

SAMSUNG SDS

Realize your vision

Techtonic 2019

Partner



Foresee

Disrupt

2019.11.14 • SAMSUNG SDS Tower B1F
Magellan Hall / Pascal Hall

Track 3 | Blockchain

삼성 블록체인 키스토어
**당신의 블록체인 어플리케이션은
안전한가요?**

이성혁 프로 (블록체인서비스그룹) / 삼성전자 무선사업부

it all happened because of

private key

What is a private key?



Alice

Send 0.05 Bitcoin 

----->

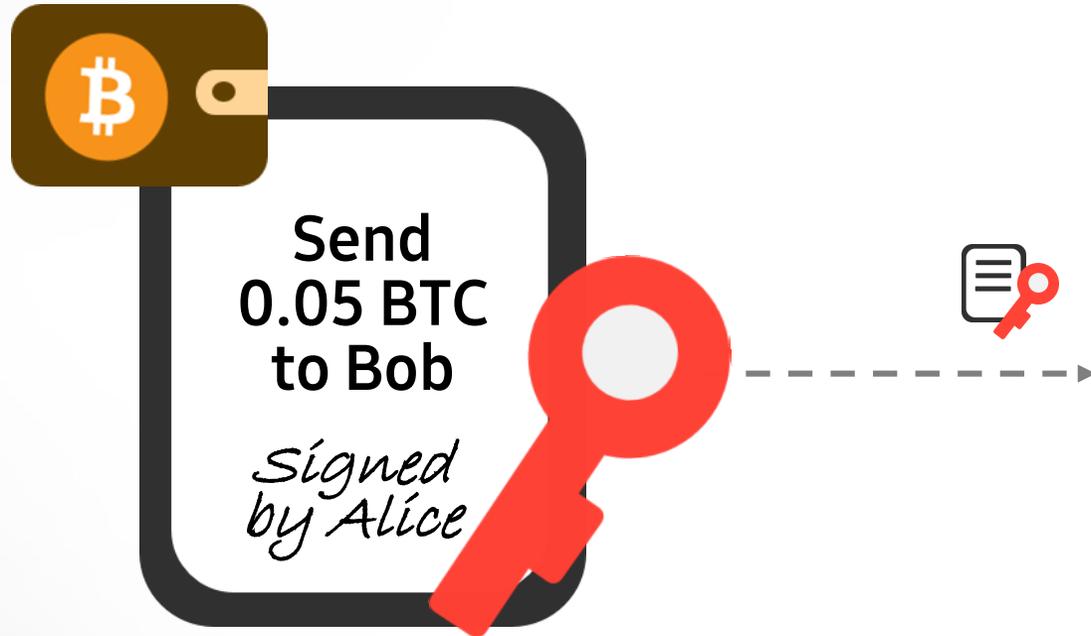


Bob

What is a private key?



Alice



Wallet

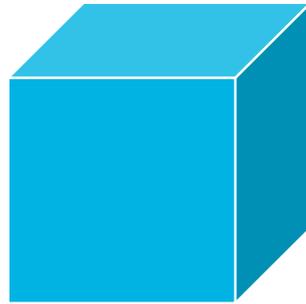


Bitcoin Network

What is a private key?



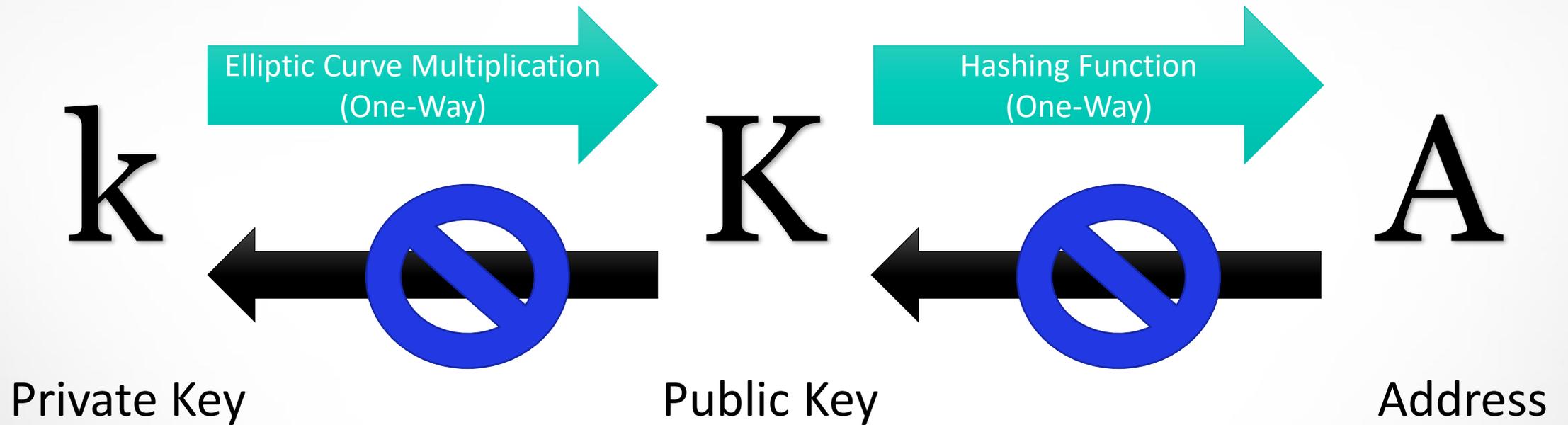
Blockchain



Bob



Blockchain address



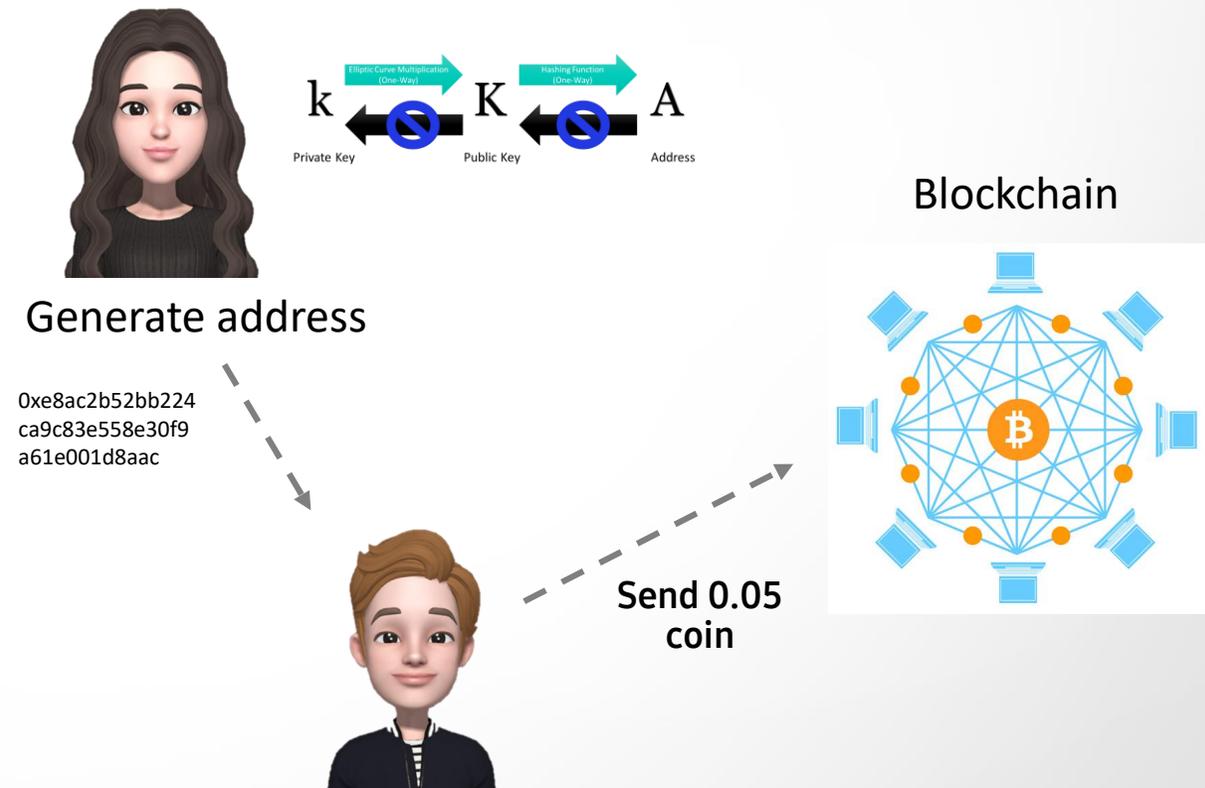
Who creates account ?

Financial institutions issue accounts



No central authority.

Alice generates key and address by herself



Private Key

Challenge is how to *safely* manage user's private key



Signature

required to make a transaction

Private Key

generates the signature

Hardware and Paper Wallet

isolated environment to avoid remote attacks



Hardware Wallet



Paper Wallet

yet remaining **usability** issues

AGENDA

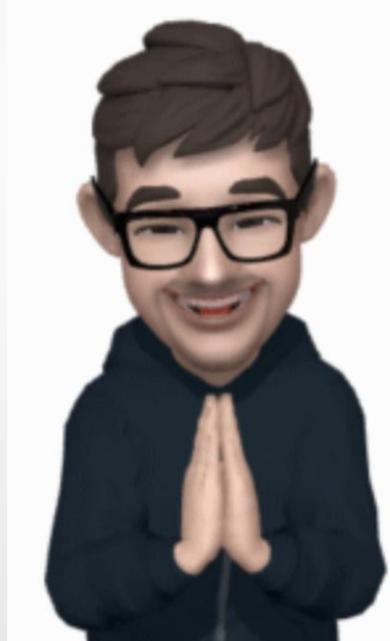
1. What is a “Good” Wallet?
2. Introduction to Samsung Blockchain Keystore
3. What makes Keystore Secure and Unique
4. Samsung Blockchain Keystore SDK
5. What’s Next

1

What is a “Good” Wallet?

