

Partner



Foresee

Techtonic 2019

Disrupt

2019.11.14 • SAMSUNG SDS Tower B1F Magellan Hall / Pascal Hall

삼성 블록체인 키스토어 당신의 블록체인 어플리케이션은 안전한가요? 이성혁 프로 (블록체인서비스그룹) / 삼성전자 무선사업부

Track 3 | Blockchain

it all happened because of

private key

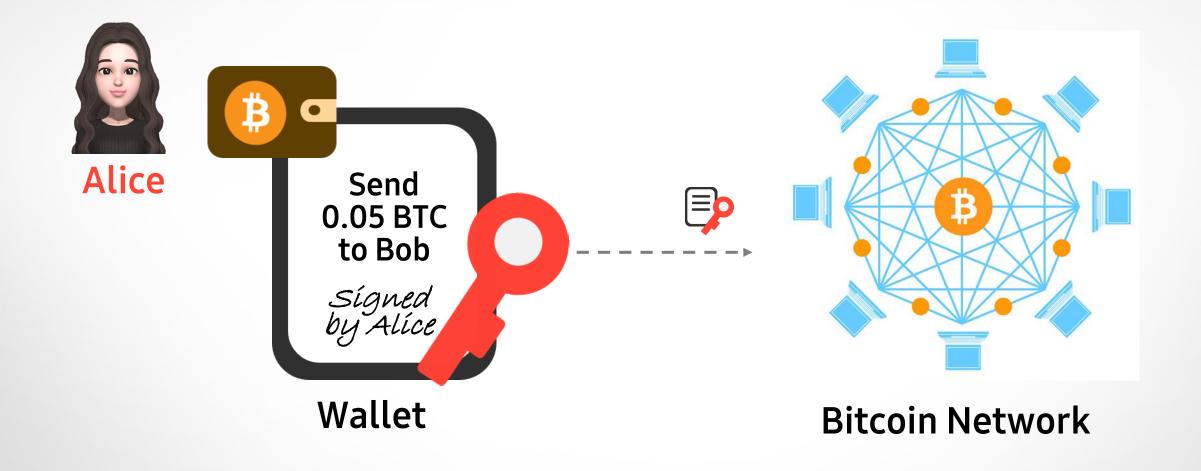
What is a private key?



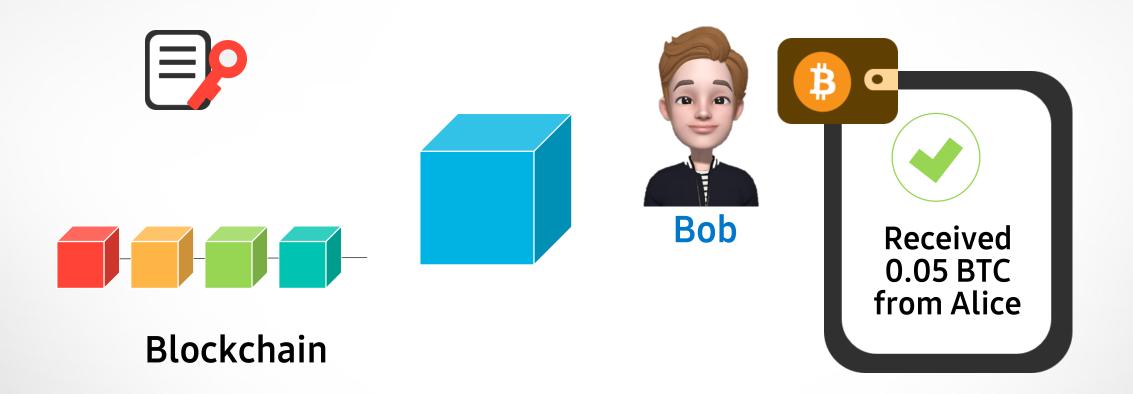
Alice

Bob

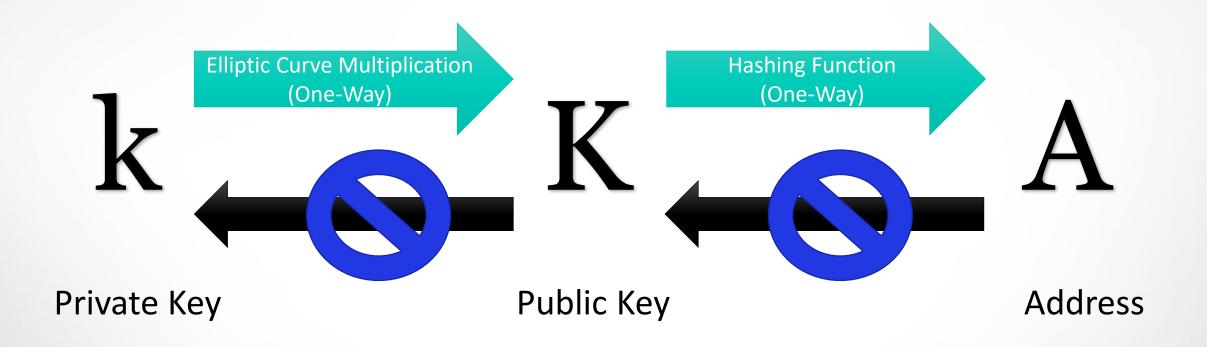
What is a private key?



