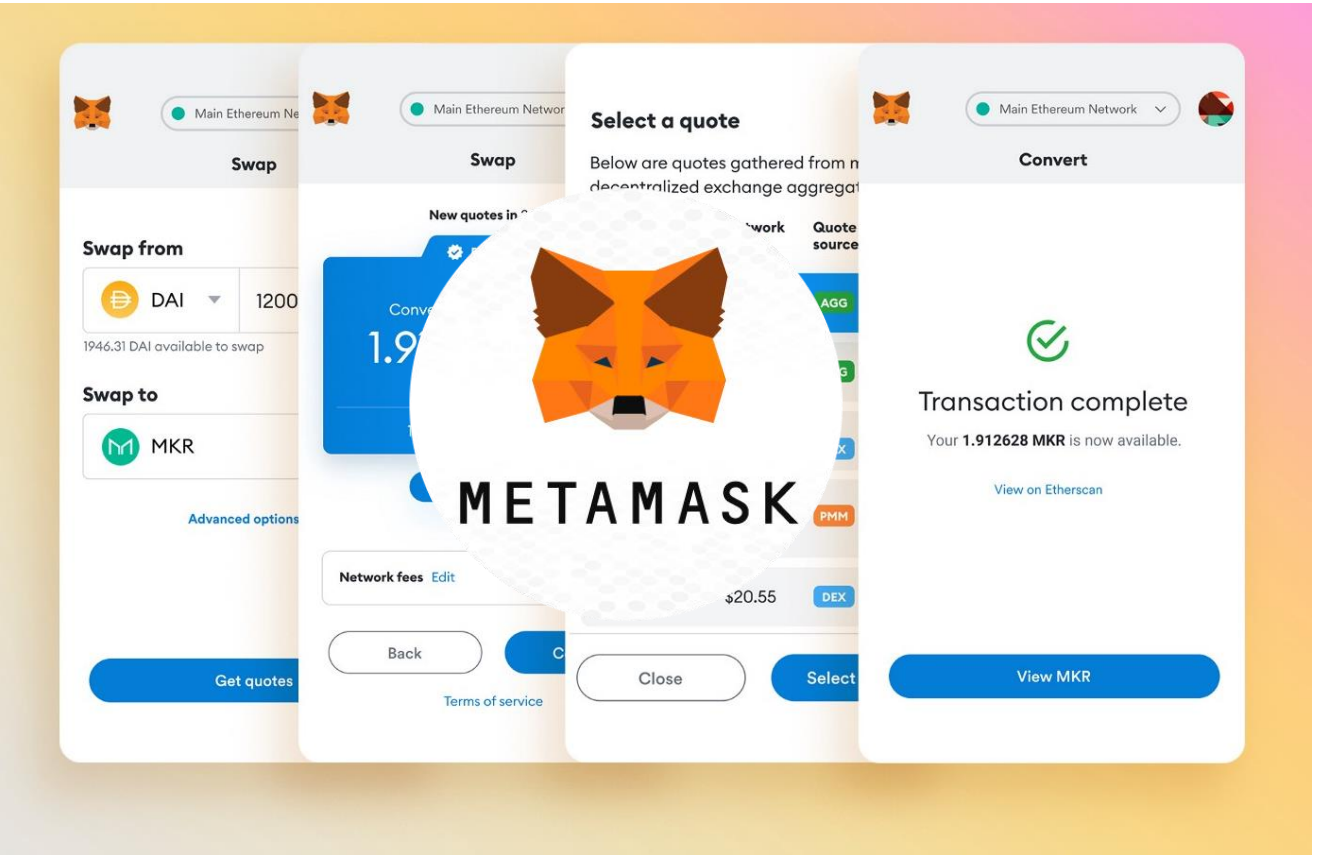
Threshold Signature Wallet for Klaytn

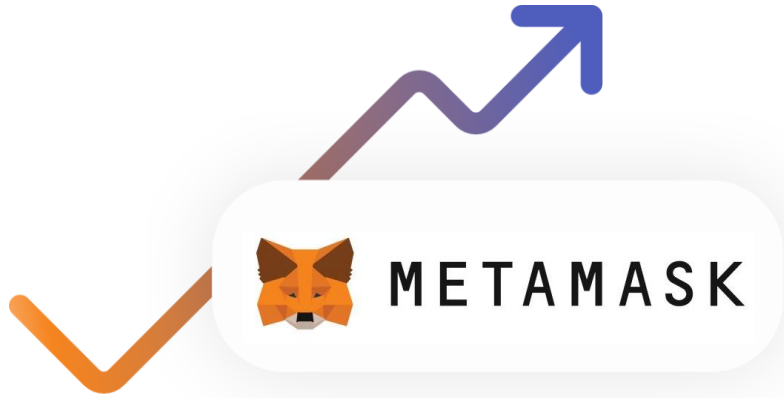
Klaytn Improvement Reserve Proposal

