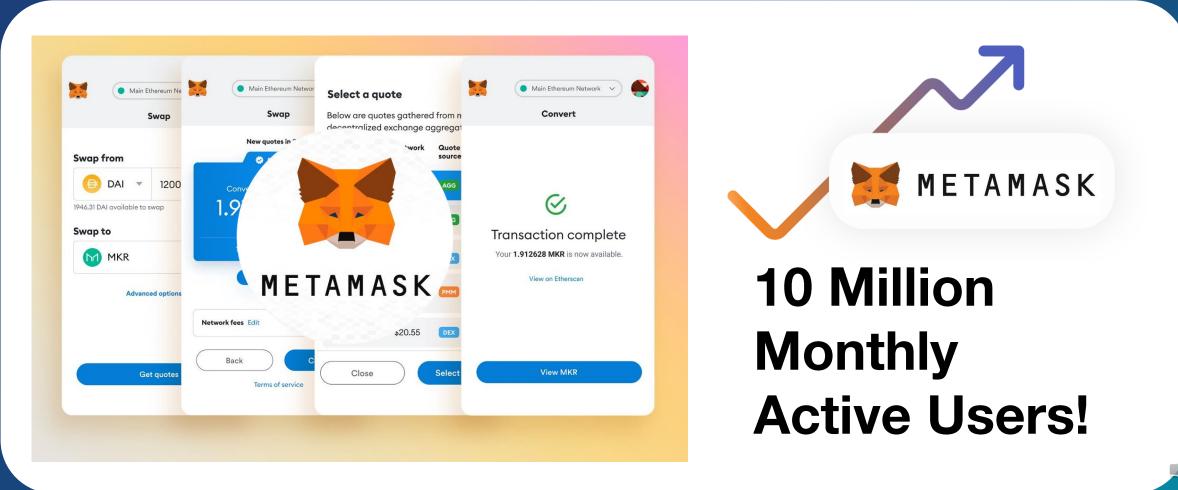
Threshold Signature Wallet for Klaytn

Klaytn Improvement Reserve Proposal October 2021



Background: Blockchain is Changing the World

People Have High Expectations for Blockchain Apps, Evidenced by Metamask



Wallet is Essential for Klaytn Ecosystem

Klaytn ecosystem is growing rapidly. Wallet is essential for Klatyn Ecosystem.

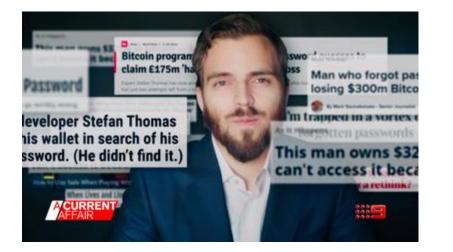


Finance

Metaverse

Two Security Problems of Wallets

User may forget the password of the wallet



A programmer living in San Francisco forgot the password to his Bitcoin wallet.