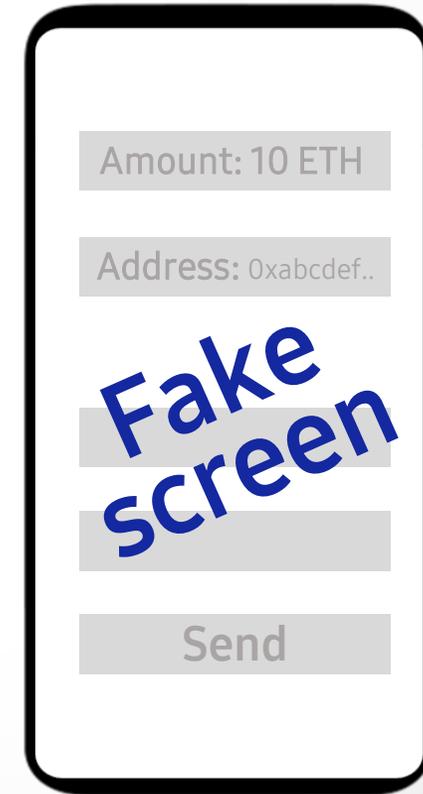
Inevitable security vulnerabilities

Concern: the **mobile environment** that the blockchain technology is executed in



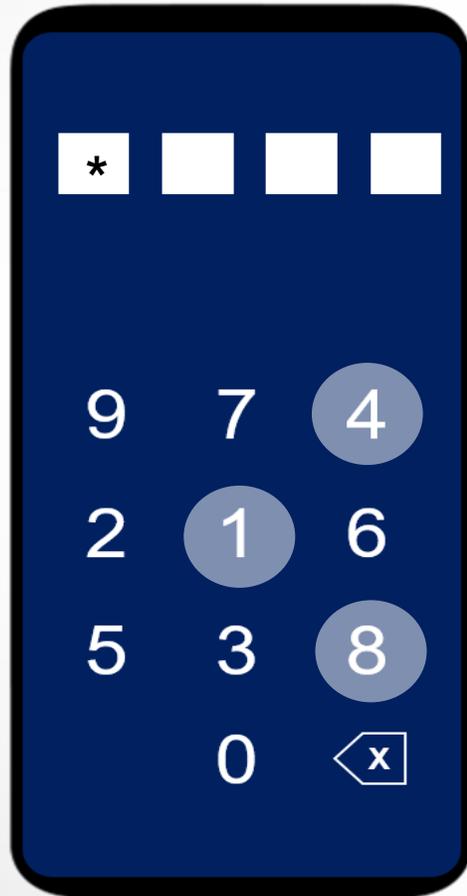
Hacker

Stealing your
key is easy!



Workaround to avoid hacking

Becoming more and more complicated



Password Criteria

- ✓ At least 8 characters
- ✓ At least 1 small letter
- ✓ At least 1 big letter
- ✓ At least 1 number
- ✓ At least 1 special character (*, !, %...)

Security Solutions

- Application Integrity
- Device Integrity



Then what is a “Good” wallet?

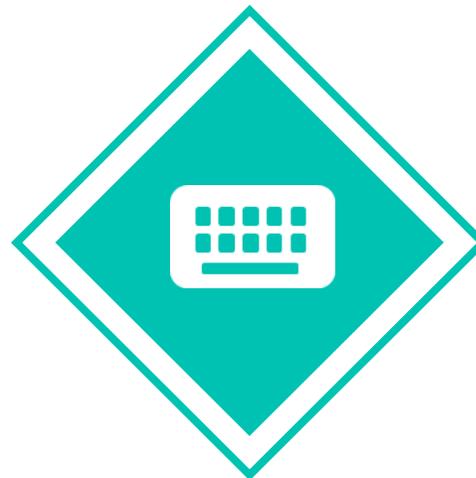
Security considerations when developing Samsung Blockchain Keystore



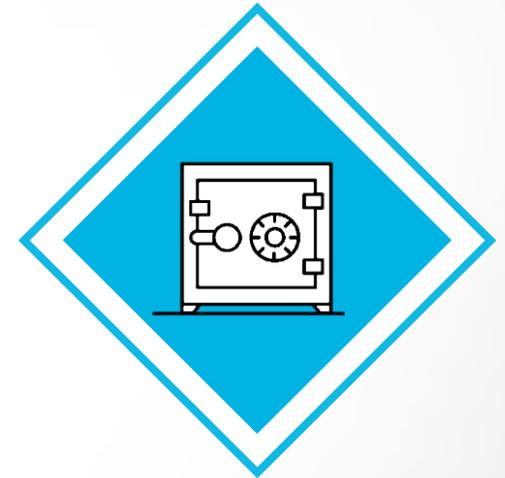
Secure
Computation



Secure
Display



Secure
Touch



Secure Storage
Keep private key safe

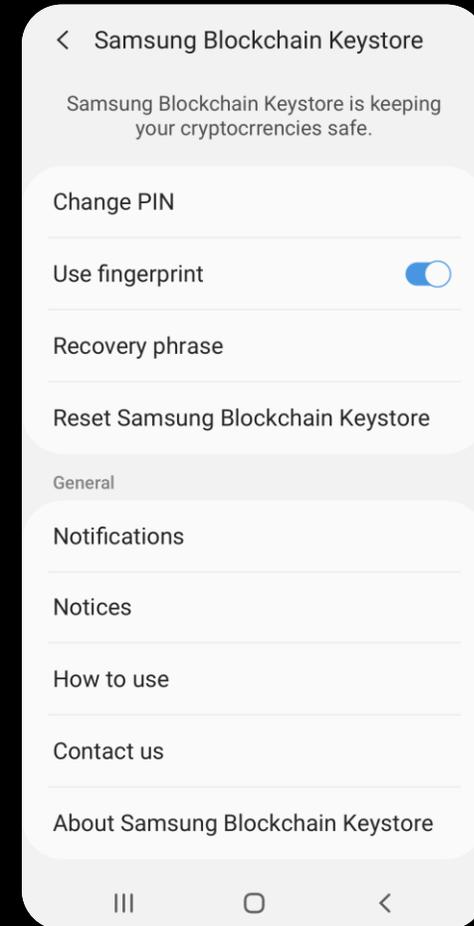
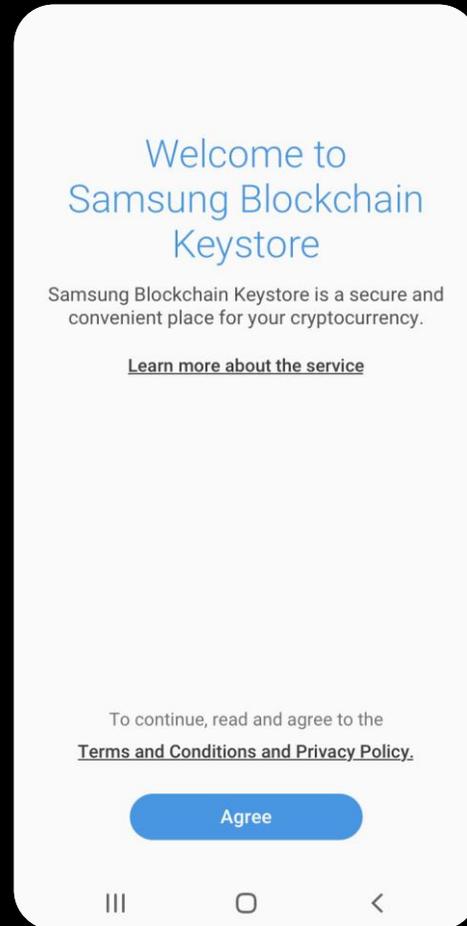
2

**Introduction to
Samsung Blockchain Keystore**



Samsung Blockchain Keystore

launched earlier this
year to keep your
private key safe



Samsung Blockchain Keystore SDK

The screenshot shows the Samsung Developers website for the Samsung Blockchain Keystore SDK. The page is titled "Samsung Blockchain Keystore SDK" and is part of the "Services & APIs" section. The navigation menu includes "Bixby", "SmartThings", "Services & APIs", "Devices", "Program", "Community", "Blog", "Events", and social media icons for Facebook, Twitter, Instagram, YouTube, LinkedIn, and RSS. The left sidebar contains a navigation menu with items like "Samsung Blockchain SDK", "Platform", "Keystore", "Understanding Keystore", "Keystore SDK", "Essential Contents", "Overview", "Technical Document", "FAQ", "Restrictions", "Cryptocurrency Specification", "Programming Guide", "Release Note", "Request for API Key", and "Apply for Partnership". The main content area is titled "Essential Contents" and lists "Samsung Blockchain Keystore SDK" (Version: 1.2.0 | Oct 29, 2019), "API Reference (JavaDoc)", and "Programming Guide". Below this is an "Overview" section with a paragraph and a list of bullet points.

Samsung Blockchain Keystore SDK

Version: 1.2.0 | Oct 29, 2019

API Reference (JavaDoc)

Programming Guide

Overview

Samsung Blockchain Keystore SDK allows your Android app DApp, to communicate directly with Samsung Blockchain Keystore, a preloaded feature on selected Galaxy devices. By integrating Samsung Blockchain Keystore SDK into your Android app, you can leverage the following:

- **Get Blockchain address to link to the Samsung Blockchain Keystore**
Developers can link user's Blockchain address like a user's account. With the address returned from Samsung Blockchain Keystore, developers can check and show users how much cryptocurrency balance is in the account as well.
- **Get Blockchain address to link to the Samsung Blockchain Keystore**
Developers can link user's Blockchain address like a user's account. With the address returned from Samsung Blockchain Keystore, developers can check and show users how much cryptocurrency balance is in the account as well.

Open to public on
Samsung Developers

key generator?

Android
keystore?

storage?



SAMSUNG
Blockchain Keystore

signatures?

visible?





SAMSUNG Blockchain Keystore

a **blockchain**-dedicated Keystore launched earlier this year



Parse blockchain transactions



User's manual confirmation



Sign multi-cryptocurrencies

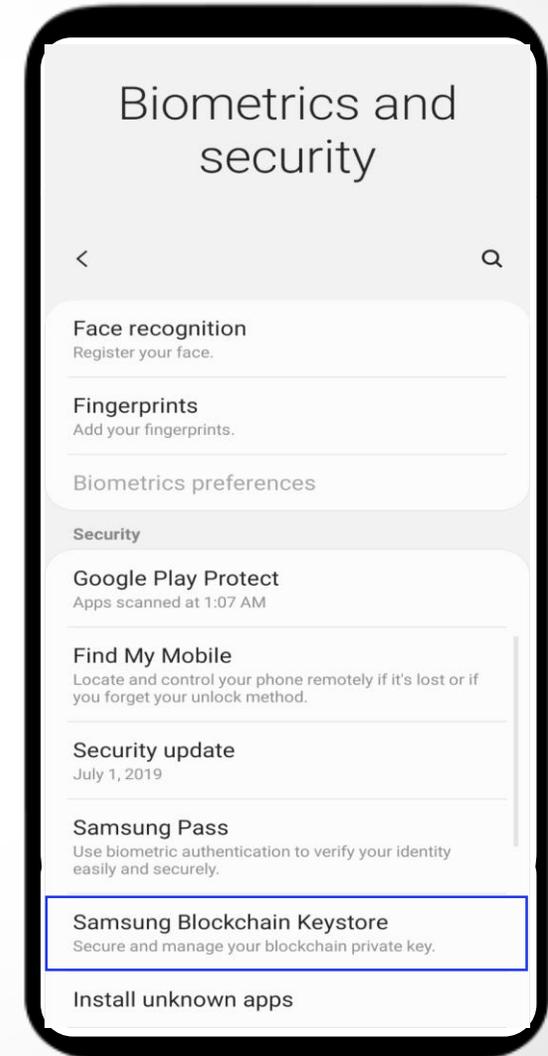
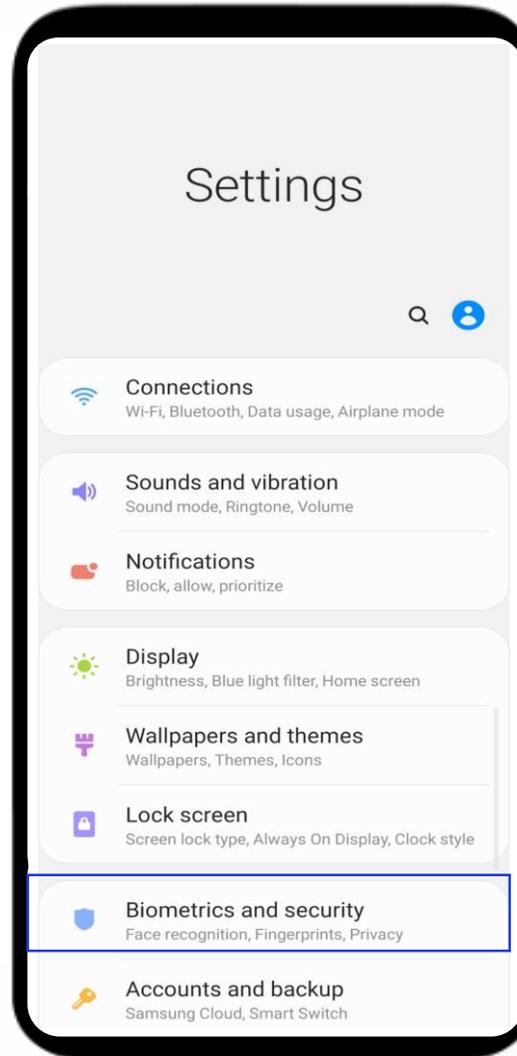
Samsung Blockchain Keystore