What is a private key?



Blockchain address



Who creates account ?

Financial institutions issue accounts



Bank

620-179283-842

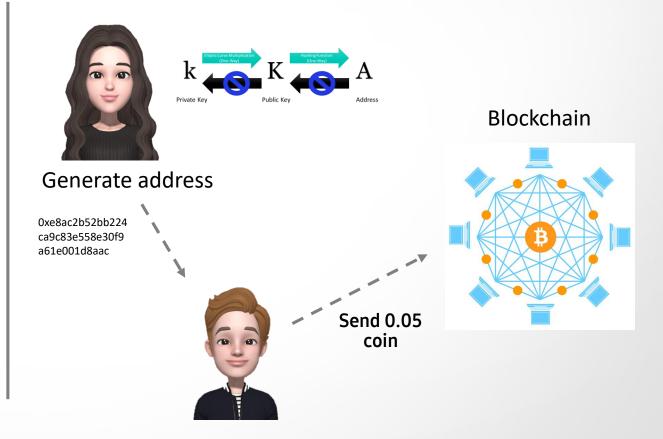
Open account

_ _ _ _ _ _ _ _ _ _ _



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



Paper Wallet

Hardware Wallet

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

What is a "Good" Wallet?

1

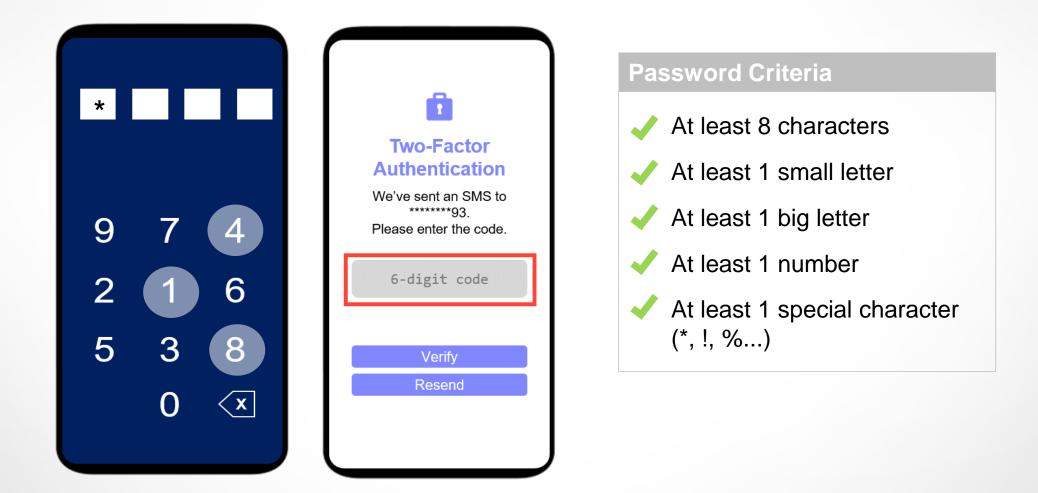
Inevitable security vulnerabilities

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



Workaround to avoid hacking

Becoming more and more complicated



Security Solutions

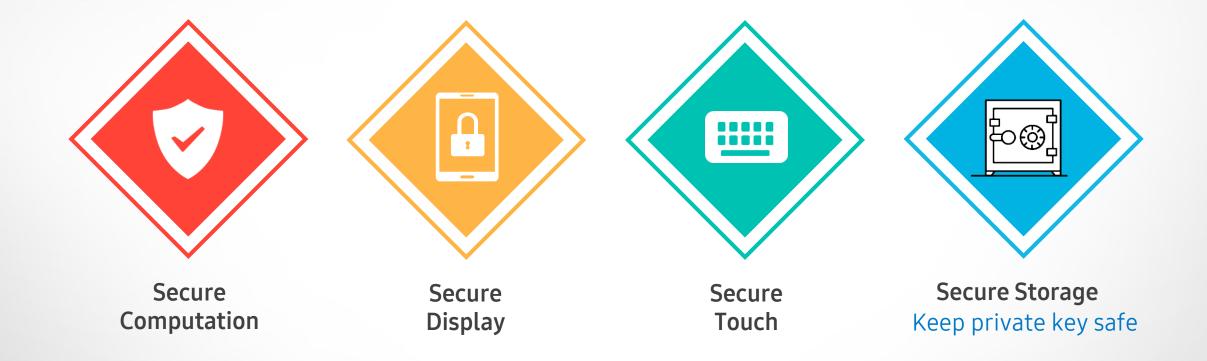
- Application Integrity
- Device Integrity





Then what is a "Good" wallet?