October 2021

TEEware

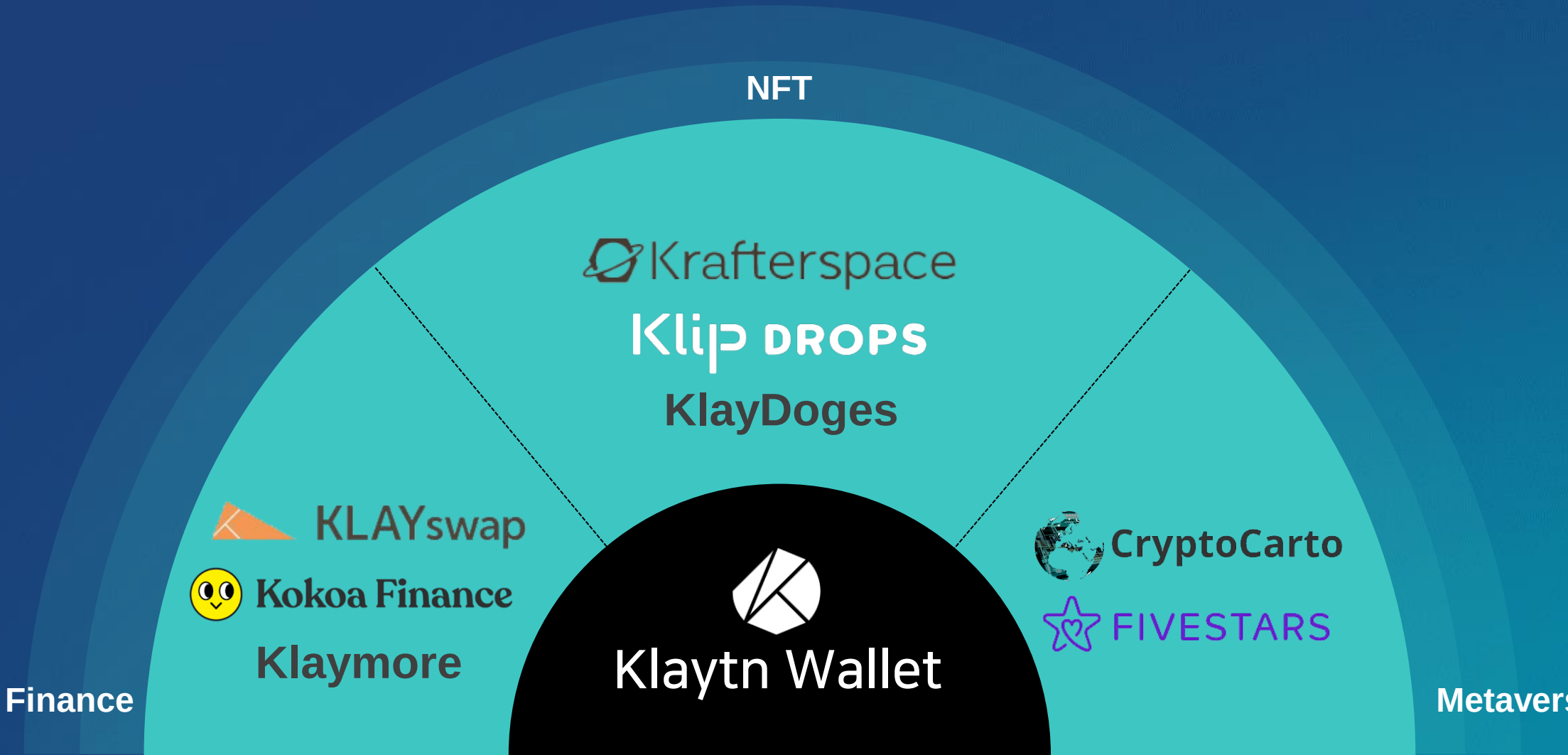
People Have High Expectations for Blockchain Apps, Evidenced by Metamask





