BLOCKSIGNAL: BLOKZİNCİR KULLANARAK KİMLİK DOĞRULAMA SEREMONİSİNİ ORTADAN KALDIRAN BİR GÜVENLİ MESAJLAŞMA UYGULAMASI

Enes ALTUNCU, Prof. Dr. Kemal BIÇAKCI
TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü

2. Ulusal Blokzincir Çalıştayı
25-26 Eylül 2019, İstanbul, TÜRKİYE

Güvenli Mesajlaşma Uygulamaları

- Uçtan uca şifreleme
  - Açık anahtar kriptografisi
  - Gönderici ve alıcı ortaklığıyla oluşturulan ortak şifreleme anahtarıyla şifreleme
- Whatsapp, Telegram, Signal

- Merkezi sunucu
  - Mesajların iletimi
  - Açık anahtar dağıtımı

Signal Protokolü

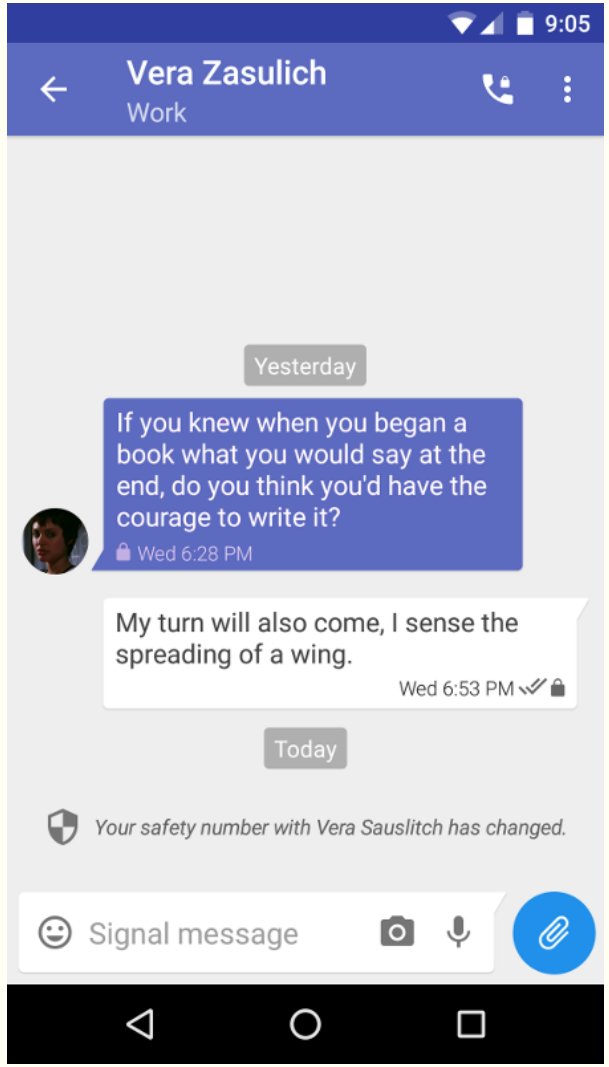
- Open Whisper Systems tarafından geliştirildi
- Açık kaynak kodlu
- Future secrecy ve forward secrecy
- Double Ratchet algoritması + X3DH anahtar anlaşma protokolü
- Uçtan uca şifreleme
  - Whatsapp da bu protokolü kullandığını açıkladı

Signal Android Messenger

- Signal protokolünü kullanır
- Açık kaynak kodlu

- Açık anahtar değişebilir
  - Uygulamanın tekrar yüklenmesi
  - Cihaz değişikliği
  - SIM kart değişikliği

- Açık anahtar değişimini tespit eder
  - Kullanıcıya bildirir
  - Kimlik doğrulama seremonisini başlatır



Kimlik Doğrulama Seremonisi

- Güvenlik seremonisi
  - Protokol haricinde yapılan tüm işlemler
  - Carl Ellison tarafından ortaya atıldı
  - Brainard güvenli mesajlaşma için özelleştirdi
    - Kimlik doğrulama seremonisi olarak isimlendirdi

- Taraflar açık anahtarı içeren bir dizi karakteri karşılaştırır
  - Signal'da emniyet numarası
    - Oturum başına üretilir
    - Kullanıcıların telefon numaralarını da içerir
  - Eşleşirse iletişim güvenli
  - Aksi halde, mesajlaşılan kişi farklı biri

Problem ve Çözüm

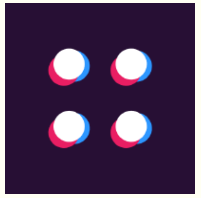
- Yapılan çalışmalarda pek çok kullanıcı
  - Bu işlemi önemsemiyor
  - Doğru bir şekilde tamamlayamıyor
  - Ne anlama geldiğini bilmiyor

- İşlemin tamamlanması zaman alıyor

- Çözüm: Otomatik açık anahtar doğrulaması
  - Kullanıcılar güvenlik çemberinin dışında olmalı
  - Daha hızlı bir çözüm
  - Nasıl?
    - Blokzincir tabanlı PKI sistemi
    - Blokzincirde tutulan açık anahtar gerektiğinde doğrulanır