The wallet may be stolen by attackers

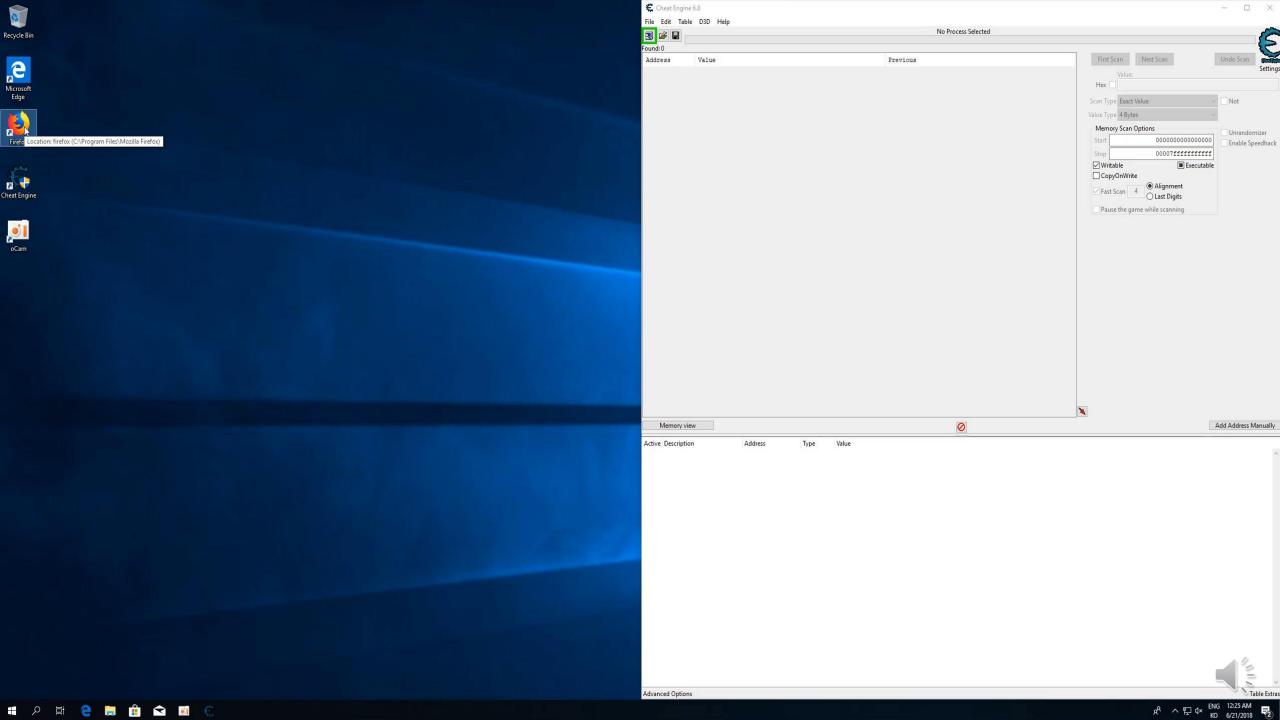


People prefer browser-based wallet for convenience, but the browser wallet may be vulnerable to hacking.

000

Demonstration of Metamask Hacking Extracting seed words from a brow<u>ser wallet</u>