Security considerations when developing Samsung Blockchain Keystore



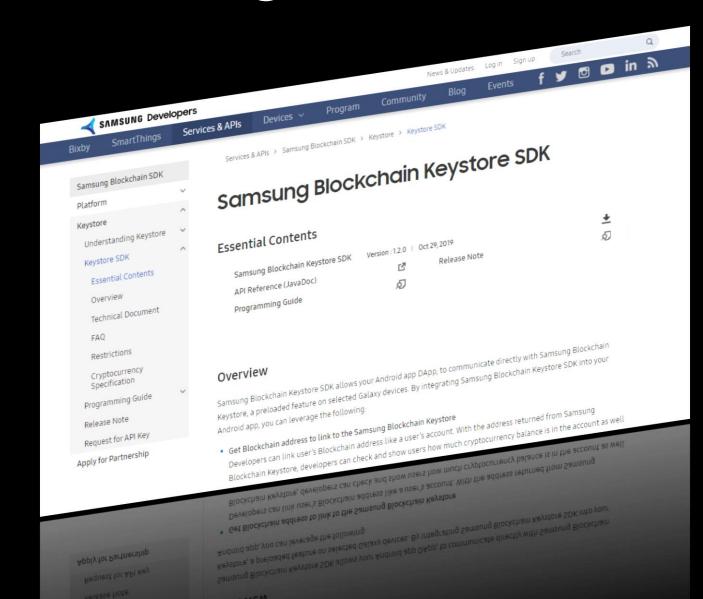


Introduction to Samsung Blockchain Keystore

launched earlier this year to keep your private key safe

We	elcome to	C		ockchain Keysto cryptocrrencies	
Samsu	ng Block		Change PIN		
Samsung Block	Ceystore chain Keystore is ace for your crypt		Use fingerpri	nt	
	nore about the ser		Recovery phr	ase	
			Reset Samsu	ing Blockchai	in Keystore
			General		
			Notifications		
			Notices		
-			How to use		
	ue, read and agree onditions and Priva		Contact us		
	Agree		About Samsu	ung Blockcha	in Keystore
	Ο	<		Ο	<
ш	0	<		0	<
			About Samsu	ing Blockcha	in Keystore

< Samsung Blockchain Keystore



Open to public on Samsung Developers

key generator?

Android keystore?

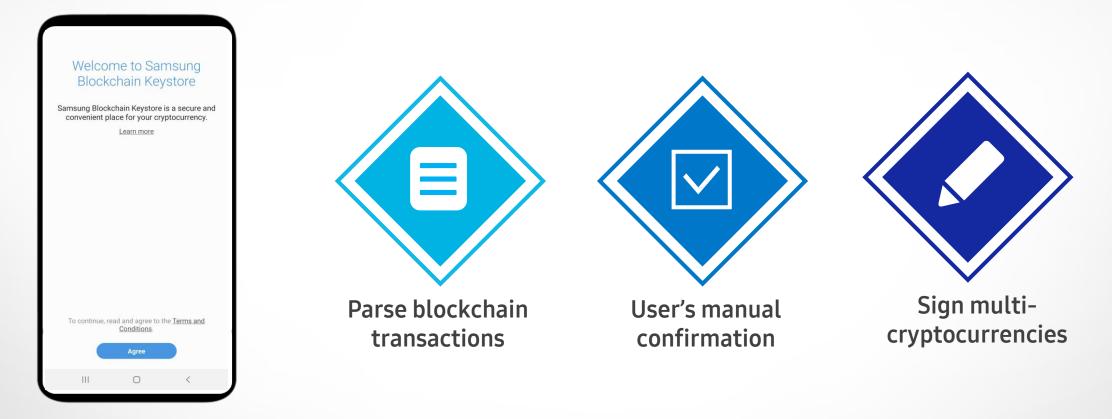
storage? **SAMSUNG** signatures?

??





a blockchain-dedicated Keystore launched earlier this year



Where can I find it?