Literatür Taraması

- Otomatize kimlik doğrulama seremonisi
  - Vaziripour ve ark. Otomatik doğrulama için sosyal medya hesaplarını kullandılar
  - Bir başka Trusted-Third-Party
  - Sosyal medya hesabı herhangi biri adına açılabilir
- Mevcut blokzincir tabanlı PKI çözümleri
  - Bitcoin tabanlı: MultiChain, Blockstack
  - Ethereum tabanlı: Ghazal, SCPKI
  - Diğer: Fredriksson'un Merkle proof tabanlı çözümü
- Blockstack haricindeki sistemlerde önemli sorunlar mevcut
  - Ölçeklenebilirlik
  - İşlem hızı
  - Uyumluluk
- Bu sebeple, Blockstack kullanıldı

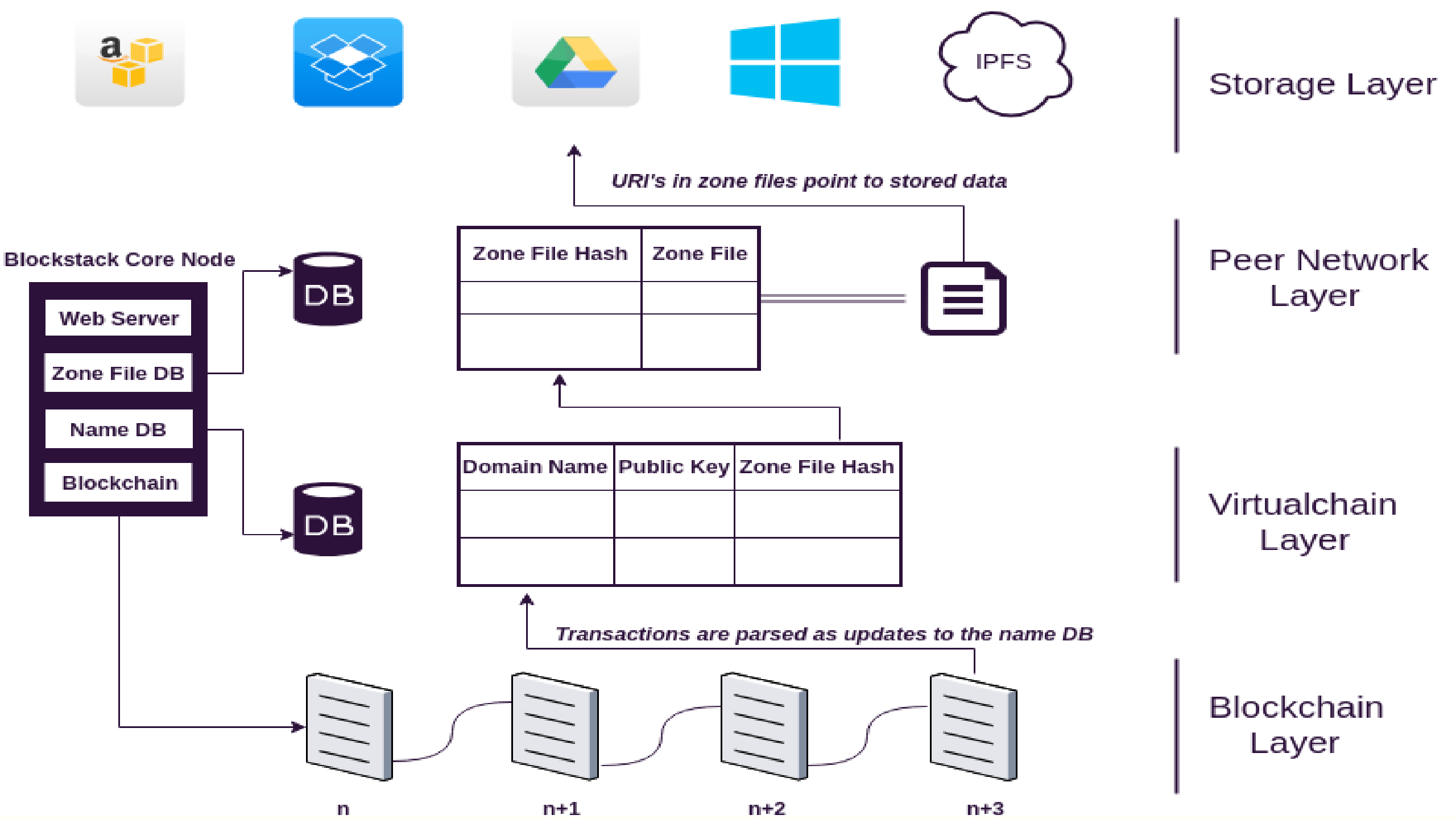


Blockstack

- Blokzincir tabanlı kimlik oluşturma, doğrulama ve depolama platformu
- Bitcoin tabanlı
- Ademi merkezi (Decentralized)
- Birleşik DNS ve PKI yapısı
- Açık kaynak kodlu, 7000'den fazla geliştirici
- Android, iOS, Ruby ve JavaScript kütüphaneleri

- Her kullanıcı ve uygulama için kullanıcı adı olarak bir alan adı («.id», «.app» vs.)
  - Her alan adı için varsayılan olarak açık anahtar