Where can I find it?

Device Settings >

Biometrics and Security >

Samsung Blockchain Keystore

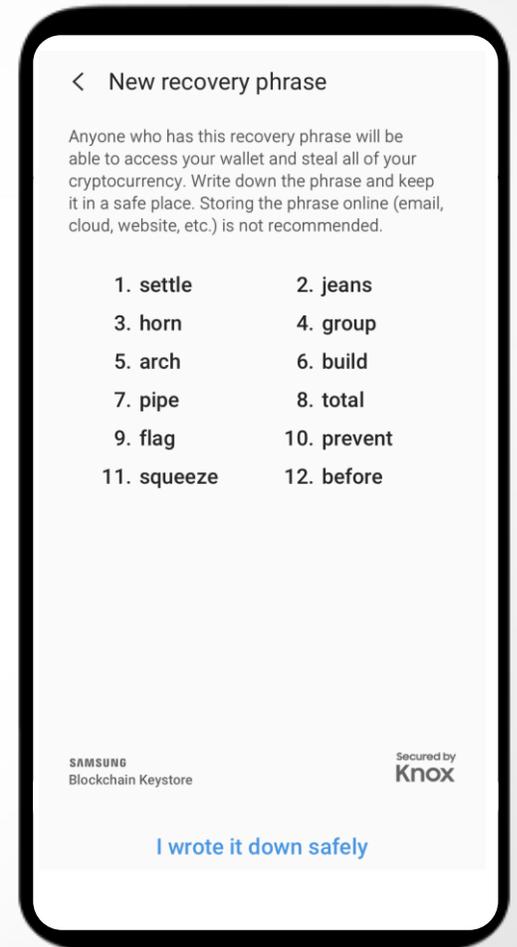
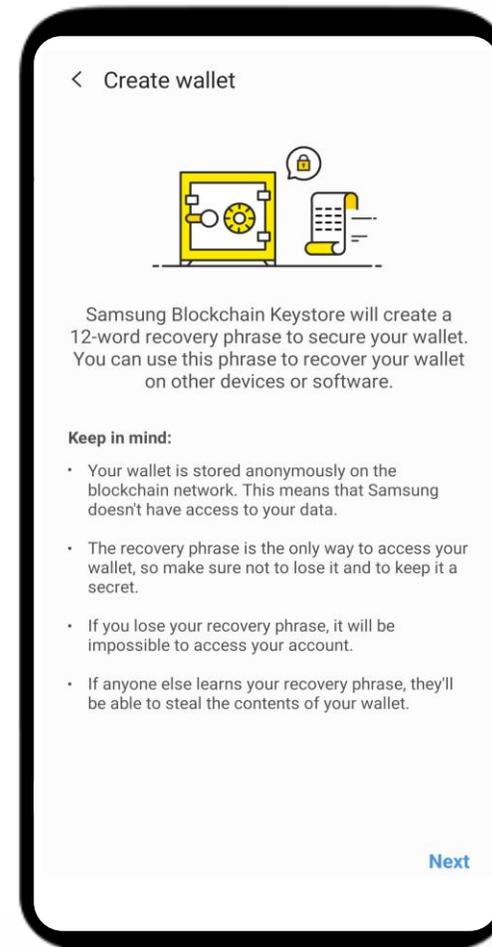
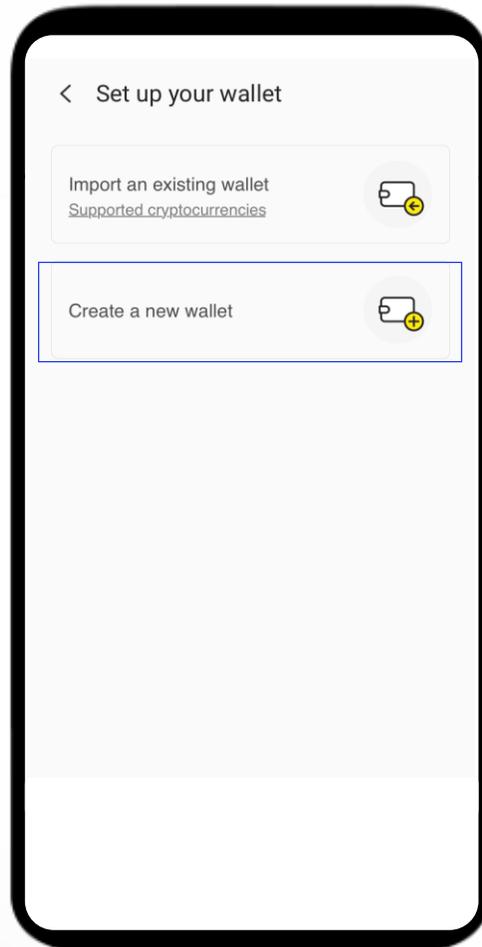


Samsung Blockchain Keystore

Main Features

(1) Key Management

Create a Wallet

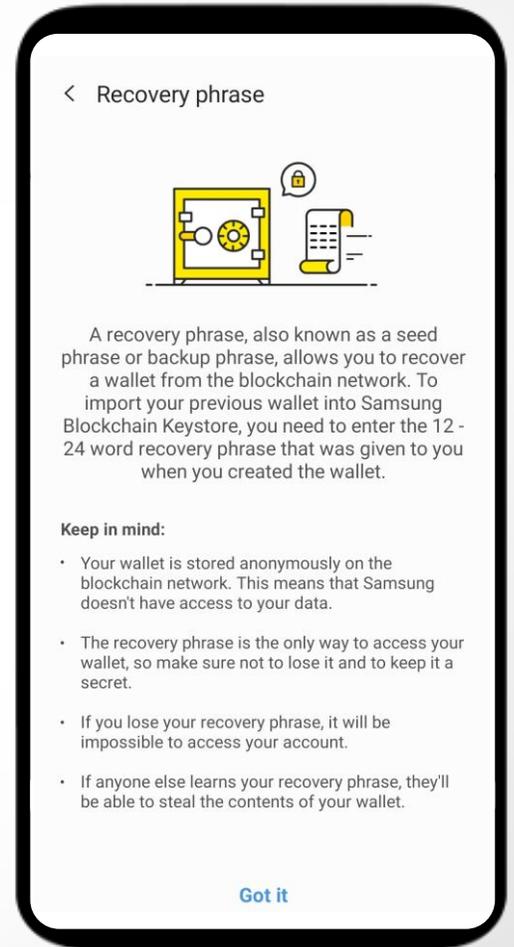
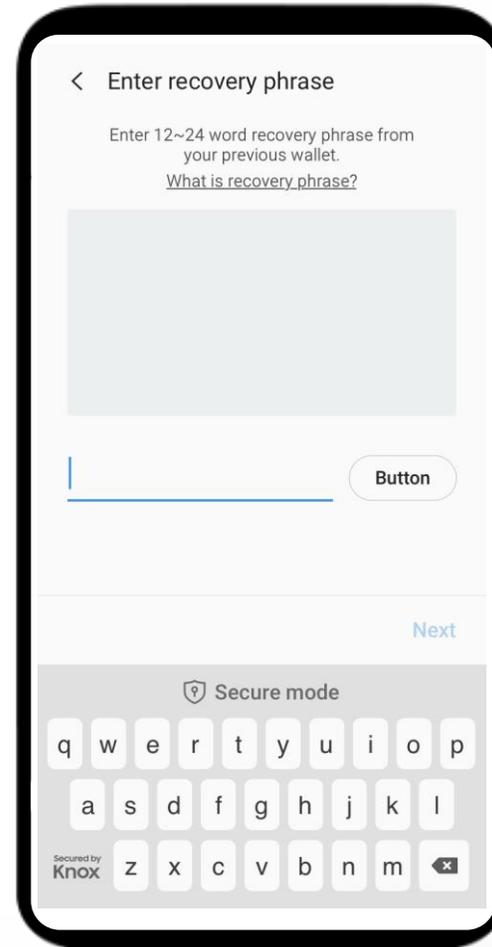
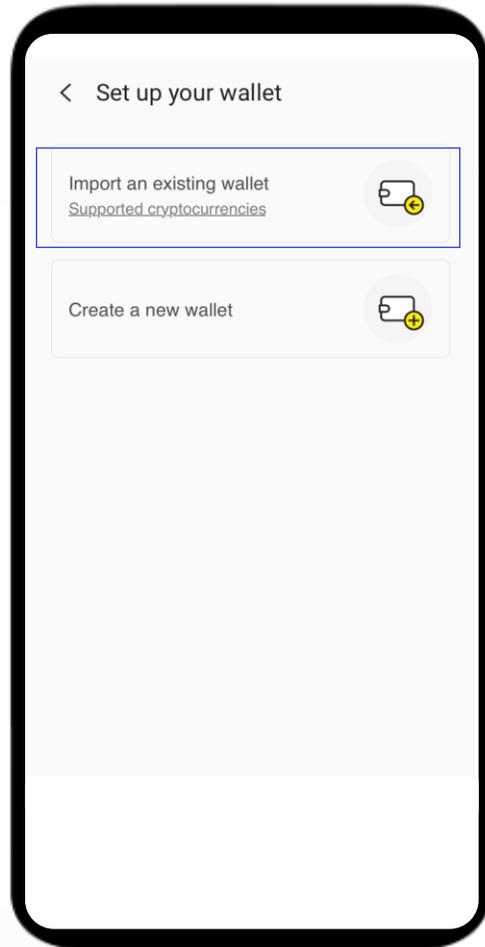