@ 세업	×	× str							🔆 Cheat Engin								
→ C' û		Q. Google로 검색하거나 주소 입력				III\ 🗊 🛎	E File Edit Tab	able D3D Help 0000121C-firefox.eve									
;	 G 웹 검색 ① 다른 브라우저에 값 상위 사이트 ↓ 	에 있는 북마크, 기록, 비밀번호를 사용해 Fil ,	refox를 이용해 보세요.			괜찮습니	→ 또 지금 가져오기	*	Found: 5 Addreas ID6A8B3DD1E ID6A8C37A48 ID6B1ACA4E8 ID6B652BD08	Value seedWords seedWords seedWords seedWords seedWords	-	Previous			Scan Typ Value Typ	Scan Next Scan Value: seedWords be Search for text e String ny Scan Options	Undo Scan Sc Codepage UTF-16 Case sensitive
	ر google ک فاواکاو⊑ ×	addons.mozilla youtube	C Memory Viewer File Search View Debu Address Bytes irrefox.exe+5/48 83 EC 28 irrefox.exe+5/48 83 C4 28 irrefox.exe+5/186 6AFEFFFF	Opcode sub call add		Comment 40 40			firefox.exe+5C30					- [Stor	000000000000000000000000000000000000000	OODOO ☐ Enable Speed cutable
		seedW	lord:	5		.R	•••	•••	in	stall	l vin	tual	i	nno	cen	t	
	METAMASK MetaMask MetaMask - bri	and the second se	ter	ce.	real	. r	unw	ay :	r <mark>ed</mark> j	ycle	stee	l bo	on <mark>e</mark>	50	und		
	browser.	local	LORDCOTDOD OF OD U	0 00 00 00 00 0	FO 00 00 00 00 01		00 00 10 00 00 00	• •		Eura(11 00 00 00 01 00 FF	E UK	vall	UA	• •		
	○ 방문한 사이!		DeADCe7Be8 00 0 LDeADCe7Be8 30 22 2 DeADCe7Be8 32 31 33 LDeADCe7C28 61 30 3 DeADCe7C88 30 78 3 DeADCe7C88 32 34 36 LDEADCe7C88 32 34 36 LDEADCe7C82 22 3 LDEADCe7C82 22 3 LDEADCe7C82 34 30 3 LDEADCe7D48 34 30 3 LDEADCe7D48 34 30 3 LDEADCe7D48 34 30 3	00 00 13 00 FF F C 22 30 78 32 3 18 37 31 31 61 3 3 10 22 22 30 7 31 61 30 61 30 62 30 7 31 61 30 61 30 62 33 34 32 36 30 32 33 30 7 37 33 30 73 33 30 73 33 30 73 33 33 30 62 32 23 31 34 32 36 31 22 34 33 30 73 33 30 61 31 22 33 34 33 30 61 31 22 35 30 61 31 22 31 33 30 33 30 34 33 30 31	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00 FF FF 00 0 30 30 22 2C 3 78 32 31 38 2 22 30 78 31 3 32 38 30 30 2 37 64 63 34 3 2C 22 30 78 3 4 30 30 22 2 62 39 61 63 6	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00 00 00 00 00 30 22 2C 22 30 31 38 37 31 30 30 30 22 2C 30 78 31 36 35 30 30 32 22 2C 33 35 39 34 30 30 78 37 37 33 30 78 37 37 33 30 22 22 23 34	0 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00	0x218711a00" 11a00", "0x21 ,"0x1dcd6500 5a0bc00","0x ,"0xee6b2800 b80","0x7735 7359400","0x "0x4190ab00" 64","0x3b9ac	,"0x21871 ","0x218711a00"," 18711a00","0x2187 00","0x185640200" x165a0bc00","0xet 0","0xb65f480"," 59400","0x773594 ","0x77359400","0x77 ","0x4190ab00","0 a644","0x3b9aca0	"0x 711 "," e6b "0x 00" 359 0x3 0x3 0",		Add Address Mar
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	LD6ADC87DA8 30 30 2 LD6ADC87DD8 39 61 6 LD6ADC87E08 30 78 3 LD6ADC87E08 30 22 2 LD6ADC87E68 61 63 6 LD6ADC87E68 61 63 6 LD6ADC87EC8 22 22 2 LD6ADC87EC8 64 35 6 LD6ADC87E28 64 36 3	12 2C 22 30 78 3 33 61 30 30 22 2 33 62 39 61 63 6 61 30 30 22 2 3 61 30 30 22 2 3 61 30 30 22 2 2 61 30 30 22 2 2 62 30 78 33 61 3 62 30 78 33 62 3 62 30 78 33 62 3 62 30 78 33 62 3 63 65 35 38 6 3 3 61 37 37 37 3 3 3	33 62 39 61 63 61 C 22 30 78 33 62 61 30 30 22 22 22 22 62 39 61 63 61 30 22 32 30 78 33 62 39 30 22 39 30 30 32 39 30	30 30 22 22 2 39 61 63 61 3 30 78 33 62 3 30 22 22 22 3 61 63 61 30 3 78 33 62 3 4 78 33 62 3 4 72 22 62 24 3 33 31 32 64 3	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	0 61 63 61 30 30 0 78 33 62 39 61 0 22 22 22 30 78 63 61 30 30 30 22 3 36 23 30 30 30 2 2 23 37 61 63 3 62 39 61 63 33 2 2 23 78 33 33 40 30 30 30 30 30 2 2 22 30 78 33 61 30 30 22 50 33 61 23 32 35 61 37 7 61 73 4C 65 60	22 2C 22 30 78 63 61 30 30 22 33 62 39 61 63 2C 22 30 78 33 61 30 30 22 20 62 39 61 63 61 7D 2C 7B 22 24 7B 36 30 22 2C 62 39 61 63 61 7D 2C 7B 22 64 78 36 35 37 34 69 74 22 3A 22	3 61 30 20 22 22 3 62 39 61 63 61 30 3 62 39 61 63 61 30 32 2 23 78 33 62 39 61 30 32 2 39 61 63 61 30 32 23 61 30 32 2 39 61 63 63 35 37 63 62 39 61 60 63 75 60 66 63 75 60 66 64 75 76 75 64 65 60 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	<pre>2 00","0x3b9cca00","(2 9aca00","0x3b9aca00","(10 0x3b9aca00","0x3b9aca00","0x19aca00","0x3b9aca00","0x3b9aca00","0x3b9aca00","0x3b9aca00","0x1 2 0x3b9aca00","0x1 2 0x1 2</pre>	0x3b9aca00", 0","0x3b9aca aca00","0x3b x3b9aca00"," ","0x3b9aca0 ca00","0x3b9 3b9aca00"]}, raData":"0x6 2","gasLimit	"0x3b9aca00","0: a00","0x3b9aca00 b9aca00","0x3b9ac 0x3b9aca00","0x3b9ac 00","0x3b9aca00","0x 9aca00","0x3b9ac 57468657266966 557468657266966 t":"0x7a121d","g	x3b "," ca0 3b9 ,"0 a00 0xb 652 asU		
		♥ 나만의 브라우징을 나만의 것으로 하고 싶은 것	하세요. 번이 있으세요? 추적 방지와 ⁻	함께 사생활 보호 모드	를 사용해 보세요.	자세히 보기		×	Advanced Option						-0	다. ¹ 4	