Device Settings > Biometrics and Security > Samsung Blockchain Keystore

	Settings	Biometrics and security
		< ٩
	ά 😝	Face recognition Register your face.
([1-	Connections Wi-Fi, Bluetooth, Data usage, Airplane mode	Fingerprints Add your fingerprints.
	Sounds and vibration Sound mode, Ringtone, Volume	Biometrics preferences
•	Notifications Block, allow, prioritize	Security Google Play Protect Apps scanned at 1:07 AM
۲	Display Brightness, Blue light filter, Home screen	Find My Mobile Locate and control your phone remotely if it's lost or if you forget your unlock method.
۳	Wallpapers and themes Wallpapers, Themes, Icons	Security update July 1, 2019
	Lock screen Screen lock type, Always On Display, Clock style	Samsung Pass Use biometric authentication to verify your identity easily and securely.
•	Biometrics and security Face recognition, Fingerprints, Privacy	Samsung Blockchain Keystore Secure and manage your blockchain private key.
ø	Accounts and backup Samsung Cloud, Smart Switch	Install unknown apps

Main Features (1) Key Management

Create a Wallet



< Create wallet	< New re
Samsung Blockchain Keystore will create a 12-word recovery phrase to secure your wallet. You can use this phrase to recover your wallet on other devices or software.	Anyone who ha able to access cryptocurrency it in a safe plac cloud, website, 1. settl 3. horn 5. arch 7. pipe
Keep in mind:	9. flag
 Your wallet is stored anonymously on the blockchain network. This means that Samsung doesn't have access to your data. 	11. sque
 The recovery phrase is the only way to access your wallet, so make sure not to lose it and to keep it a secret. 	
 If you lose your recovery phrase, it will be impossible to access your account. 	
 If anyone else learns your recovery phrase, they'll be able to steal the contents of your wallet. 	
	SAMSUNG Blockchain Keysto
Next	I w

ecovery phrase

as this recovery phrase will be your wallet and steal all of your . Write down the phrase and keep ce. Storing the phrase online (email, etc.) is not recommended.

1. settle	2. jeans
3. horn	4. group
5. arch	6. build
7. pipe	8. total
9. flag	10. prevent
11. squeeze	12. before

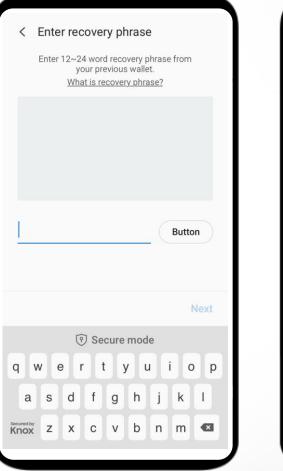
Secured by Knox

vrote it down safely

Main Features (1) Key Management

Import a Wallet

e.	Ente
€_	
	r.
	q w
	a s



< Recovery phrase
A recovery phrase, also known as a seed phrase or backup phrase, allows you to recover a wallet from the blockchain network. To import your previous wallet into Samsung Blockchain Keystore, you need to enter the 12 - 24 word recovery phrase that was given to you when you created the wallet.

Keep in mind:

- · Your wallet is stored anonymously on the blockchain network. This means that Samsung doesn't have access to your data.
- · The recovery phrase is the only way to access your wallet, so make sure not to lose it and to keep it a secret.
- · If you lose your recovery phrase, it will be impossible to access your account.
- · If anyone else learns your recovery phrase, they'll be able to steal the contents of your wallet

Got it

Main Features (2) Sign a transaction

< Confirm trans	saction details			
	F			
	ails below are cor ng this transactior			
Recipient address mzrJwjneuUBgDjl U1BYF	HAPEb1bB8Wps	ngU		
Amount	0.001	втс		
Fee	0.00001	BTC		
Total	0.00101	BTC		
SAMSUNG Blockchain Keystore		ecured by		
				ŝ
Co	onfirm		J	

ť		
Make sure the deta		
before confirmin	ng this transaction	
Recipient address		2000
)xE7425EE1BC64A E76FD545F1A9	AB7C51CE36170	CB83
Amount	0.001	ETH
	0.001 0.1474	
Amount Fee - Gas price : - Gas limit :	0.1474 0.00000022	ЕТН
Fee Gas price :	0.1474 0.00000022	ETH 2 ETH 700000
Fee Gas price : Gas limit : Total	0.1474 0.000000022 67 0.1484 se	ETH 2 ETH 700000 ETH
Fee Gas price : Gas limit : Fotal	0.1474 0.000000022 67 0.1484 se	ETH 2 ETH 700000 ETH
Fee Gas price : Gas limit : Fotal	0.1474 0.000000022 67 0.1484 se	ETH 2 ETH 700000 ETH