Samsung Blockchain Keystore

Main Features

(1) Key Management

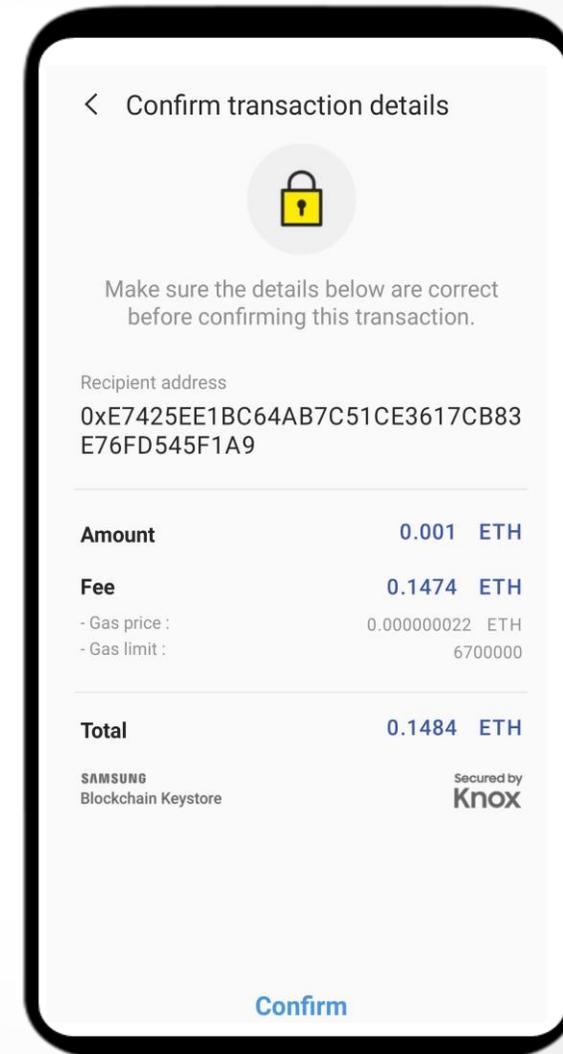
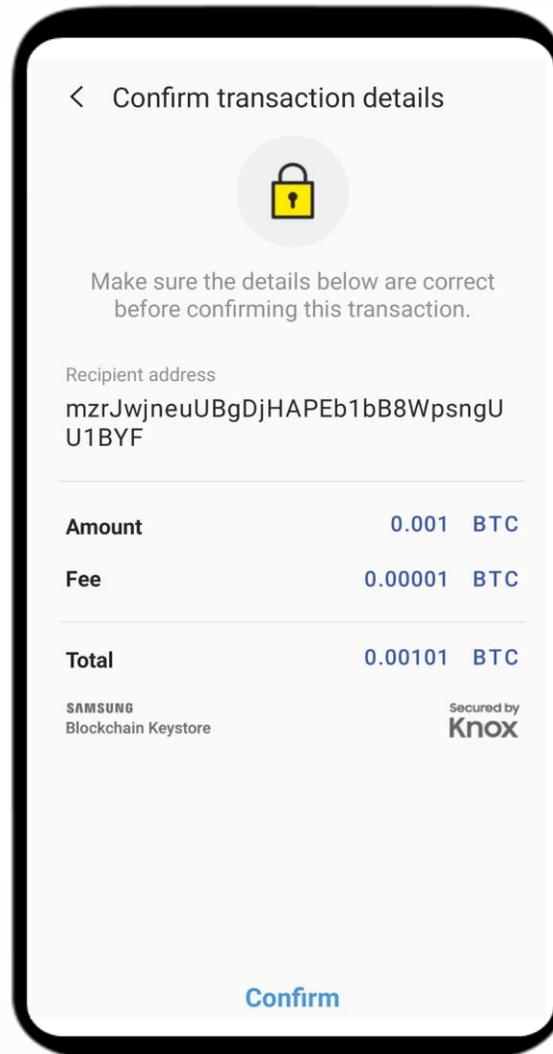
Import a Wallet



Samsung Blockchain Keystore

Main Features

(2) Sign a transaction

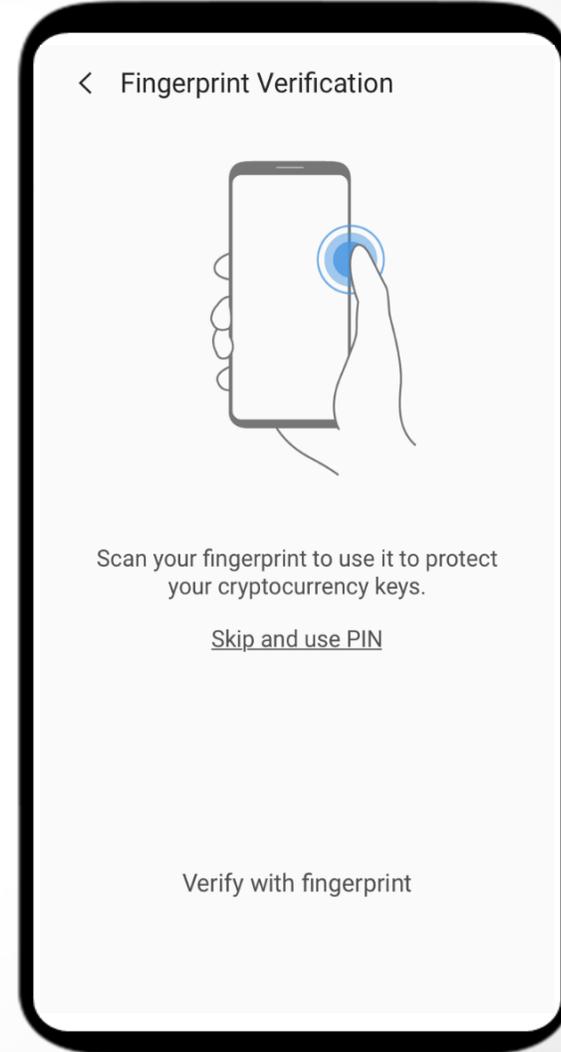
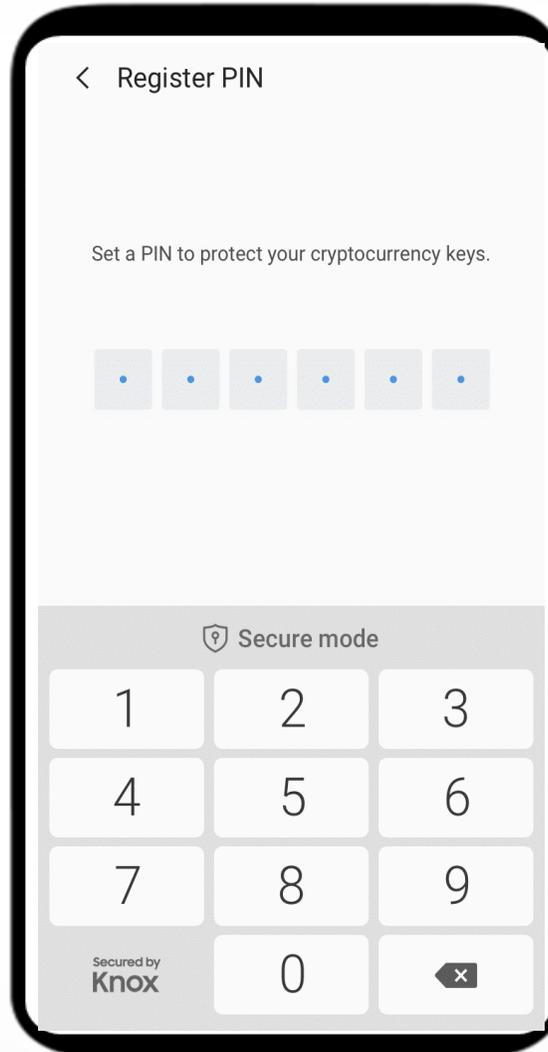


Samsung Blockchain Keystore

Main Features

(3) Manage Authentication

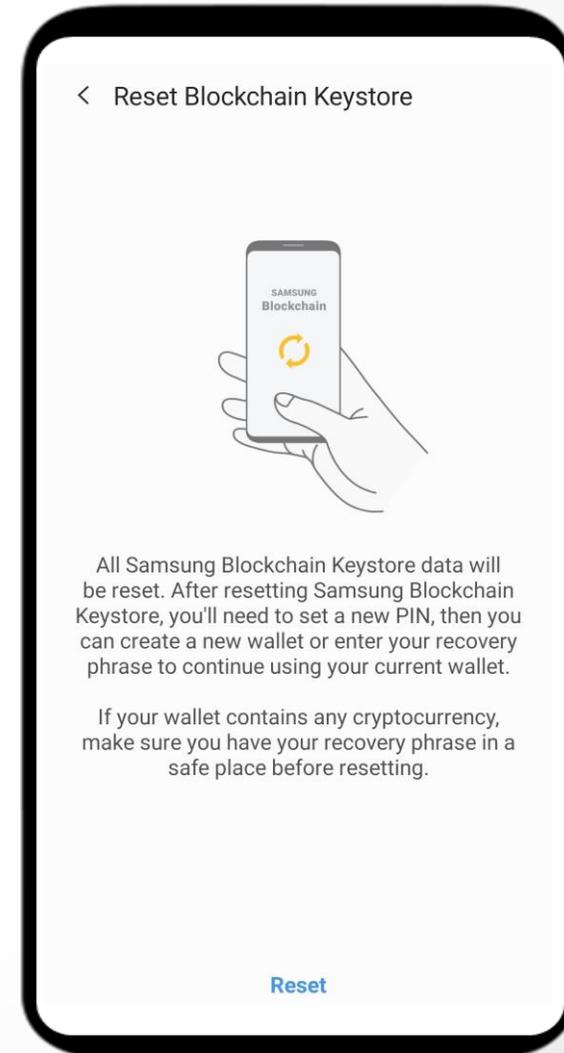
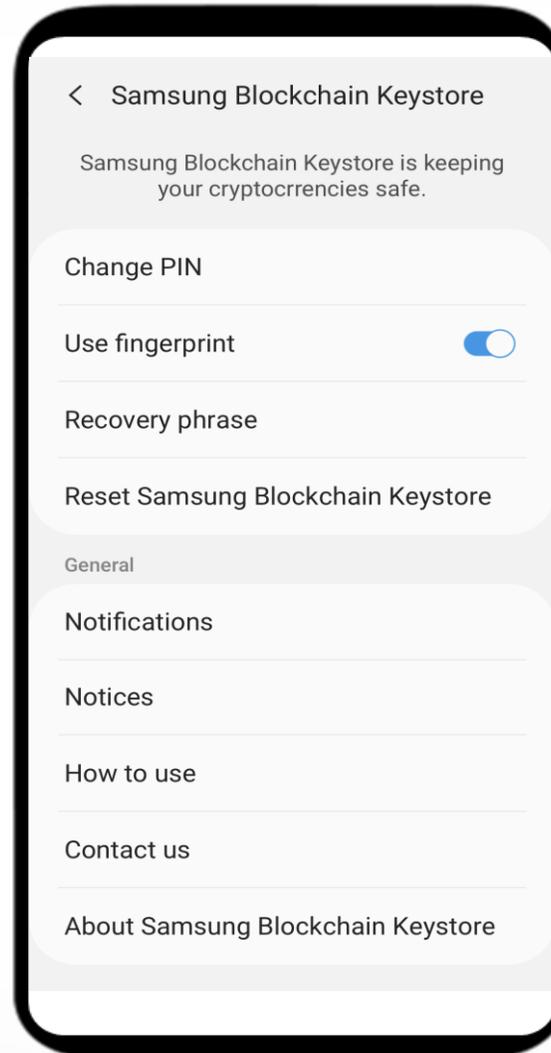
Authentication is needed to confirm a transaction



