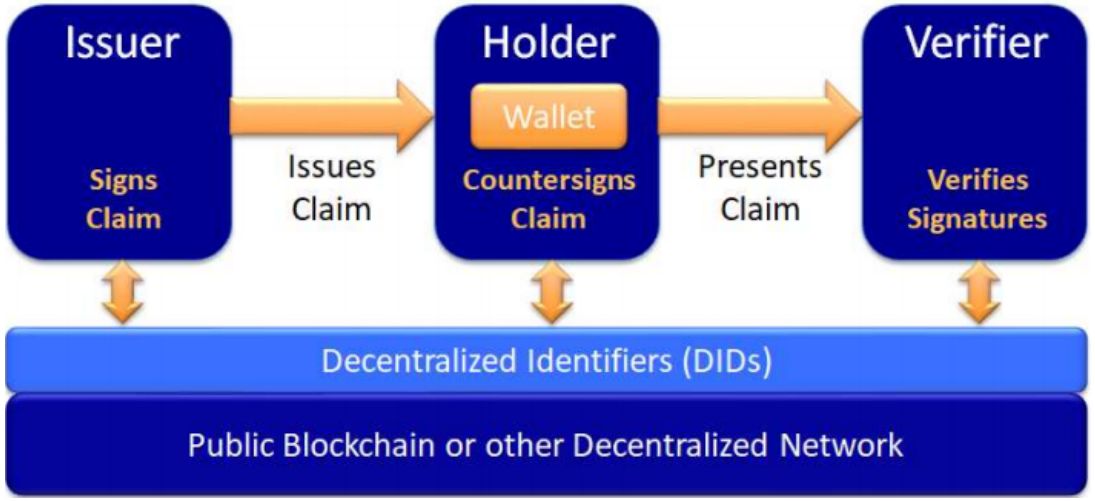


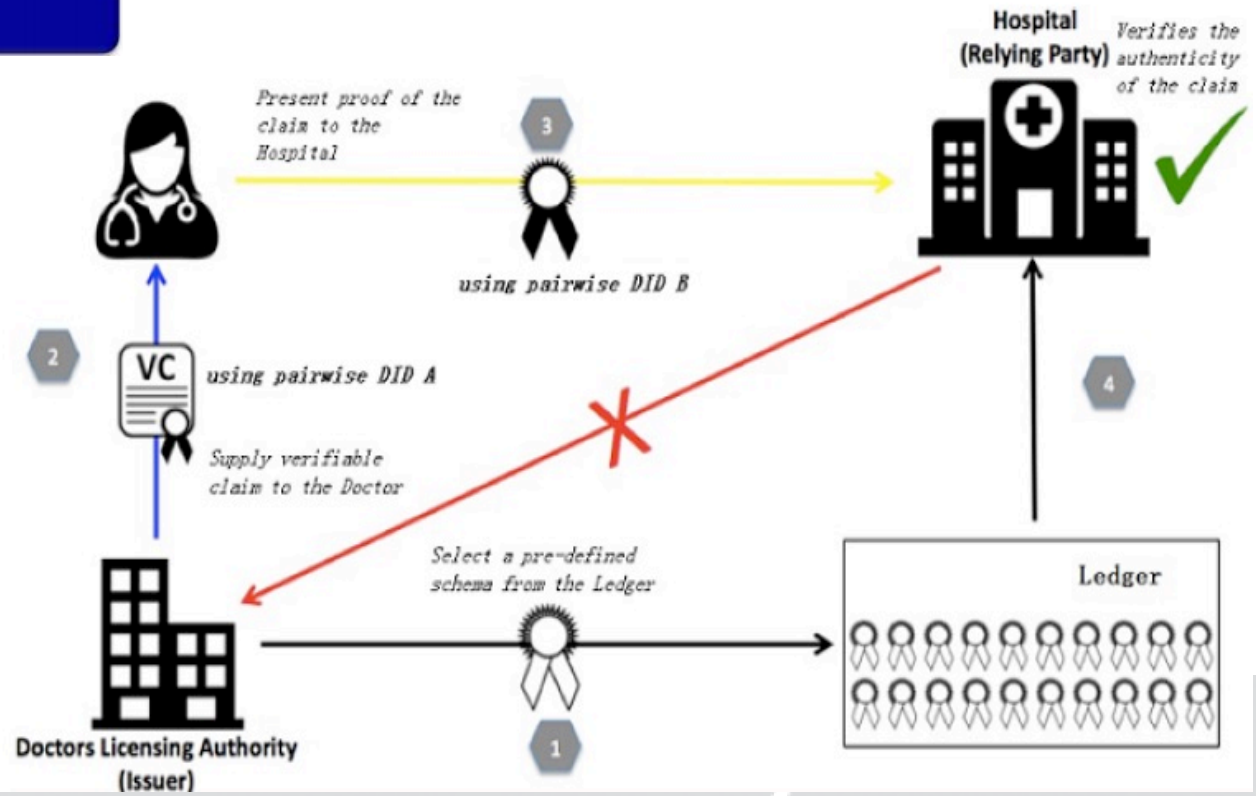
Uzaktan sistemlerde oturum açma



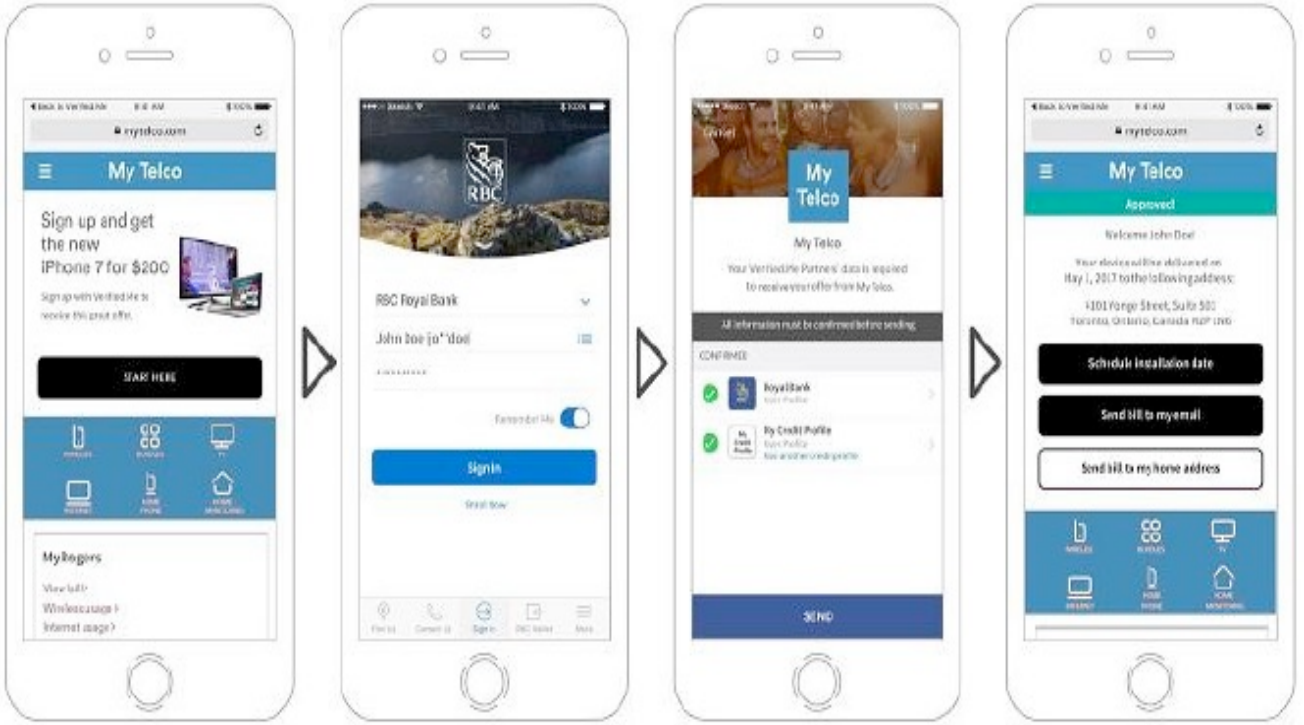
- Mahremiyet: DIDs ve anahtarlar – kimlik ispati – kimlik sahibi tarafından kontrol.
  - Google yada Facebook gibi merkeziyetçi değil.
  - Nirvana: DID e dayalı bir bağlantı sayesinde kullanıcı adı /şifre olmadan oturum açma mekanizması.

Doğrulanabilir referanslar





İzine dayalı veri paylaşımı



Telekom (Bilgi talep eden)	Kullanıcı (Kimlik sahibi)	Banka (Bilgi sağlayıcı)
		1. Banka kullanıcının kimliğini doğrular
8. Doğrulanabilir talep telekom şirketine ulaşır.	**2.** Kullanıcı hangi bilgiyi paylaşacağını seçer	
		3. Banka bir şema tanımı seçer
9. Telekom şirketi, dijital imzalar vasıtasıyla bu belgenin kullanıcıdan geldiğini ve bankadan onaylı olduğunu doğrular.	**6.** Doğrulanabilir talep bankadan kullanıcıya ulaşır. Kullanıcı kendi gizli anahtarıyla bu talebi imzalar. Artık hem kullanıcı hem bankanın imzası doğrulanabilir talebin üzerindedir.	**4.** Banka, kullanıcının paylaşmak istediği bilgiye göre bir talep oluşturur.
10. Kullanıcının bilgilerini doğruladıktan sonra, telekom şirketi yeni hizmetini kullanıcıya açar.	**7.** Kullanıcı orijinal doğrulanabilir talep belgesini ve imzalı versiyonunu telekomünikasyon şirketine yollar.	**5.** Banka, kendi gizli anahtarıyla talebi imzalar ve kullanıcıya gönderir.

Neden Blokzincir?

- İzole çalışan kişi ve kurumları bir araya getirebilmek

Blokzincir nasıl kullanılır?

- Kimliklerin (DID) sağlanması, aranması, doğrulanması
- Doğrulanabilir referansların doğrulanması ve iptal mekanizması
- Veri paylaşım loglarının tutulması
- Ödüllendirme mekanizması (crypto-currency)

Hangi Blokzincir teknolojisi?

- Public-permissioned
- Hyperledger Indy

Belirsizlikler ve Zorluklar

- Olgunluk aşamasında değiliz
- Olasi performans düşüklüğü
- Kurumlarin sisteme dahil edilme zorluklari
- Uzman personel azlığı
- Yasal mevzuatlar

Teşekkürler.

- **Soru cevap ?**