Main Features

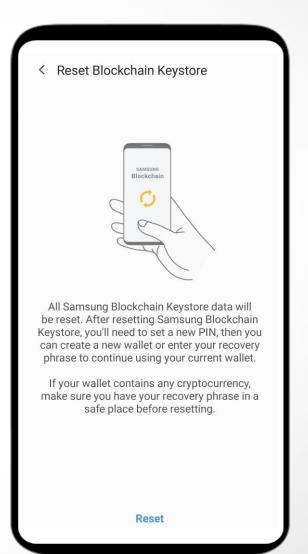
(3) Manage Authentication

Authentication is needed to confirm a transaction

(DIN		
	< Register Set a PIN to p	rotect your cryptoc	eurrency keys.	Keingerprint Verification
				Scan your fingerprint to use it to protect your cryptocurrency keys.
	τ	গ্ Secure mode	•	Skip and use PIN
	1	2	3	
	4	5	6	
	7	8	9	Verify with fingerprint
	Secured by Knox	0		

Main Features (4) Manage Settings

< Samsung Blockchain Keystore
Samsung Blockchain Keystore is keeping your cryptocrrencies safe.
Change PIN
Use fingerprint
Recovery phrase
Reset Samsung Blockchain Keystore
General
Notifications
Notices
How to use
Contact us
About Samsung Blockchain Keystore





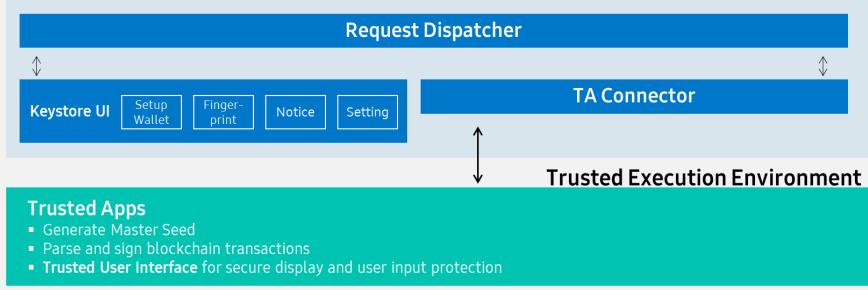
What Makes Keystore Secure and Unique

Architecture



Samsung Blockchain Keystore

Rich Execution Environment



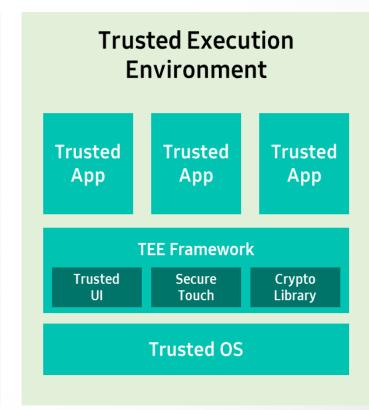
SAMSUNG KNOX Hardware Root of Trust



Secure Computation Trusted Execution Environment

Rich OS Trusted OS

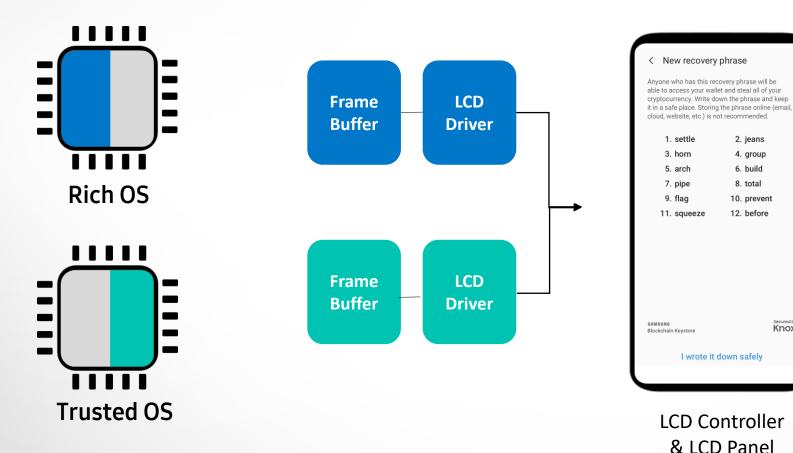
Rich Execution Environment App App App Android Framework **Rich OS**