We Need to Protect the Private Key

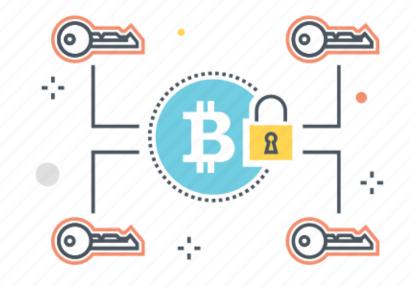
1. Use a H/W wallet

- + The private key never exposed
- You must carry the device with you



2. Use a Multi-signature wallet

- + Having safeguard features (key recovery)
- Additional fees required
- Not all blockchain supports MultiSig

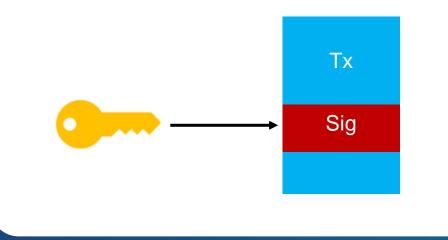


Comparison Between SingleSig and MultiSig

MultiSig is More Secure than SingleSig, But It is Inefficient

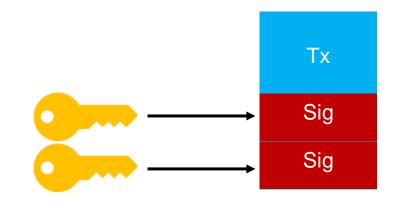
SingleSig

 An account depends on single private key



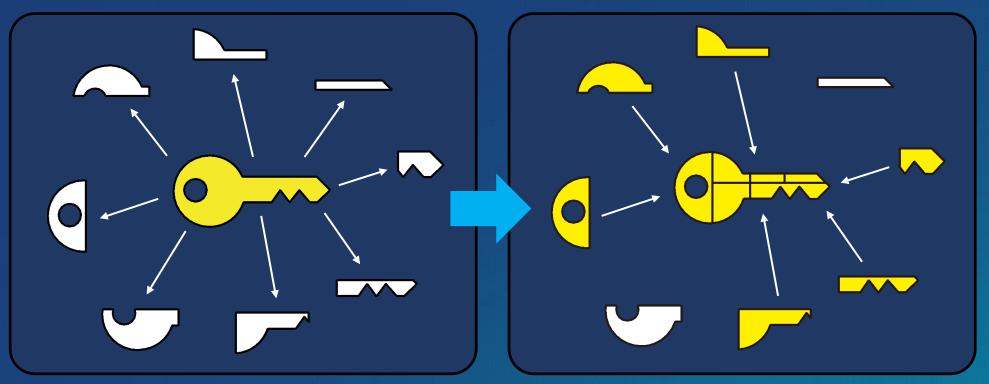
MultiSig

- t-of-n approval security
- Requires platform support
- Higher transaction fees





Threshold Signature is Superior to MultiSig



- ✓ Distributed key generation and signing
- ✓ No one has the private key
- ✓ Supports t of n key shares
- Compatible with any blockchain network