Samsung Blockchain Keystore

Main Features

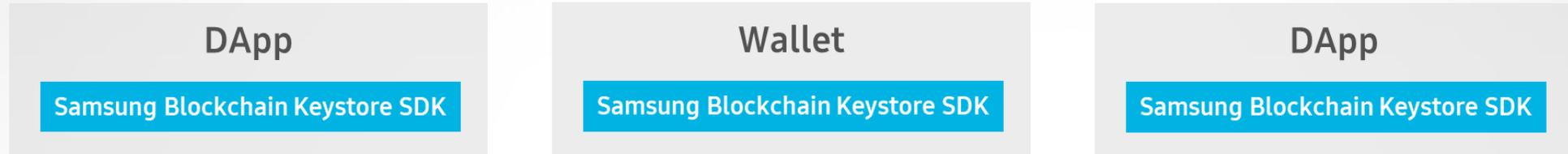
(4) Manage Settings



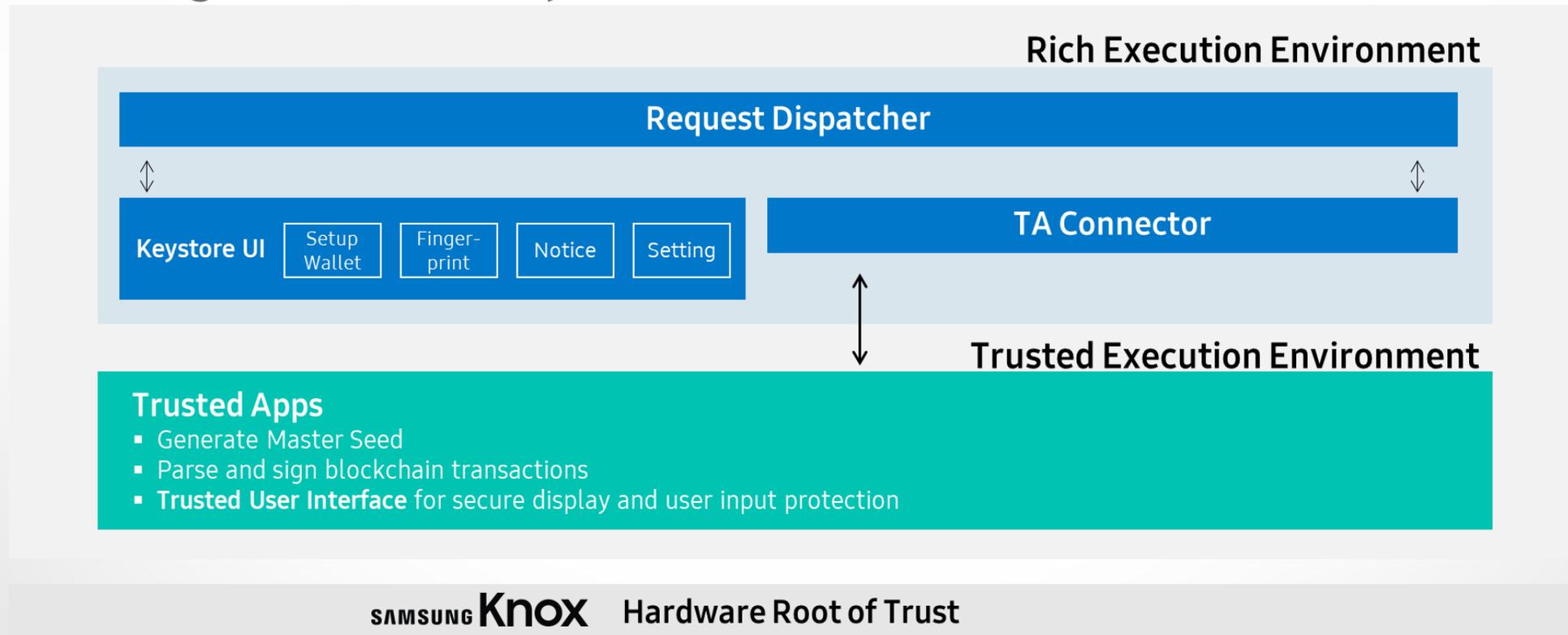
3

What Makes Keystore Secure and Unique

Architecture



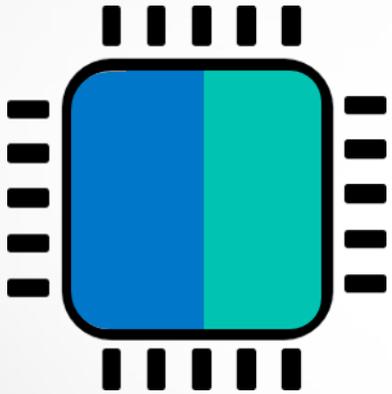
Samsung Blockchain Keystore



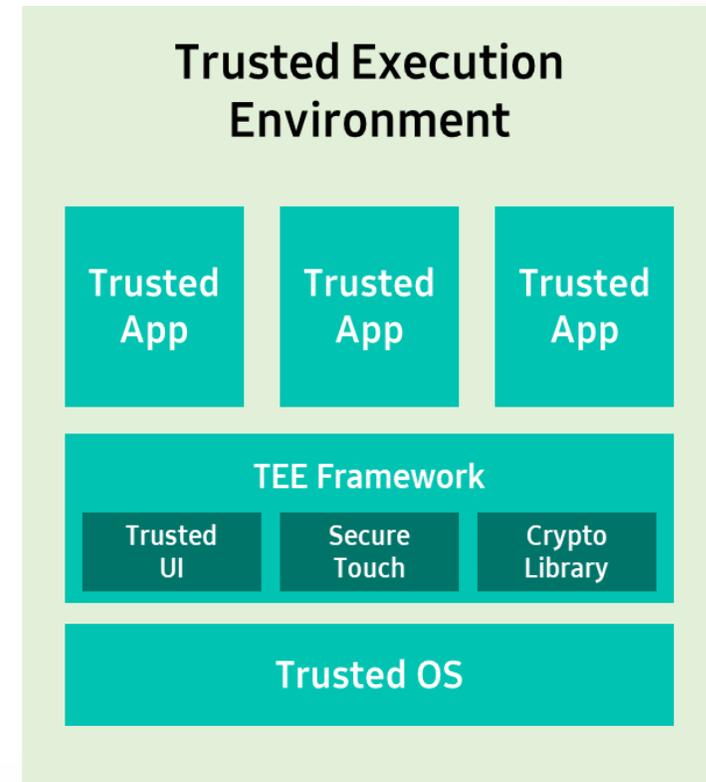
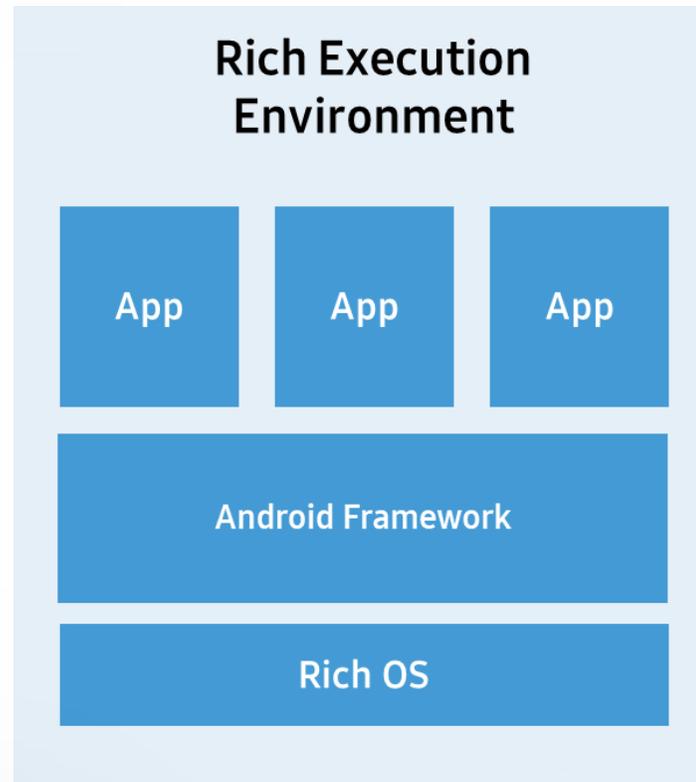


Secure Computation

Trusted Execution Environment



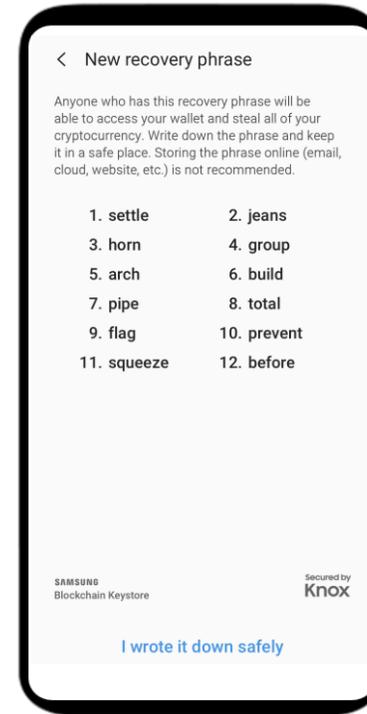
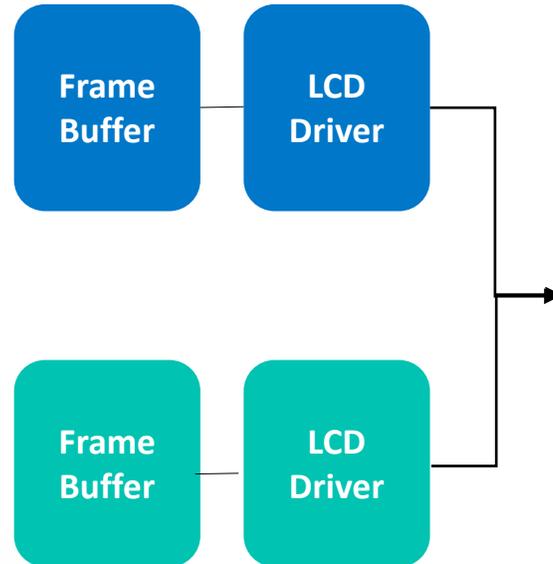
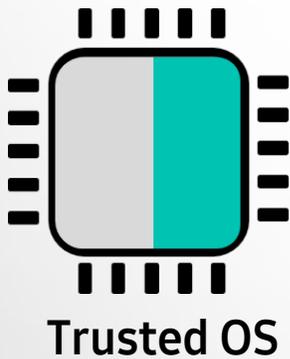
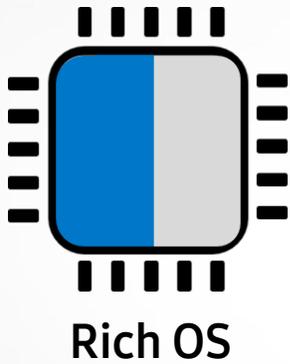
Rich OS Trusted OS