- Açık anahtarların özeti blokzincirde tutulur
  - Gerektiğinde doğrulanabilir


IPFS
Storage Layer
URI's in zone files point to stored data
Blockstack Core Node
Web Server
Zone File DB
Name DB
Blockchain
DB
DB
Zone File Hash
Zone File
Peer Network Layer
Domain Name
Public Key
Zone File Hash
Virtualchain Layer
Transactions are parsed as updates to the name DB
n
n+1
n+2
n+3
Blockchain Layer

Tehdit Modeli

- Kötücül/Ele geçirilmiş sunucu:
  - Insider veya ortadaki adam saldırısı (MITM)
  - İlk kurulum esnasında, sunucu saldırganın anahtarını dağıtabilir
    - Signal'da kimlik doğrulanabilir, kullanıcı uyarılmaz
  - Mesajlaşma esnasında, MITM olabilir
    - Signal kullanıcıyı uyarır, kimlik doğrulama seremonisi tamamlanmalıdır

- SSL sabitlemeyi atlatma:
  - Signal, sunucunun SSL sertifikasını uygulamaya gömer
  - MITM saldırıları engellenir
  - Tersine mühendislik gibi yöntemlerle atlatılabilir

Tehdit Modeli

- SIM kart klonlama:
  - Kayıtlı kullanıcının SIM kartı klonlanır ve yeni bir oturum başlatılır
  - Günümüzde zor olsa da mümkündür

- Bilinmeyen anahtar paylaşımı saldırıları (Unknown key-share attacks):
  - Ortak anahtarın bir tarafı, diğer tarafla başka birinin anahtar oluşturmasını sağlar
  - İstenmeyen bir kullanıcıyla oturum kurulur
  - Signal, emniyet numarasıyla bu saldırıları önler
    - Ancak, eski bir Signal sürümü yüklü ve parmakizini paylaşmış kullanıcı için hala tehdit

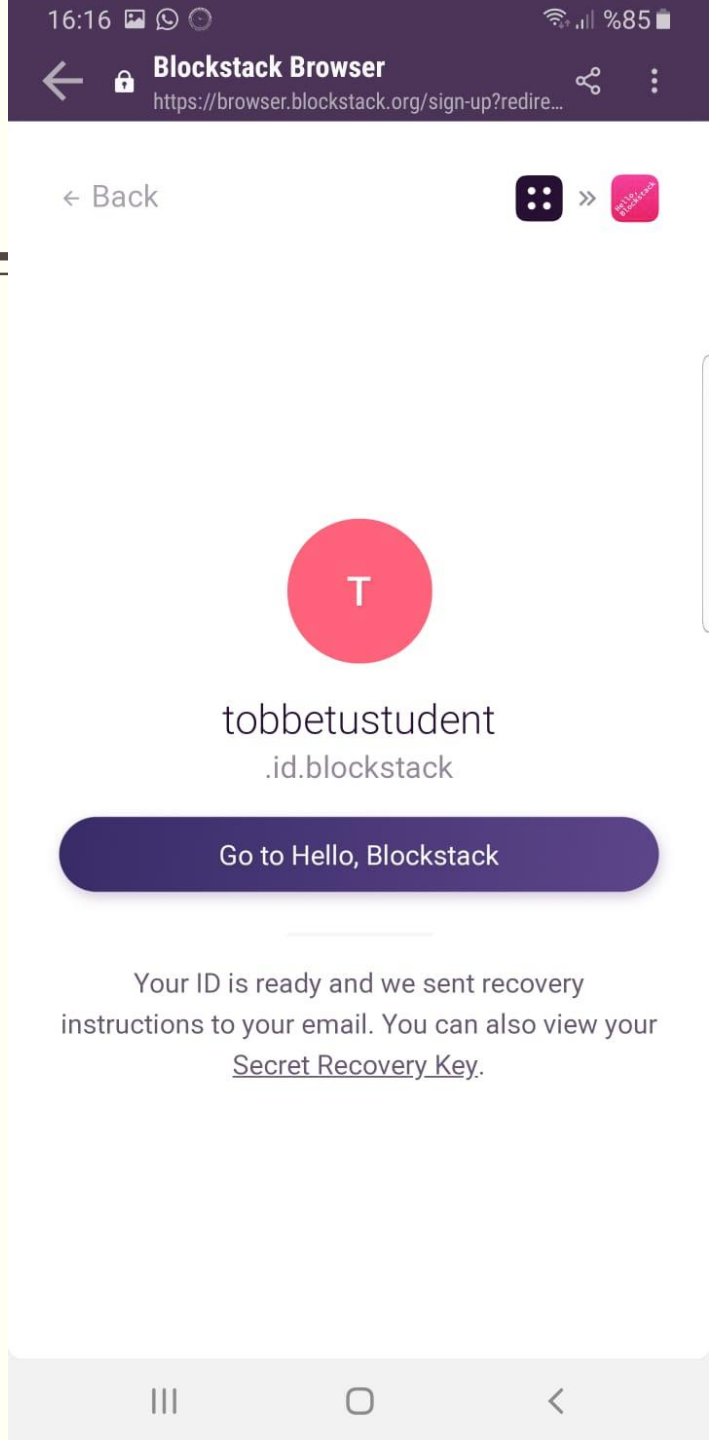
- Blockstack ile ilgili tehditler:
  - Ademi merkezi yapısından ötürü veri ve anahtarlara erişemez
  - Depolanan veri şifreli, imzalı ve farklı adreslerde tutulduğundan bulut platformları erişemez
  - Kimlik doğrulamada e-posta adresi, sosyal medya hesapları ve kullanıcı adı kullanır
    - Yeterli değil, başkası adına bu bilgiler düzenlenebilir