10 Million Monthly Active Users!

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



Two Security Problems of Wallets

User may forget the password of the wallet

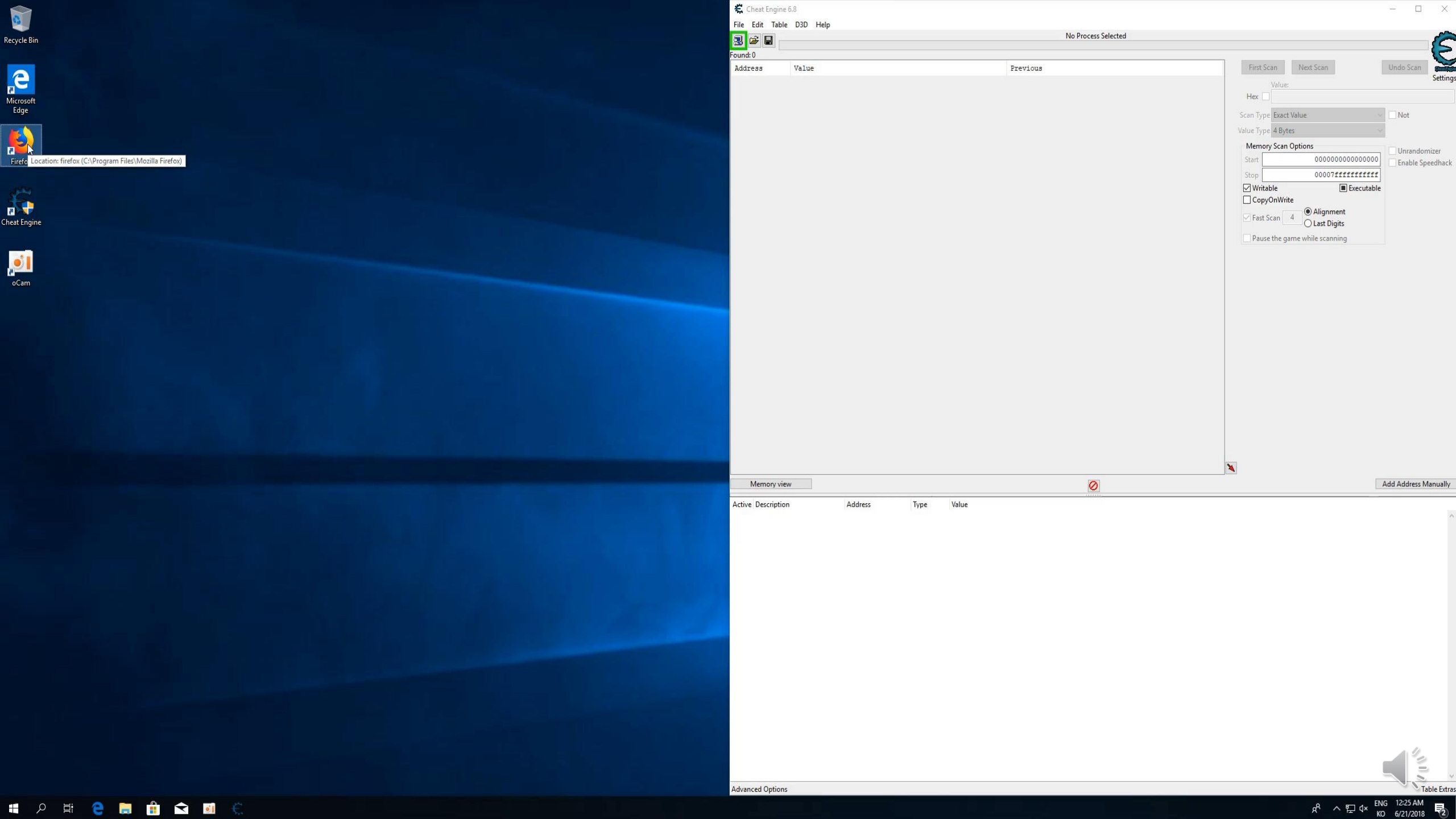
A programmer living in San Francisco forgot the password to his Bitcoin wallet.