Secure Display

Trusted User Interface



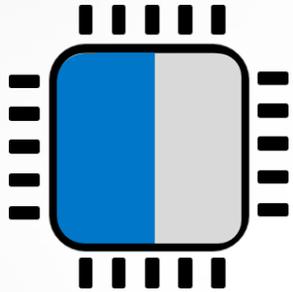
LCD Controller & LCD Panel

**No
screen
capture!**

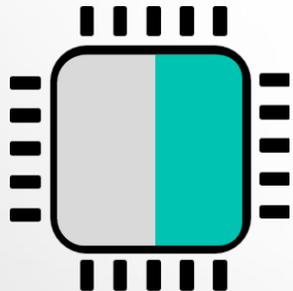


Secure Touch

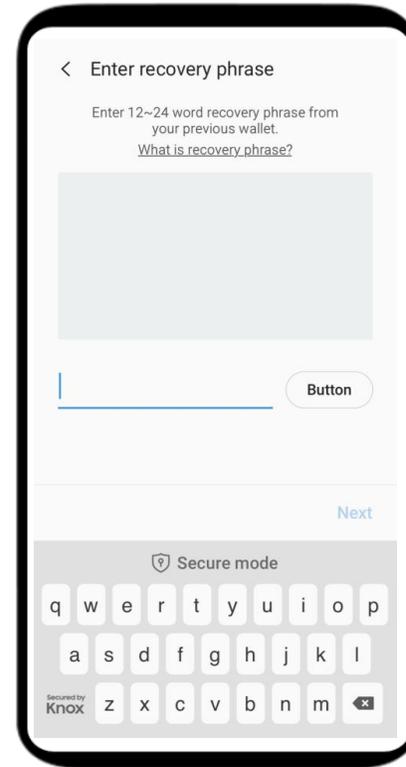
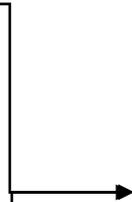
Trusted User Interface



Rich OS

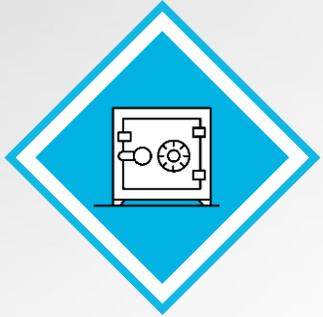


Trusted OS



Touch Screen Panel

No touch hooking!



Secure Storage

Hardware-based encryption



Trusted OS

encrypted and
safely stored

Secure your app with Keystore

Two main service flows of Keystore integration

1. Get Blockchain Address

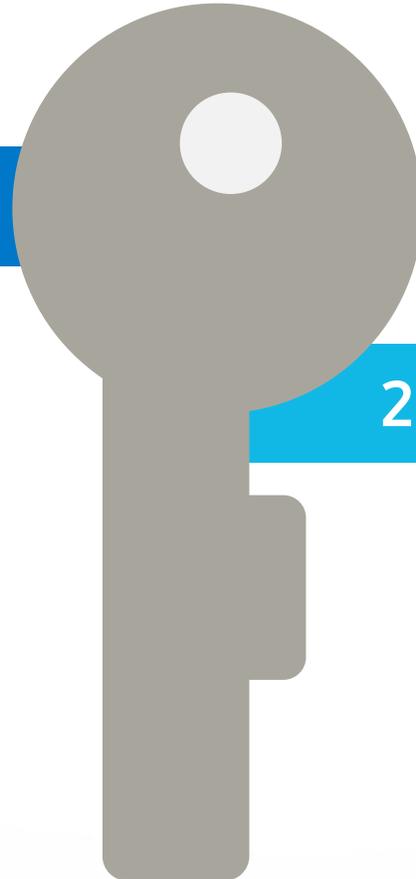


0xe8ac2b52bb224ca9c83e55
8e30f9a61e001d8aac

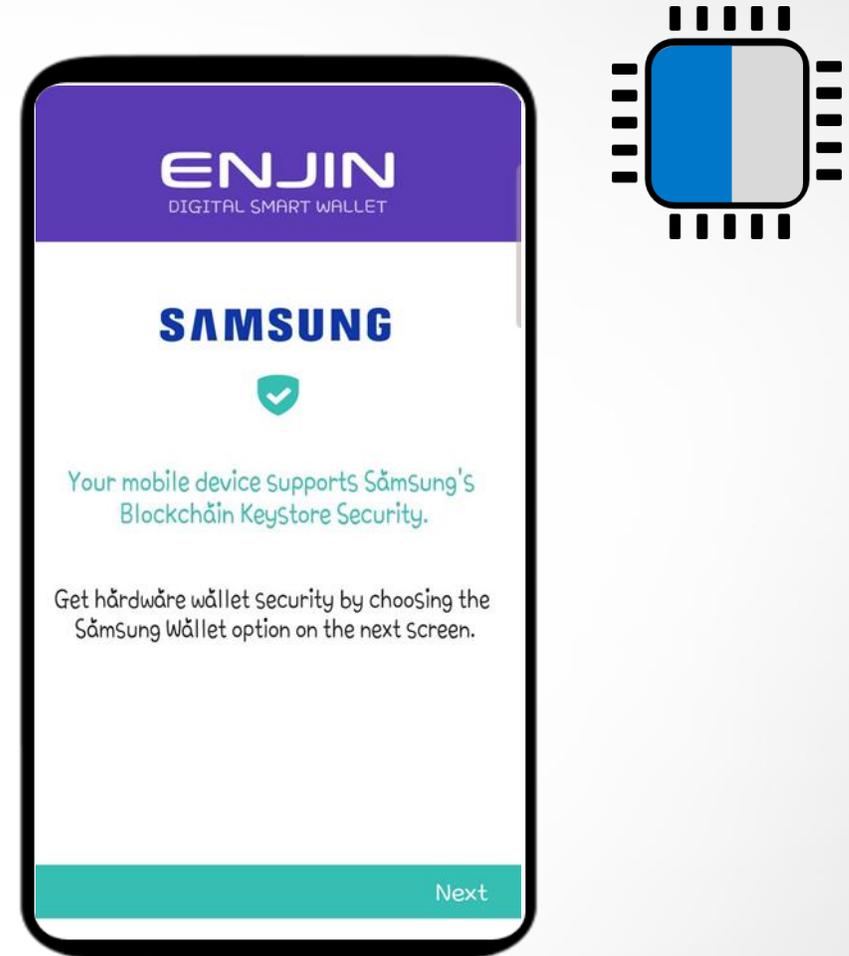
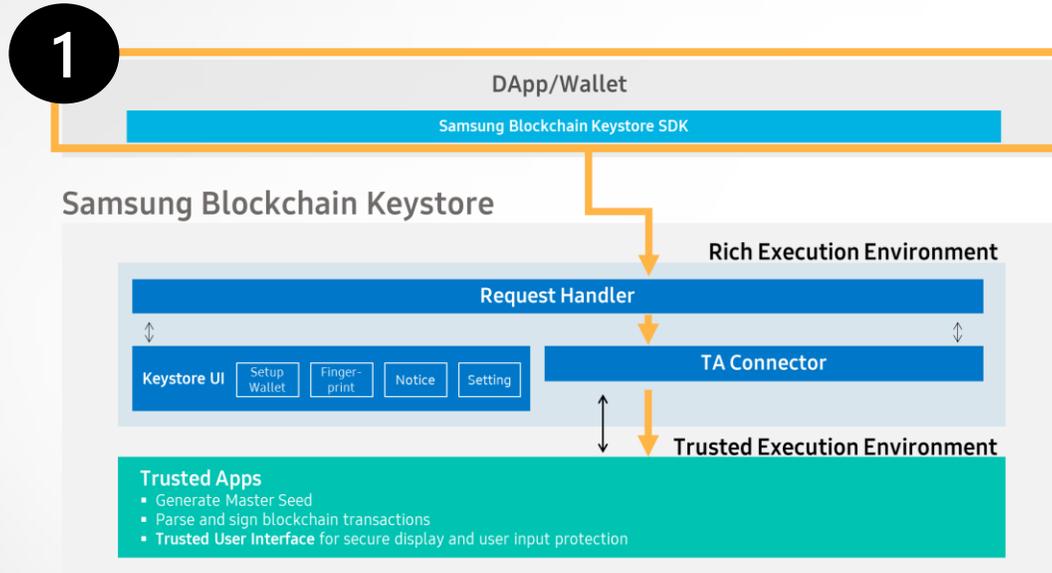