BlockSignal Tasarımı

- Signal ile Blockstack entegrasyonu
- Blockstack Android SDK
- Signal ve Blockstack kütüphaneleri tasarıma göre modifiye edildi

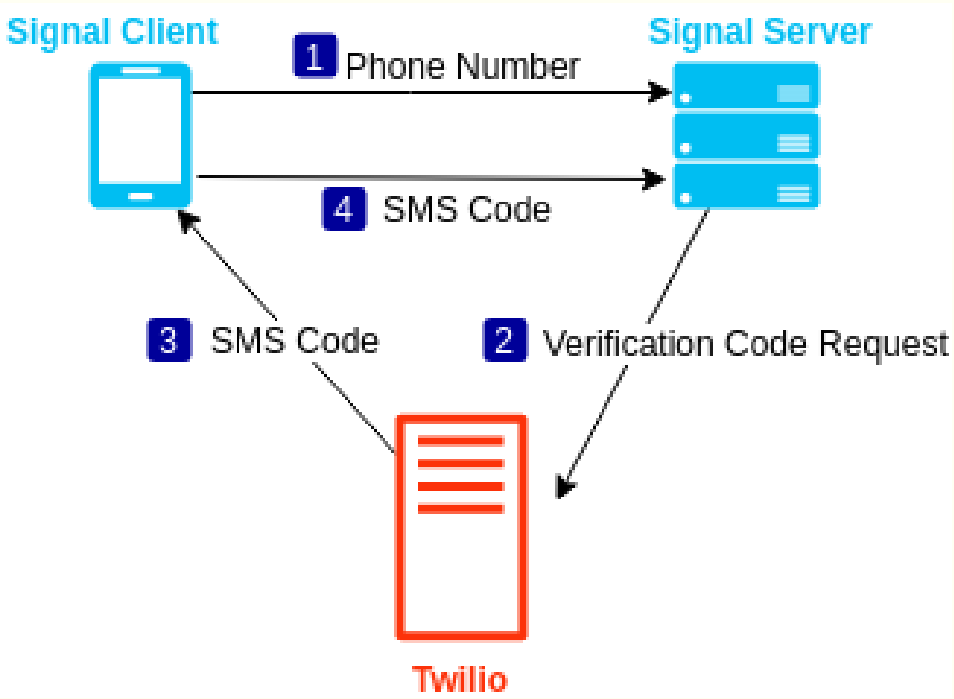
İlk kayıt

- Signal'da bulunan SMS doğrulaması ile Blockstack'te oturum açma
- BlockSignal üzerinden Blockstack hesabı açma
  - Kullanıcı adı, parola ve e-posta adresi girilir
  - E-posta ile «Magic Recovery Code» gönderilir
- BlockSignal açıldığında, kayıt olunan Blockstack kullanıcı adı seçilerek giriş yapılır
- Signal açık anahtarı, Blockstack gizli anahtarıyla imzalı olarak Gaia hubda saklanır
- SMS doğrulaması için girilen telefon numarası yine imzalı olarak Gaia huba yazılır
  - Sunucuya Gaia hub URL verilir, sunucu oradan numarayı çekip doğrulama kodunu gönderir
  - Böylece, Blockstack hesabı ile Signal hesabı eşleştirilir