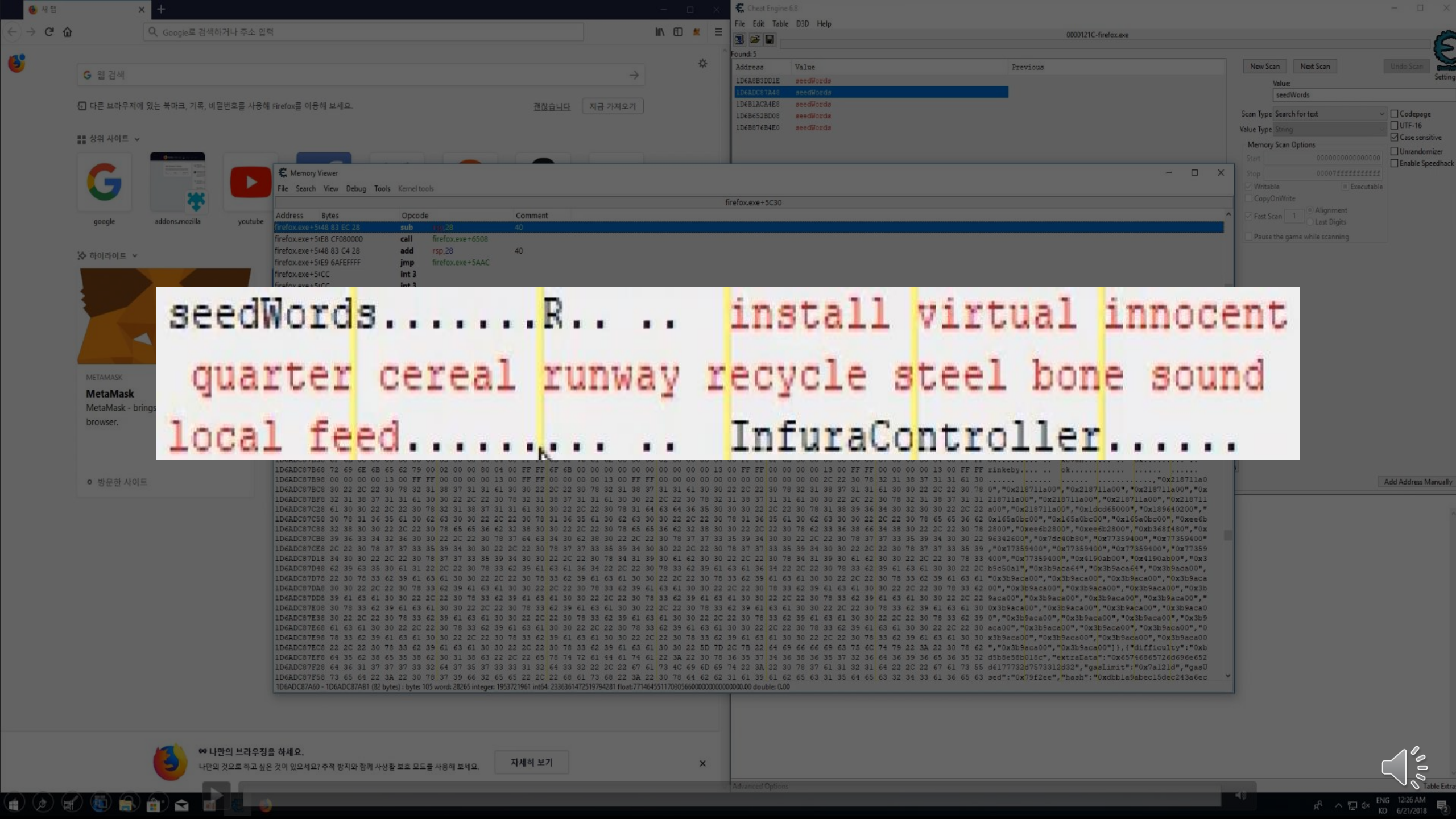
The wallet may be stolen by attackers

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

Demonstration of Metamask Hacking

Extracting seed words from a browser wallet


Recycle Bin
Microsoft Edge
Location: firefox (C:\Program Files\Mozilla Firefox)
Cheat Engine
oCam
Cheat Engine 6.8
File Edit Table D3D Help
No Process Selected
Found: 0
Address Value Previous
First Scan Next Scan Undo Scan
Settings
Value:
Hex
Scan Type Exact Value
Value Type 4 Bytes
Not
Memory Scan Options
Start 0000000000000000
Stop 00007fffffffffff
Writable Executable
CopyOnWrite
Fast Scan 4
Alignment
Last Digits
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add Address Manually
Active Description Address Type Value
Advanced Options
Table Extras
ENG KO
12:25 AM 6/21/2018


seedWords.....R.. .. install virtual innocent
quarter cereal runway recycle steel bone sound
local feed..... .. InfuraController.....