Threshold Signature Scheme: High Compatibility, and Low Transaction Fees

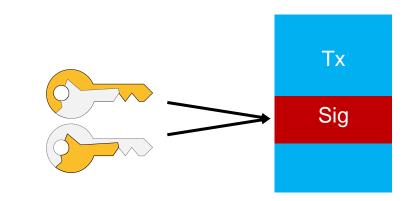
MultiSig

- t-of-n approval security
- Requires platform support
- Higher transaction fees



ThresholdSig

- t-of-n approval security
- Platform-independent
- Low transaction fees as singlesig



Our Solution: Threshold Signature Wallet

TSS wallet: A "Keyless" solution

SATISFIES SECURITY, EFFICIENCY, USABILITY



Private key never revealed



No additional transaction fee incurs



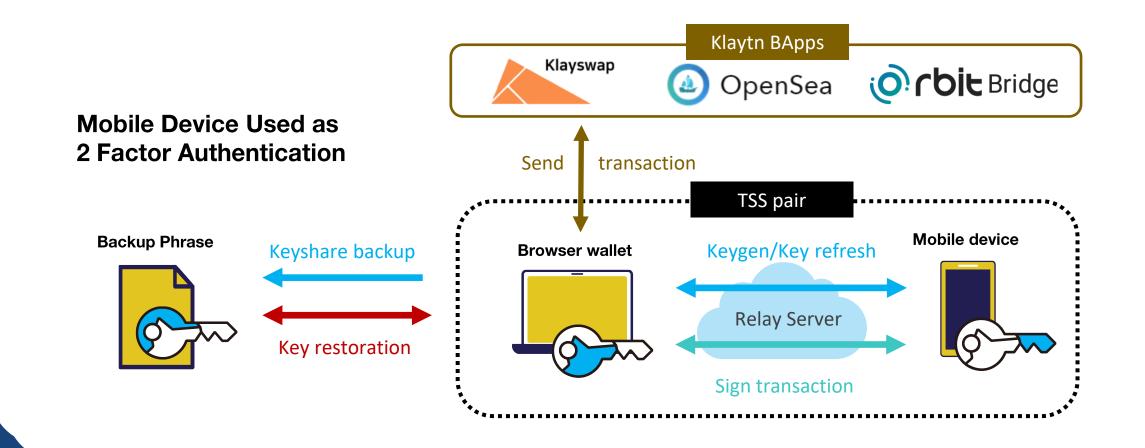


Compatible with all blockchain networks

No additional H/W device required

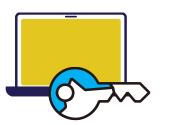


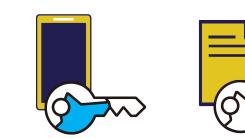
PC and Mobile Device Co-work for Keygen and Sign



TSS wallet Design Choice

2-of-3 Key Shares





Browser extension

Mobile device

Backup phrase

- Three different key shares are generated
- Two distinct shares are used for sign transactions

Advantages of our design choice



Provides two-factor authentication method



Privacy-preserved key recovery



OK even if part of device lost or stolen



No additional fees for key recovery



Browser extension

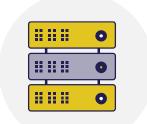
- Initiate TSS keygen and sign
- Create a backup phrase