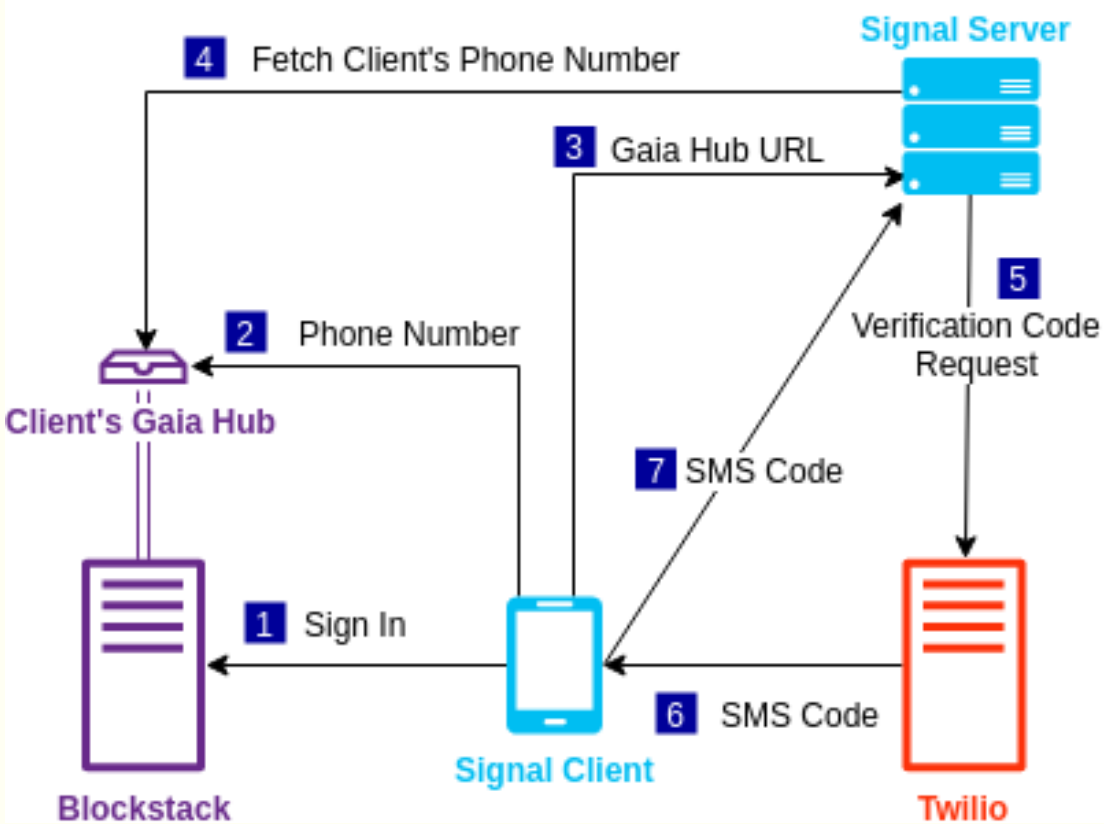


İlk Kayıt – Arka Plan

Signal



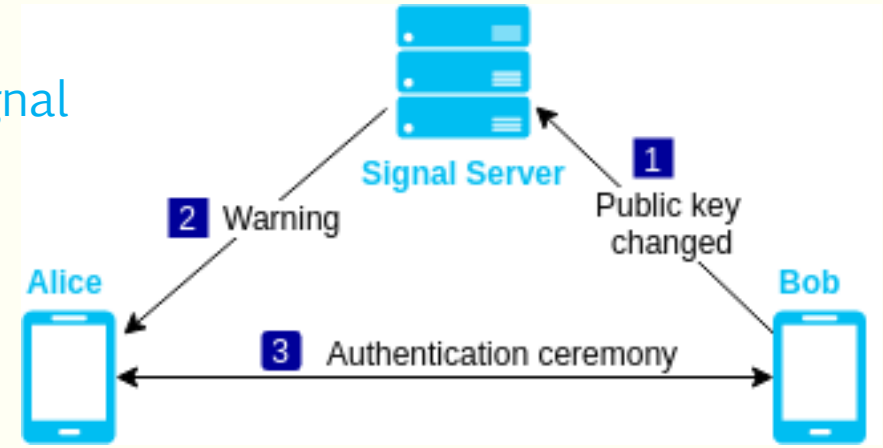
BlockSignal



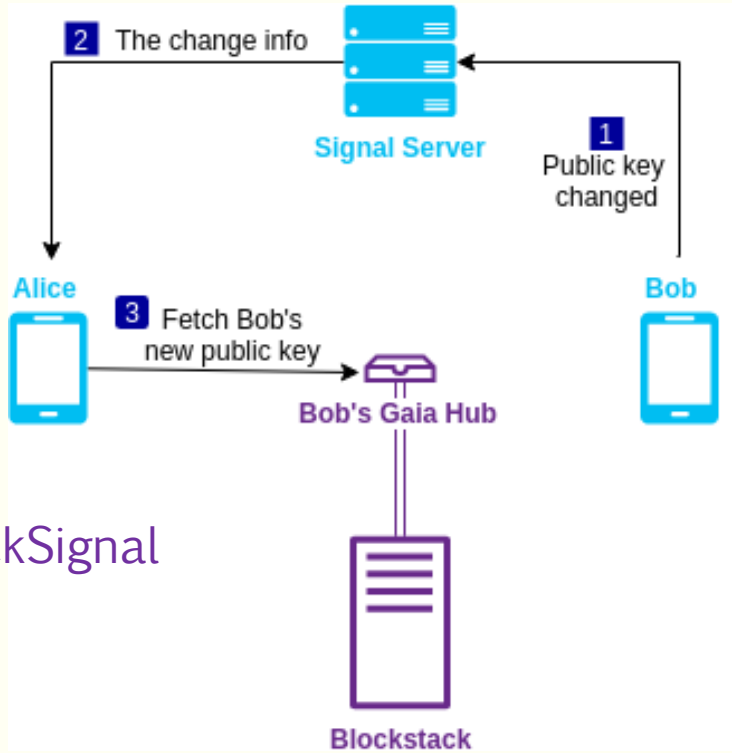
Mesajlaşma

- Mesajlaşma açısından Signal ile BlockSignal aynı
- Ancak, BlockSignal kimlik doğrulama seremonisi yerine otomatik olarak açık anahtar ve telefon numaralarını doğrular
- BlockSignal, Signal açık anahtarı değiştiğinde
  - İstemci tarafında alıcının açık anahtarını ve telefon numarasını Gaia hubından çeker
  - İmzaları alıcının Blockstack açık anahtarıyla doğrular
  - Doğrulama başarılı ise dönüt verilmeksizin oturum devam eder
  - Aksi halde, oturum kullanıcı bilgilendirilerek sonlandırılır