Secure Display

Trusted User Interface



2. jeans 4. group 6. build 8. total 10. prevent 12. before

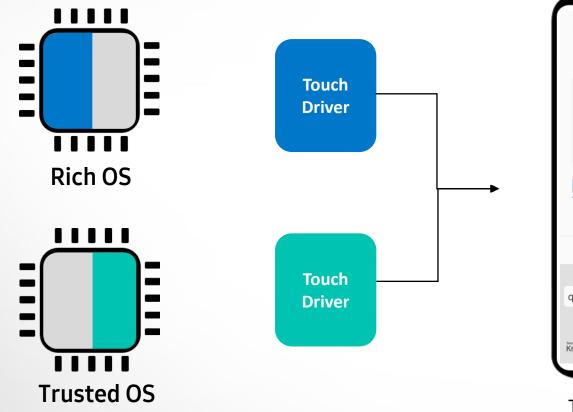
Knox

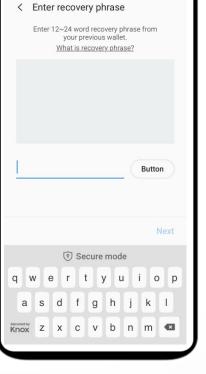
No screen capture!



Secure Touch

Trusted User Interface





No touch hooking!

Touch Screen Panel



Secure Storage

Hardware-based encryption





encrypted and safely stored

Secure your app with Keystore

Two main service flows of Keystore integration

1. Get Blockchain Address



0xe8ac2b52bb224ca9c83e55 8e30f9a61e001d8aac

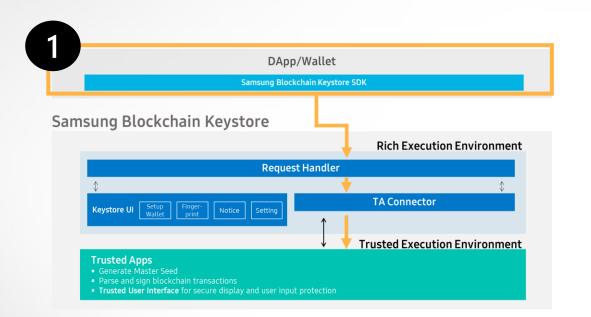


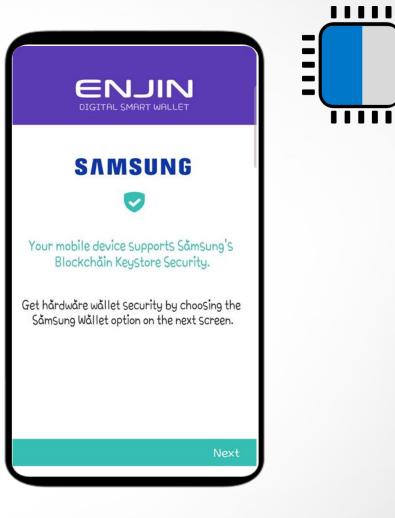
1F7FAt5kW55W9g7C2utnV21 Maz3e4weZnh

2. Sign a transaction



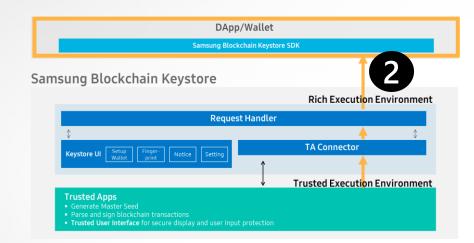
Flow 1. Get Address

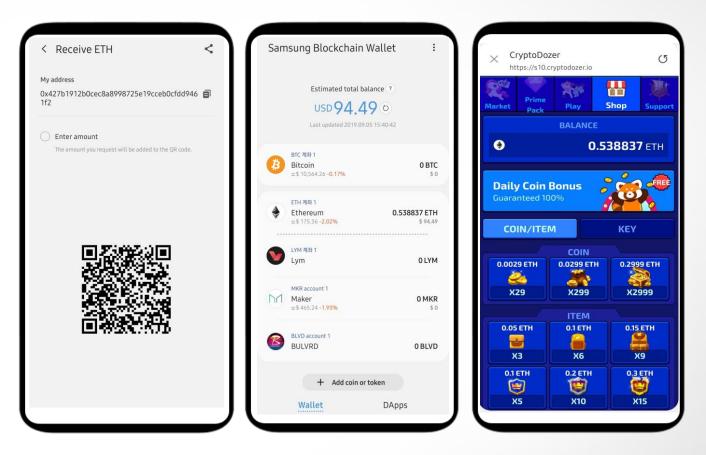




Wallet or DApp links to the Keystore by requesting the user's blockchain address

Flow 1. Get Address





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

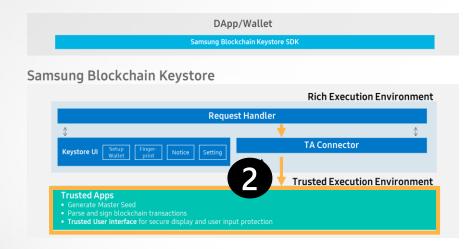
Flow 2. Sign a transaction

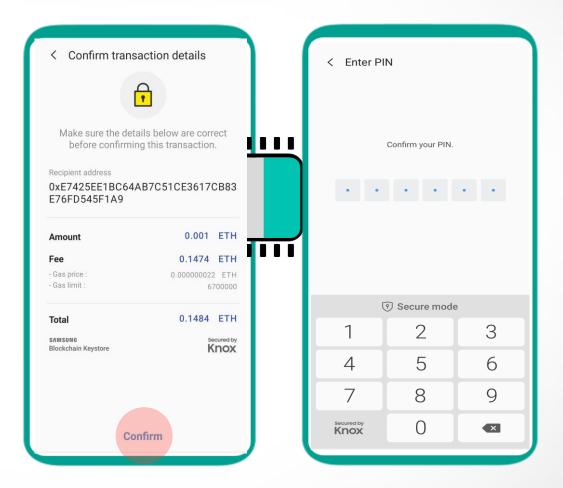
DApp	/Wallet			
Samsung Blocke	chain Keystore SDK			
amsung Blockchain Keystore				
	Rich Execution Environment			
Request	t Handler			
\$	\$			
Keystore UI Setup Finger- Notice Setting	TA Connector			
Wallet print Notice Secting	1			
	Trusted Execution Environment			
Trusted Apps Generate Master Seed Parse and sign blockchain transactions Trusted User Interface for secure display and user input	protection			

0xE8Ac2B5 F9A61E001		33E558e30 💄 🔡	Mark		Shop Suppor
Amount		able balance: 0.538837 ETH)	Pay	ment information	×
0.001 ETH		Max	Defa	ult account information	
				27b1912b0cec8a8998725e19cce d9461f2	0.538837 ETH \$ 92.14