1F7FAt5kW55W9g7C2utnV21
Maz3e4weZnh

2. Sign a transaction

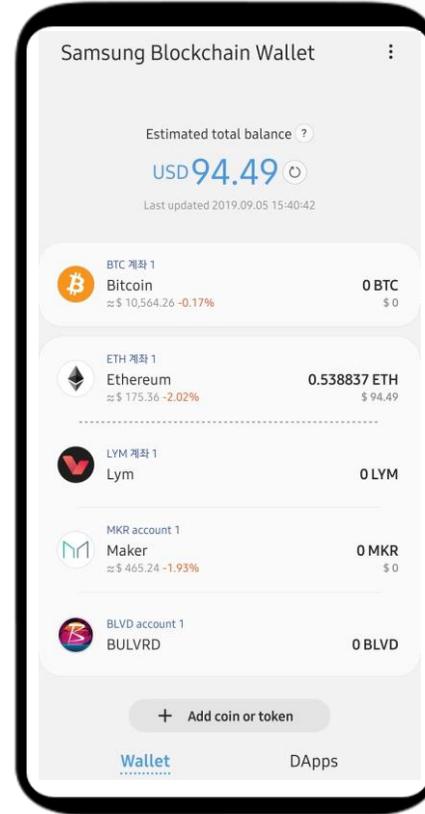
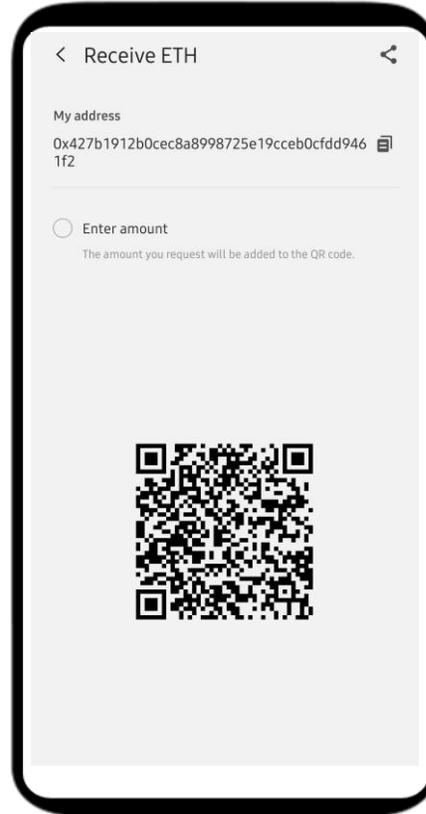
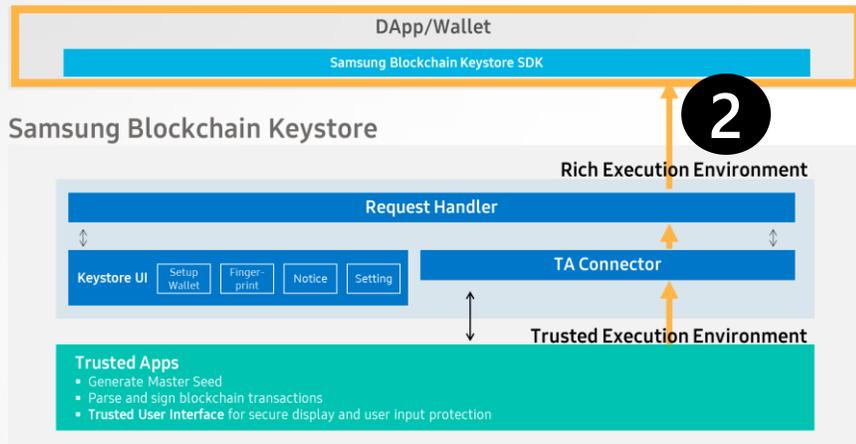


Flow 1. Get Address



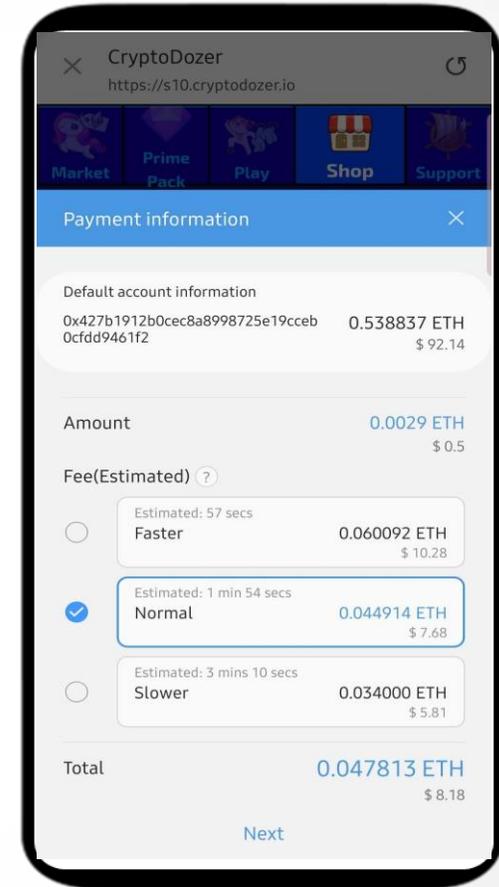
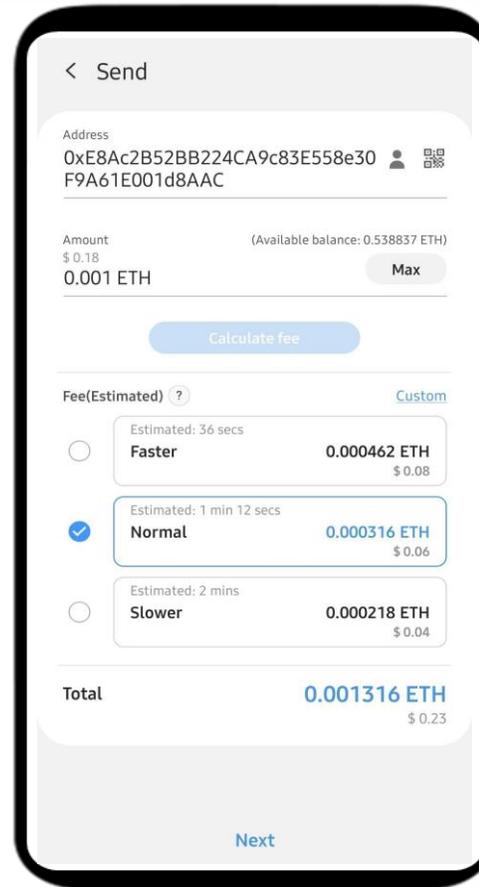
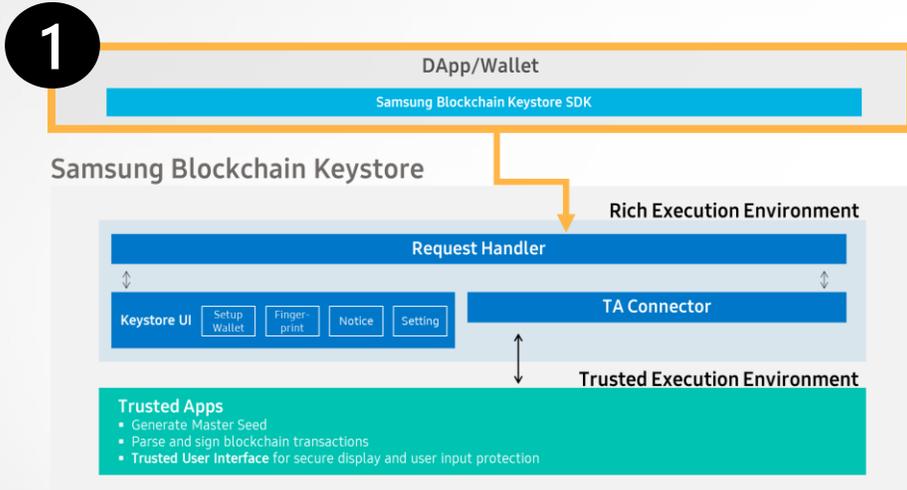
Wallet or DApp links to the Keystore by requesting the user's blockchain address

Flow 1. Get Address



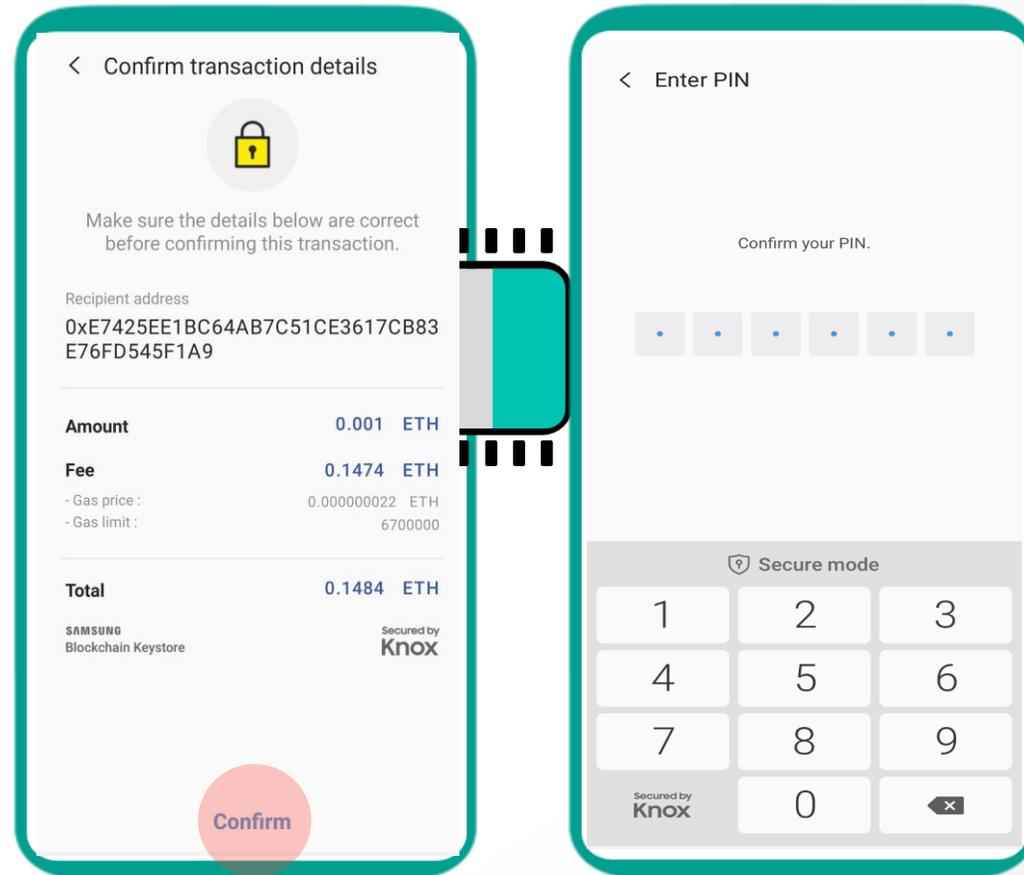
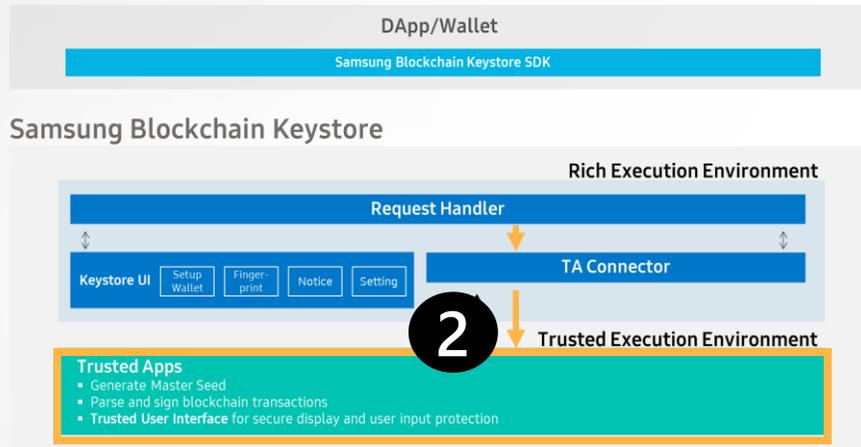
User's blockchain address is now linked to the wallet or DApp!