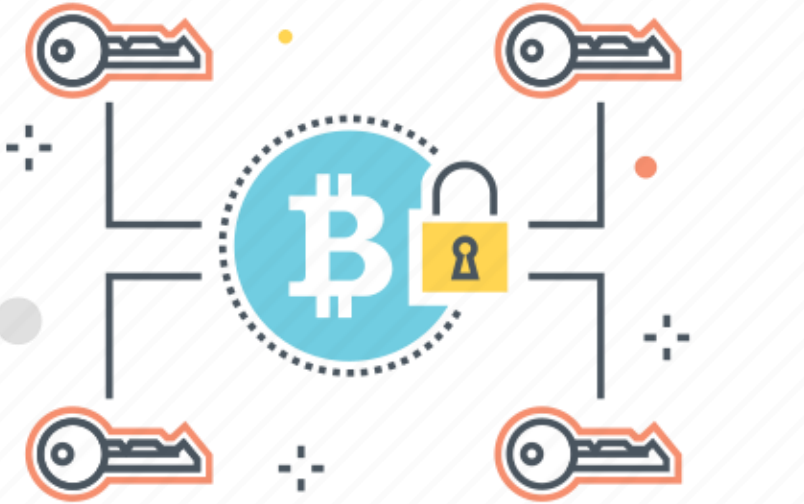
We Need to Protect the Private Key

1. Use a H/W wallet

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

2. Use a Multi-signature wallet

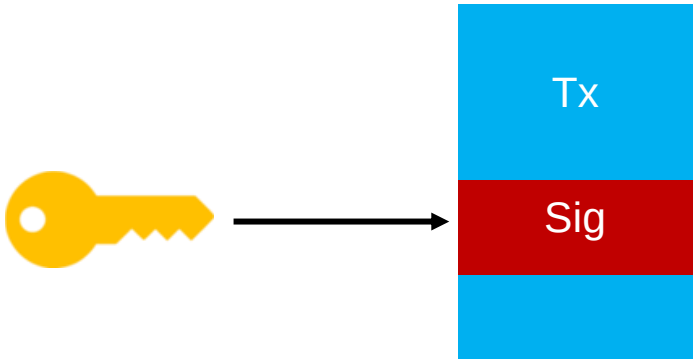
+ Having safeguard features (key recovery)
- Additional fees required
- Not all blockchain supports MultiSig