Components of TSS Wallet



Mobile device app

• Participate in TSS keygen and signing transactions

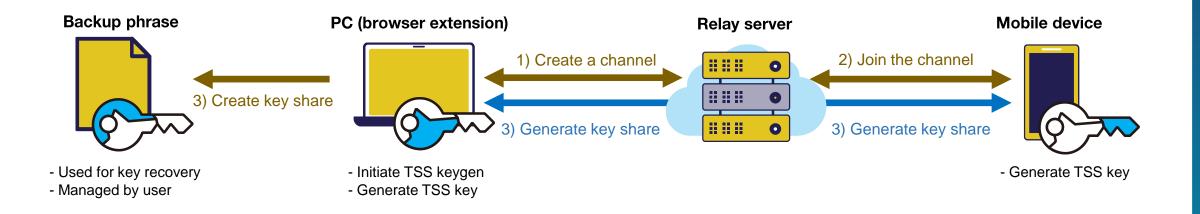


Relay server

• Create a secure channel between two entities

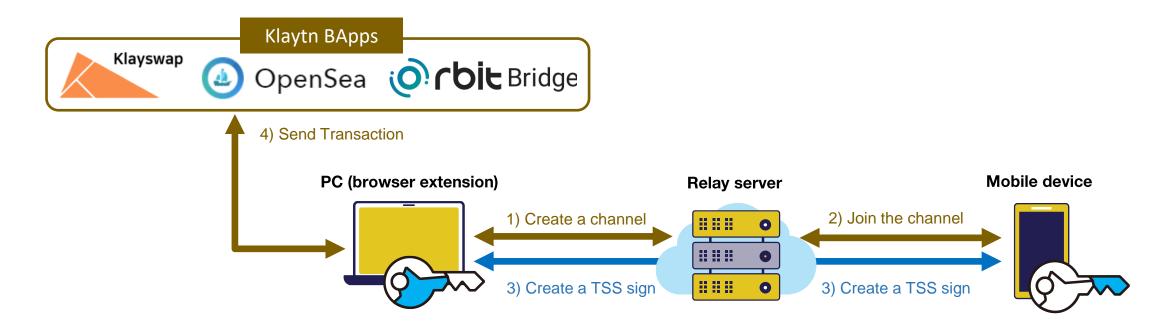


TSS Key Generation example





TSS Sign Example





Features of TSS wallet

Comparison With Existing Wallets

Security Features

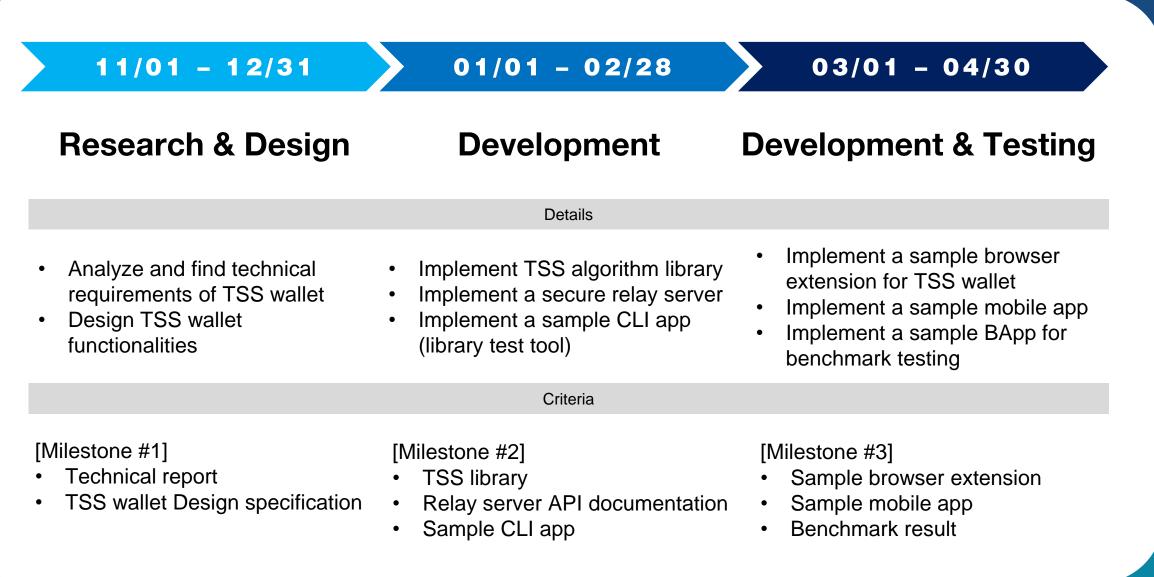
Features	Browser Wallet	TSS wallet	H/W Wallet		
Key Never Exposed	x	о	о		
Anti-Key Theft	x	о	x		
Key Refresh	X	о	X		

Features of TSS wallet

Comparison With Existing Wallets

Usability Features

Features	Browser Wallet	TSS wallet	H/W Wallet		
Easy Installation	о	о	x		
Hardware Price	Free	Free	\$100 - \$200		
Wallet Sync	X	о	X		



Securing your wallet, For our Klaytn World

TEEware