Signal

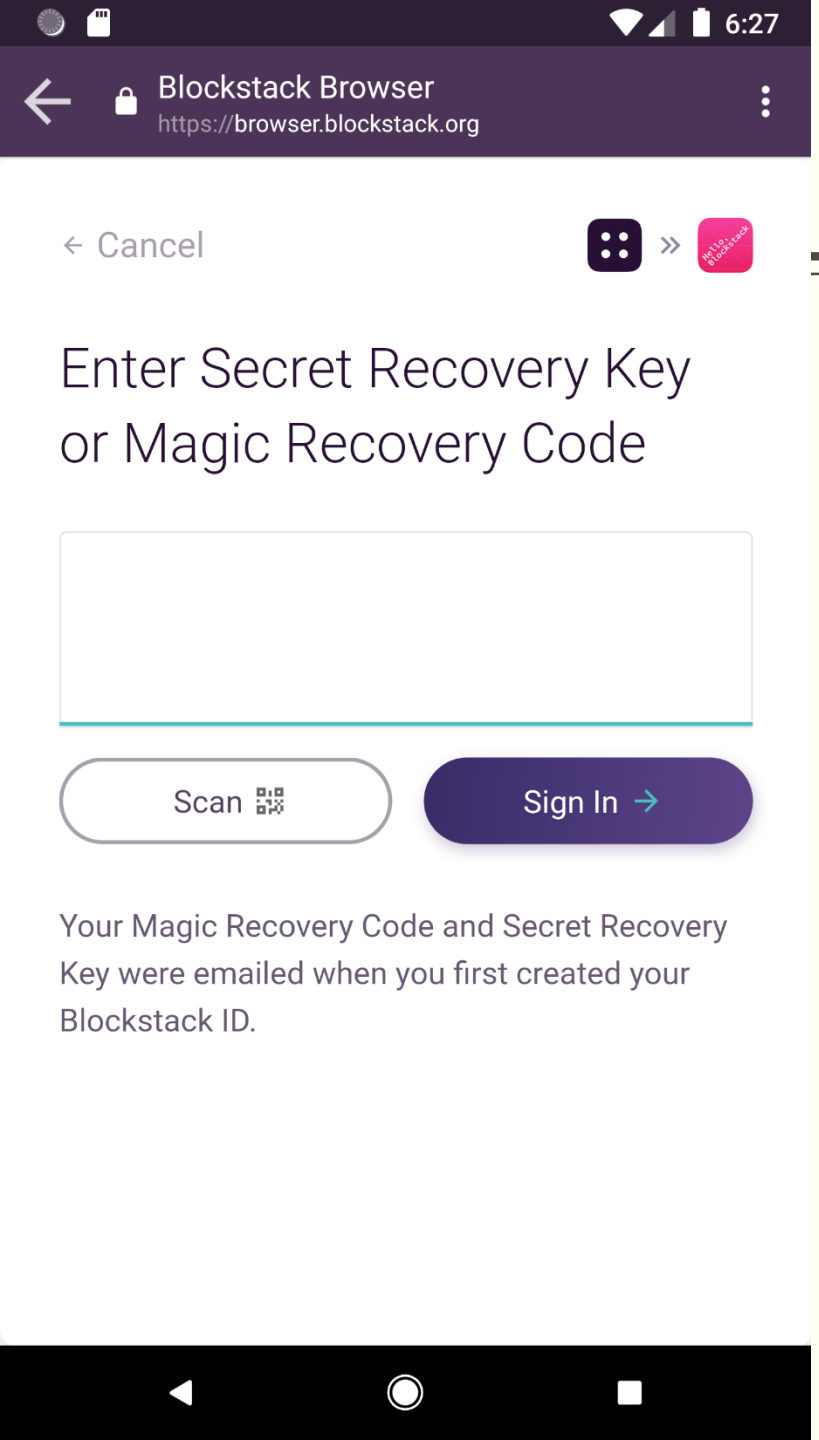


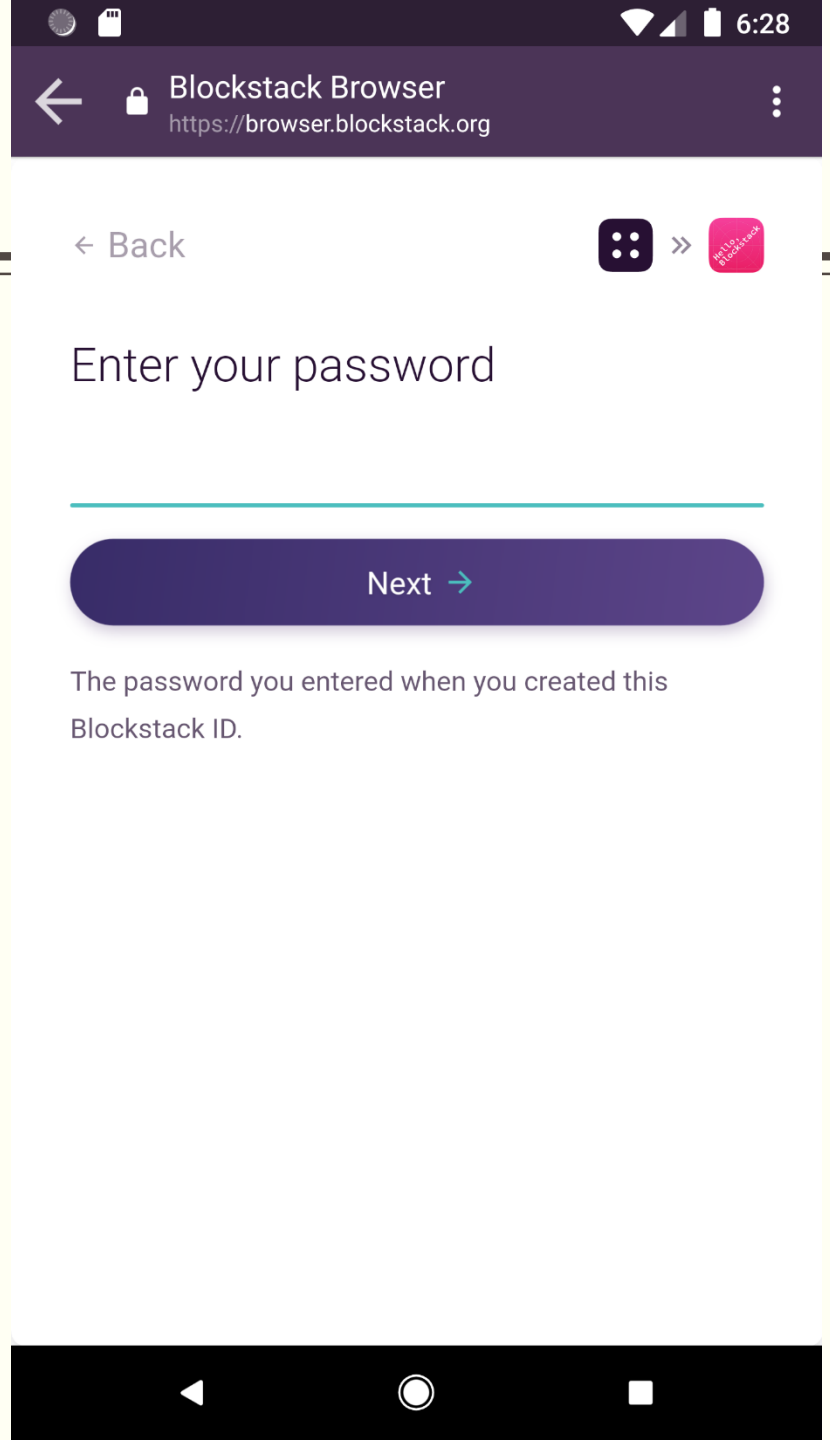
BlockSignal

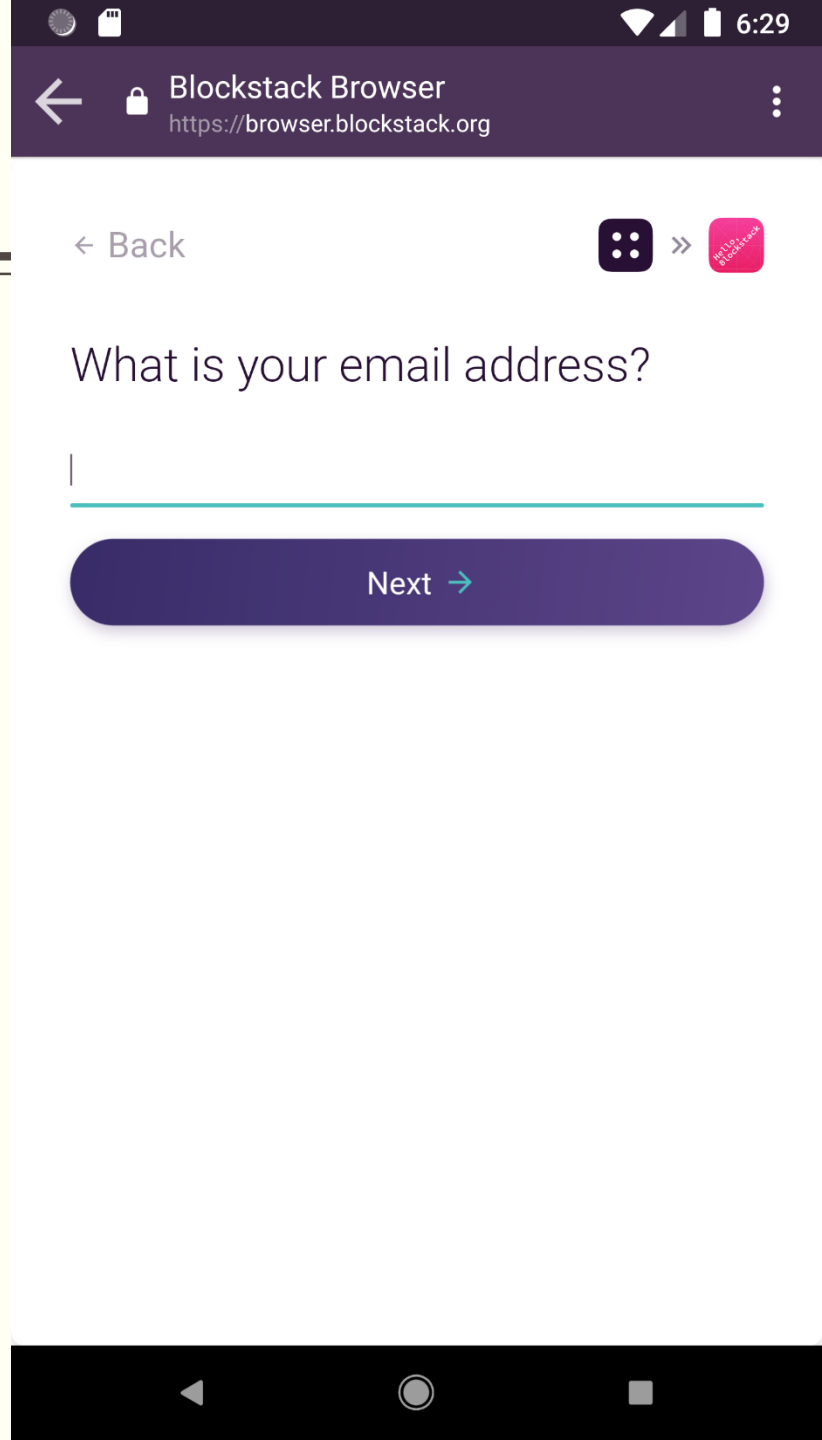


Tekrar Kayıt

- Kullanıcıların çeşitli nedenlerle BlockSignal'a tekrar kaydolması gerekebilir
- Tekrar kaydolma sebebine göre işlem basamakları farklılık gösterir
- 1. durum: Cihaz değişikliği
  - Bu durumda, gizli anahtar da kaybolduğundan yeniden üretilmelidir
  - E-posta ile gönderilen «Magic Recovery Code» kullanılarak Blockstack hesabına giriş yapılır
    - Ardından, parola ve e-posta sırasıyla girilir
    - Bu şekilde, anahtar çifti üretilir ve cihaza kaydedilir
- 2. durum: SIM kart değişikliği veya uygulamayı yeniden yükleme
  - Bu durumda, gizli anahtar aynı kalır
  - BlockSignal açıldığında oturum açılmış kullanıcı adı belirir
    - Kullanıcı adına tıklanarak SMS doğrulamaya geçilir


6:27
Blockstack Browser
https://browser.blockstack.org
Cancel
Enter Secret Recovery Key or Magic Recovery Code
Scan
Sign In