ee(Estimated)	?	Custom			
C Estimation Faster	ated: 36 secs P	0.000462 ETH \$ 0.08		ount (Estimated) ?	0.0029 ETH \$ 0.5
Section Norm	ated: 1 min 12 secs nal	0.000316 ETH \$ 0.06	0	Estimated: 57 secs Faster	0.060092 ETH \$ 10.28
-	ated: 2 mins er	0.000218 ETH \$ 0.04	0	Estimated: 1 min 54 secs Normal	0.044914 ETH \$ 7.68
Slow		0.001316 ETH	0	Estimated: 3 mins 10 secs Slower	0.034000 ETH \$ 5.81
Slow		\$ 0.23			

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 DApp/Wallet < Transaction details Wallet Sending... 3 Samsung Blockchain Keystore O 0.001 ETH Rich Execution Environment Speed up **Request Handler** Signed tx **TA Connector** Finger-print Notice Transaction ID 0x2802...6492f6 Received **Trusted Execution Environment** From Trusted Apps 0x427b1912b0cec8a8998725e19cceb0cfdd9461f2 0xf86c4085051f4d5c0083663be To Frusted User Interface for secure display and user input protection 094e8ac2b52bb224ca9c83e558e 0xe8ac2b52bb224ca9c83e558e30f9a61e001d8aac 30f9a61e001d8aac87038d7ea4c 68000801ca04885df148ea1b02d 0.001 ETH Amount 6b0478dd4a48556a171521f9cd1 \$0.18 fbc17e67e8d0073208ac0a04fc0 Fee(Estimated) 0.000218 ETH 863a01feaa56b05823784f7f8d5 - Gas price : 0.0000000104 ETH \$0.04 Gas limit : 21000 dc37ab41ab123cb1fbf2423a582 6e27ec More info Total 0.001218 ETH (Estimated) \$0.21

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



Samsung Blockchain Keystore SDK

Why Keystore SDK?

Benefits from integrating Samsung Blockchain Keystore



Developers

Key Ownership Free from DApp dependency!

Users

Mobile Apps with Keystore SDK

Games



[Crypto Fishing]



[The Onion Knights]



[Dozer Bird]