MultiSig is More Secure than SingleSig, But It is Inefficient

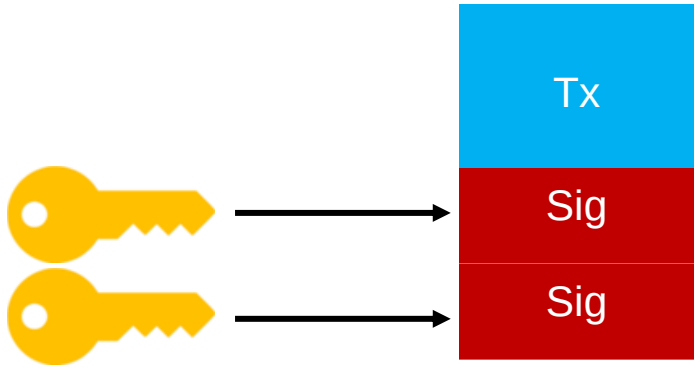
SingleSig

- An account depends on single private key

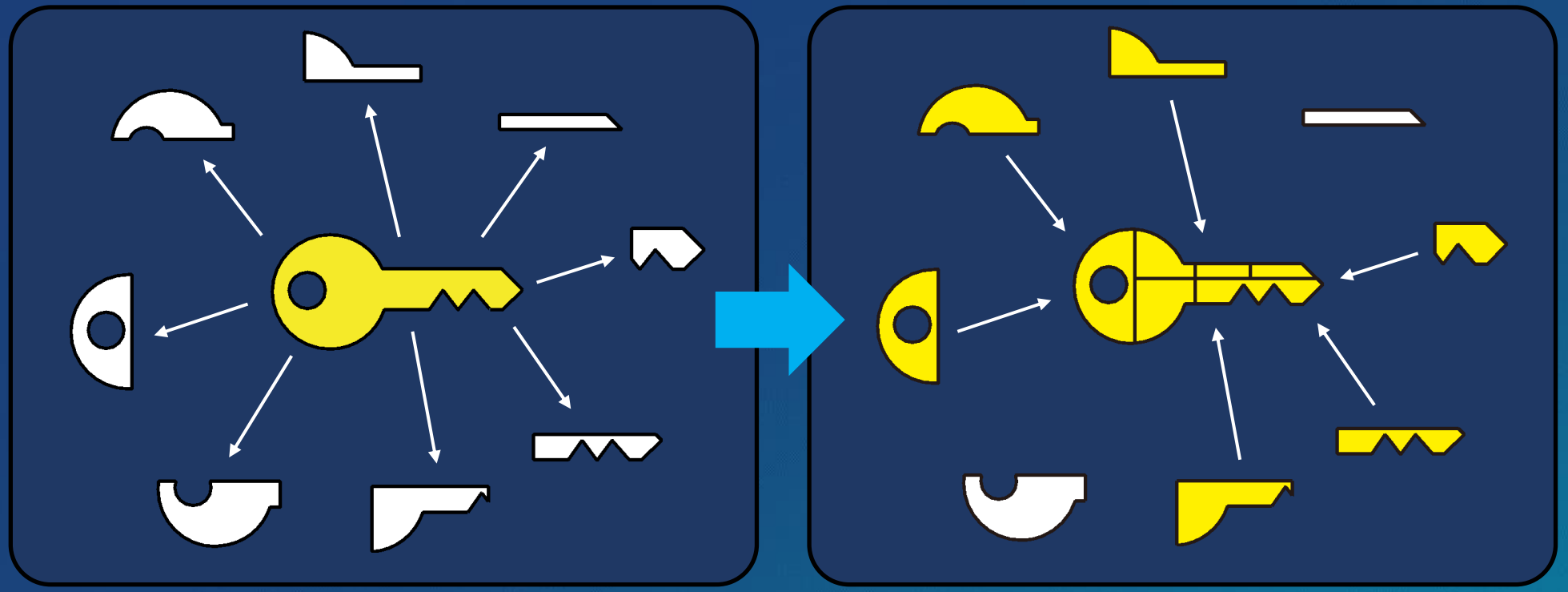


MultiSig

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



Threshold Signature is Superior to MultiSig

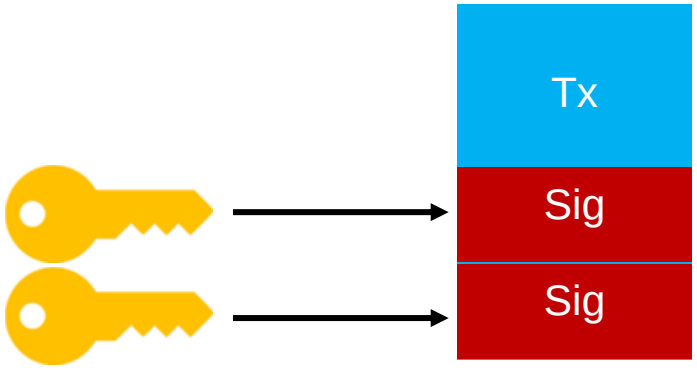


- ✓ Distributed key generation and signing
- ✓ No one has the private key
- ✓ Supports t of n key shares
- ✓ Compatible with any blockchain network