Flow 2. Sign a transaction



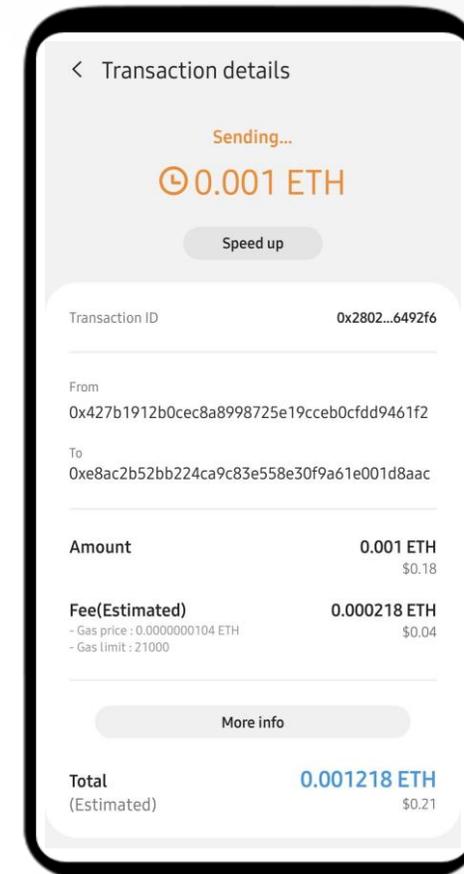
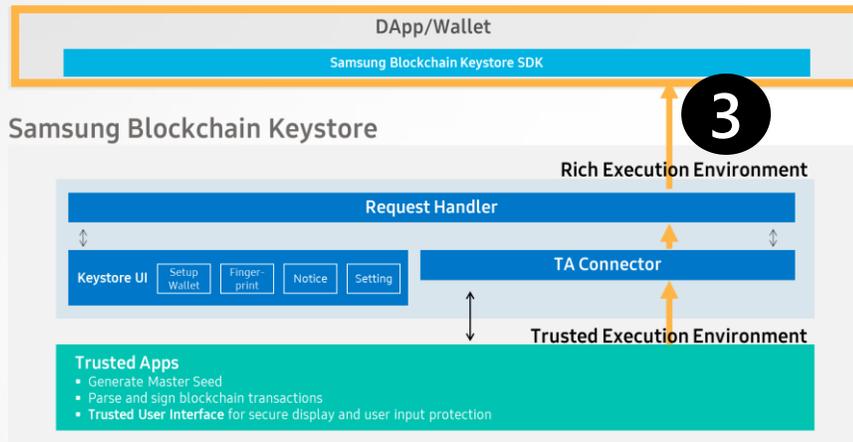
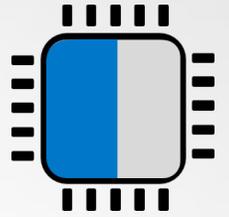
Transactions created by a wallet that integrated Samsung Blockchain Keystore SDK

Flow 2. Sign a transaction



Transaction Details > User Confirmation > Sign

Flow 2. Sign a transaction



Signed transaction is returned to the wallet
Wallet sends the transaction to blockchain network

4

Samsung Blockchain Keystore SDK

Why Keystore SDK?

Benefits from integrating Samsung Blockchain Keystore

Developers

Leverage **security features**
Free from key management!

Users

Key Ownership
Free from DApp dependency!

Mobile Apps with Keystore SDK

Games



[Crypto Fishing]



[The Onion Knights]



[Dozer Bird]

Media



[Gotchu]

Payment



[Linka]

Social Funding



[Gotchu]

+ more than 100 on development

Quick and Simple Integration Steps



Android app

Provide service with easy use of blockchain



Download SDK

Open to **public** in **Samsung Developers Site**



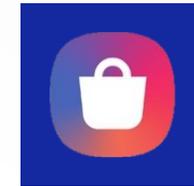
Integration

Consume Keystore SDK APIs and use Developer Mode



Add API Key

Upload your app on Developers Site to issue an API Key

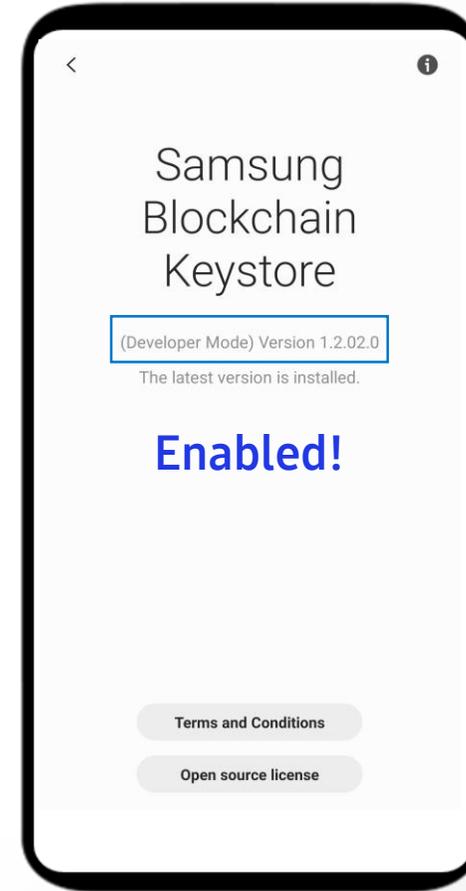
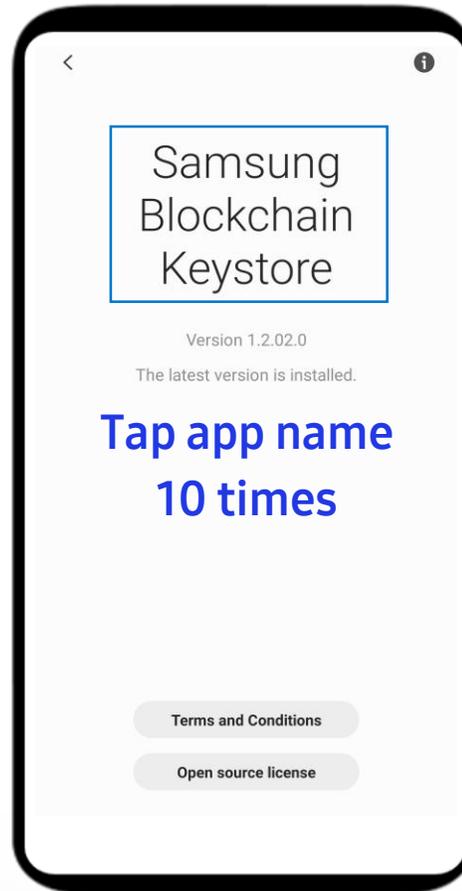
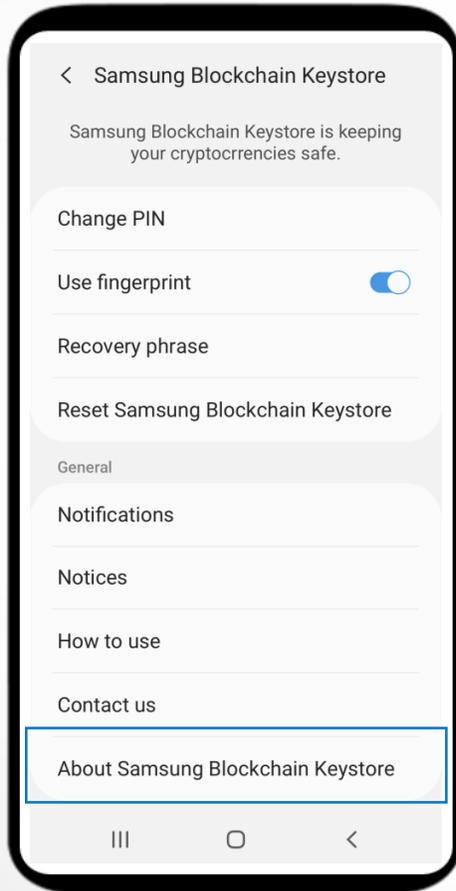


Deploy

Deploy your app in the market

Developer Mode

Enable it with just a quick tap!



Keystore currently supports...

Cryptocurrencies



Bitcoin



Ethereum



Klaytn



Tron

Devices

- Galaxy S10 series
- Galaxy Note10 series
- Galaxy Fold
- A90 5G



Countries

US

Korea

Canada

UK

Germany

Spain

Switzerland



5

What's Next

What's Next?

Easy integration, yet stronger security for blockchain app developers

- ✓ **More cryptocurrencies**
- ✓ **More devices**
- ✓ **More countries**
- ✓ **More user/developer friendly**
- ✓ **Greater security**

leverage SPU for hardware tamper-proof key storage



Find out more!

Samsung Developers

- Open to public
- Provide tech support

The screenshot shows the Samsung Developers website interface. At the top, there's a navigation bar with the Samsung Developers logo, links for News & Updates, Log in, Sign up, and a search bar. Below this is a secondary navigation bar with categories like Bixby, SmartThings, Services & APIs, Devices, Program, Community, Blog, and Events, along with social media icons for Facebook, Twitter, Instagram, YouTube, and LinkedIn.

The main content area is titled "Samsung Blockchain Keystore SDK". It features a left-hand navigation menu with options like Platform, Keystore, Understanding Keystore, Keystore SDK (selected), Essential Contents, Overview, Technical Document, FAQ, Restrictions, Cryptocurrency Specification, Programming Guide, Release Note, Request for API Key, and Apply for Partnership.

The "Essential Contents" section includes a table with the following items:

| | | |
|---------------------------------|--------------------------------|--------------------------|
| Samsung Blockchain Keystore SDK | Version : 1.2.0 Oct 29, 2019 | Download |
| API Reference (JavaDoc) | External Link | Release Note |
| Programming Guide | External Link | |

The "Overview" section contains a paragraph explaining that the Samsung Blockchain Keystore SDK allows Android apps to communicate with Samsung Blockchain Keystore. It lists the following key feature:

- **Get Blockchain address to link to the Samsung Blockchain Keystore**
Developers can link user's Blockchain address like a user's account. With the address returned from Samsung Blockchain Keystore, developers can check and show users how much cryptocurrency balance is in the account as well as view the transaction history. Samsung Blockchain Keystore supports BIP-39 compatible HD (Hierarchical Deterministic) Wallet – a standard tree structure, represented by derivation paths. Developers can use Samsung Blockchain Keystore API to enter an HD Path. Samsung Blockchain Keystore will derive the address from the public

- **sunghyuk.lee@samsung.com**
- **<https://developer.samsung.com/blockchain>**



Thank You



The graphic features the text 'Q & A' in a clean, sans-serif font. The 'Q' and 'A' are white, while the ampersand is a vibrant lime green. To the right of the text, two orange triangles point towards a large, dark blue circle on the far right. The background is a dark blue gradient with a pattern of lighter blue circles on the left side.

Q & A

Partner Disrupt Foresee