Media



Payment



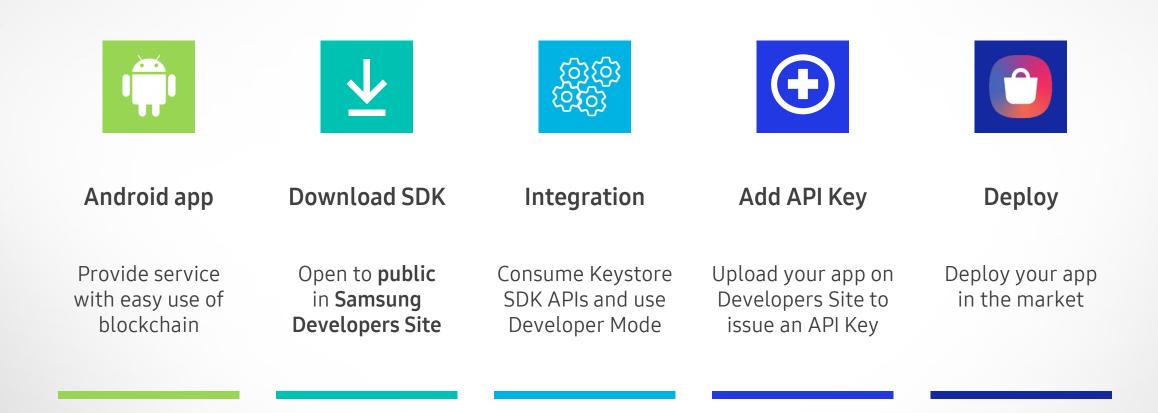


Social Funding

포스팅		후원거리		정보
	-			-
매수수량		가격		애도수량
1.200	1		800	3
			900	5
			1,000	5
수량				0
가격				0
도 가능 수량				0 CHU
1래 가능 금액				0 캐수
주운금액				0 캐수
OH	E		•	I÷
내 주	문내역		실시긴	체결

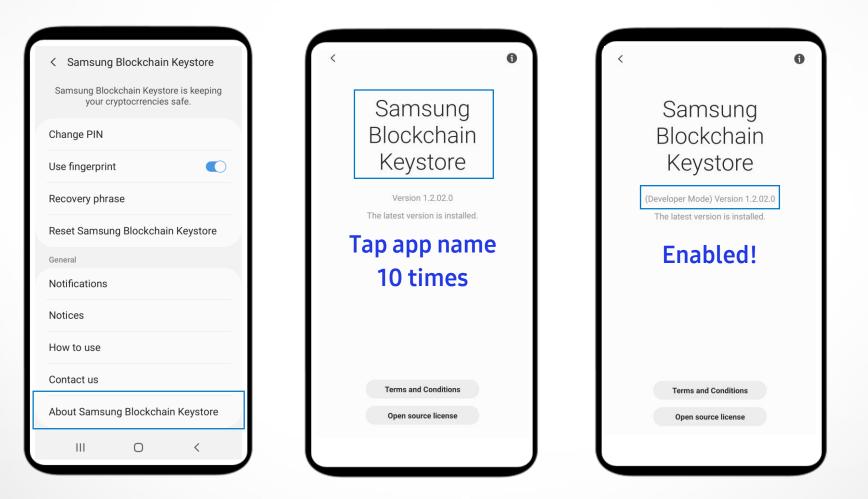
+ more than 100 on development

Quick and Simple Integration Steps



Developer Mode

Enable it with just a quick tap!



Keystore currently supports...

Cryptocurrencies **Devices Countries** Galaxy S10 series UK US Bitcoin Galaxy Note10 series Germany Korea Spain Galaxy Fold Ethereum Canada Switzerland • A90 5G Klaytn Tron SAMSUNG



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

d sv	MSUNG Devel	opers				١	lews & Updates	Log in Sign	up Sea	irch		
Bixby	SmartThings	Service	es & APIs	Devices \vee	Program	Community	Blog	Events	f ¥	đ	D	in
Samsung l	Blockchain SDK		Services	& APIs > Samsung Bl	ockchain SDK > I	Keystore > Keystor	e SDK					
Platform		\sim										
Keystore		^	Samsung Blocka			chain Keystore SDK						
Underst	anding Keystore	\sim		•								
Keystore	e SDK	\sim	Essent	ial Contents								
Essen	tial Contents											. 1
Overv	iew		Sams	ung Blockchain Key	vstore SDK V	/ersion : 1.2.0 Oct	29, 2019				<u>+</u>	
Techn	ical Document		API R	eference (JavaDoc)		ß	Release Not	te			ĺ,	
FAQ			Progr	amming Guide		ହ						
Restri	ctions											
	ocurrency fication											
Program	nming Guide	\sim	Overvi	ew								
Release	Note		Samsung Blockchain Keystore SDK allows your Android app DApp, to communicate directly with Samsung Blockchain									
Request	for API Key		Keystore, a preloaded feature on selected Galaxy devices. By integrating Samsung Blockchain Keystore SDK into your									
Apply for F	Partnership		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 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 								u	

Blockchain Keystore API to enter an HD Path. Samsung Blockchain Keystore will derive the address from the public

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

Thank You



Partner Disrupt Foresee