Threshold Signature Scheme: High Compatibility, and Low Transaction Fees

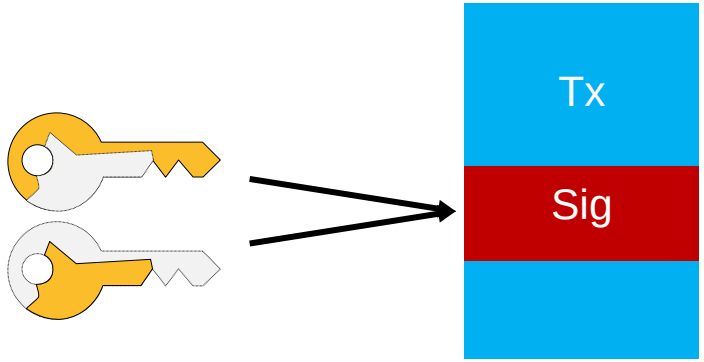
MultiSig

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



ThresholdSig

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



TSS wallet: A “Keyless” solution

SATISFIES SECURITY, EFFICIENCY, USABILITY

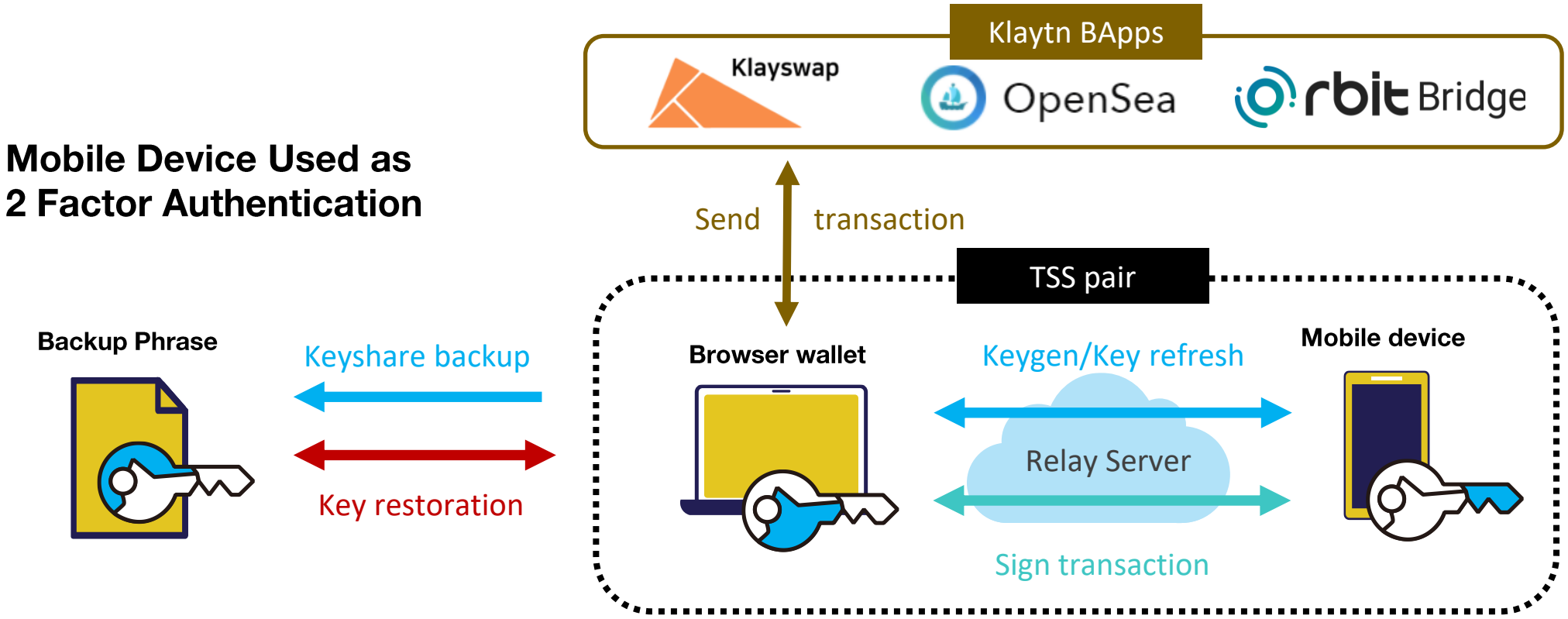
Private key never revealed

No additional transaction fee incurs

Compatible with all blockchain networks

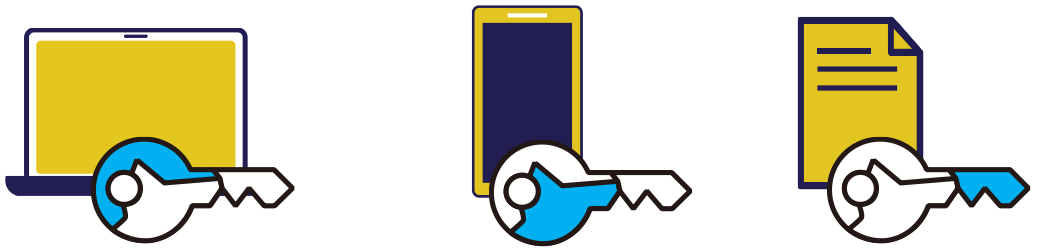
No additional H/W device required

PC and Mobile Device Co-work for Keygen and Sign



TSS wallet Design Choice

2-of-3 Key Shares



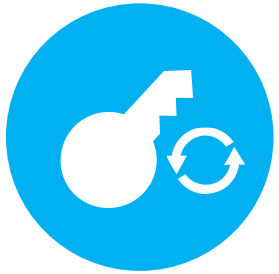
Browser extension **Mobile device** **Backup phrase**