Your Magic Recovery Code and Secret Recovery Key were emailed when you first created your Blockstack ID.


6:28
Blockstack Browser
https://browser.blockstack.org
Back
Enter your password
Next
The password you entered when you created this Blockstack ID.


6:29
Blockstack Browser
https://browser.blockstack.org
Back
What is your email address?
Next

Güvenlik Analizi

- Kötücül/Ele geçirilmiş sunucu:
  - İlk kurulum esnasında, iki taraf birbirinin Blockstack kullanıcı adını biliyorsa
    - Blockstack kullanıcı adıyla Gaia'dan çekilen imza doğrulanamaz
  - Mesajlaşma esnasında, MITM olursa
    - Açık anahtar değişmiş görünse de Gaia'da aynıdır, imza doğrulanamaz

- SSL sabitlemeyi atlatma:
  - Ele geçirilmiş sunucuda olduğu gibi saldırganın açık anahtarı Gaia'daki imzayı doğrulayamaz

- SIM kart klonlama:
  - Saldırgan, Blockstack hesabına da giriş yapmalıdır
  - Blockstack hesabını ele geçirmesi gerekir
  - Mevcut oturumda yapılırsa imza yine doğrulanamaz

Güvenlik Analizi

- Bilinmeyen anahtar paylaşımı saldırıları (Unknown key-share attacks):
  - Signal'da bu saldırıların gerçekleştirlmesi için saldırganın açık anahtarını başka bir kullanıcının doğrulaması gerekir
  - BlockSignal'da böyle bir mekanizma olmadığından saldırı yapılamaz

- Blockstack ile ilgili tehditler:
  - Telefon numaraları kullanıcıları doğru bir şekilde tanımlayabilir
  - Blockstack oturum açma işlemlerine telefon numarası dahil edildi
  - Blockstack hesabı ile telefon numaraları eşleştirildi

Sonuç

- Güvenli mesajlaşma uygulamalarında kimlik doğrulama seremonisine ihtiyaç olmadığı gösterilmiştir
- Blokzincirin güvenli mesajlaşma uygulamalarında kullanılabileceği ortaya konulmuştur
- Açık anahtar doğrulamasında insan faktörü güvenlik çemberinin dışına taşınmıştır
- Çözüm açık kaynaklı olarak paylaşılarak araştırmacıların faydasına sunulmuştur
- Çözümün güvenlik analizi yapılarak Signal'da ortaya çıkabilecek muhtemel tehditlere karşı dayanıklılığı gösterilmiştir

TEŞEKKÜRLER...