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

Advantages of our design choice

Provides two-factor authentication method

OK even if part of device lost or stolen



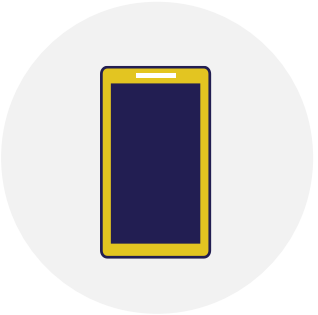
Privacy-preserved key recovery

No additional fees for key recovery

Components of TSS Wallet

Browser extension

- Initiate TSS keygen and sign
- Create a backup phrase



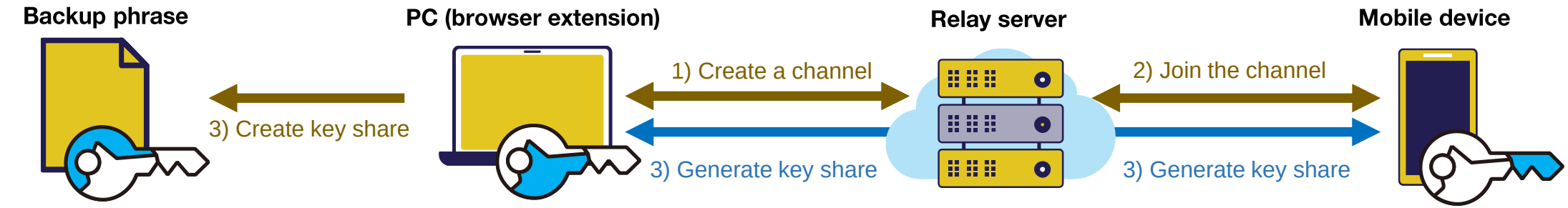
Mobile device app

- Participate in TSS keygen and signing transactions

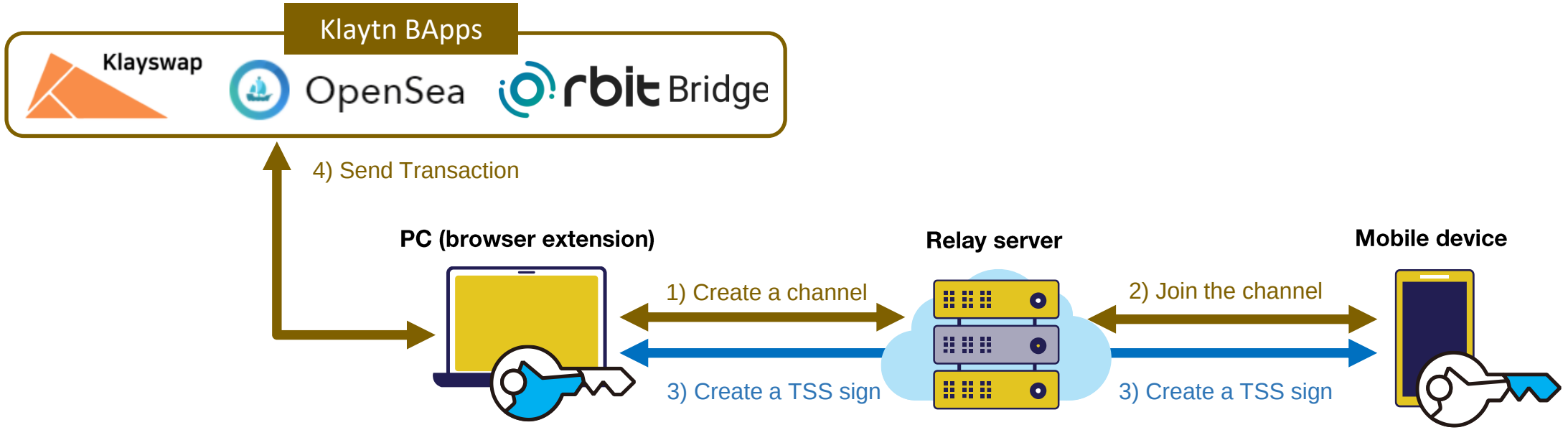
Relay server

- Create a secure channel between two entities

TSS Key Generation example



TSS Sign Example



Comparison With Existing Wallets

Security Features

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

Comparison With Existing Wallets

Usability Features

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

Milestones and Schedule

11/01 – 12/31	01/01 – 02/28	03/01 – 04/30
Research & Design	**Development**	**Development & Testing**
Details		
• Analyze and find technical requirements of TSS wallet • Design TSS wallet functionalities	• Implement TSS algorithm library • Implement a secure relay server • Implement a sample CLI app (library test tool)	• Implement a sample browser extension for TSS wallet • Implement a sample mobile app • Implement a sample BApp for benchmark testing
Criteria		
[Milestone #1] • Technical report • TSS wallet Design specification	[Milestone #2] • TSS library • Relay server API documentation • Sample CLI app	[Milestone #3] • Sample browser extension • Sample mobile app • Benchmark result

Securing your wallet, For our Klaytn World