



**ZKSAFE**

Centralized Experience Decentralized Implementation

# Existing safety situation

PrivateKey stolen happens everyday

According to Keystone, only 10% crypto users use hardware wallet. The other 90%, they don't have any protection for their assets

Hardware or MultiSig ? Come on, they're hard to use (not fit for normal users)

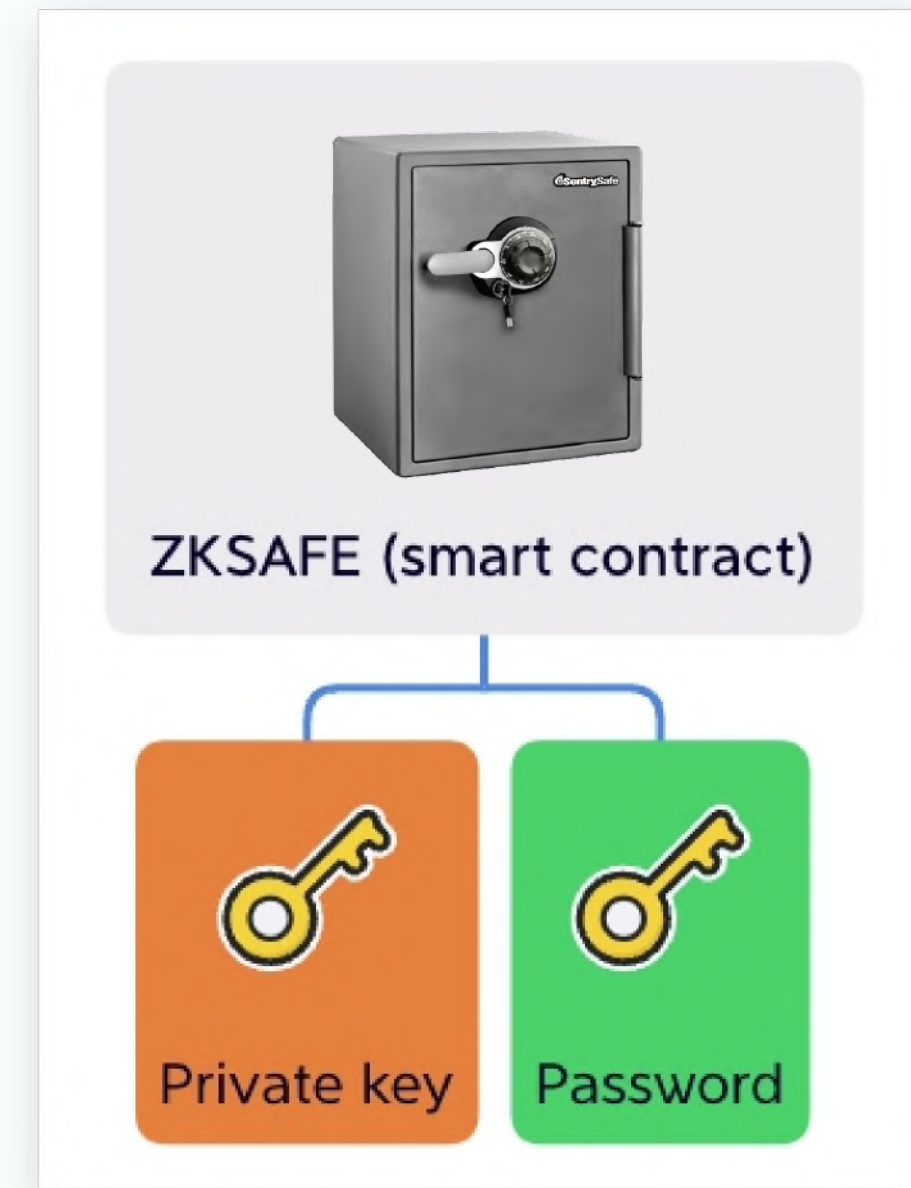


# New safety solution

If your **Private key** is Stolen, your asset is **still Safe**

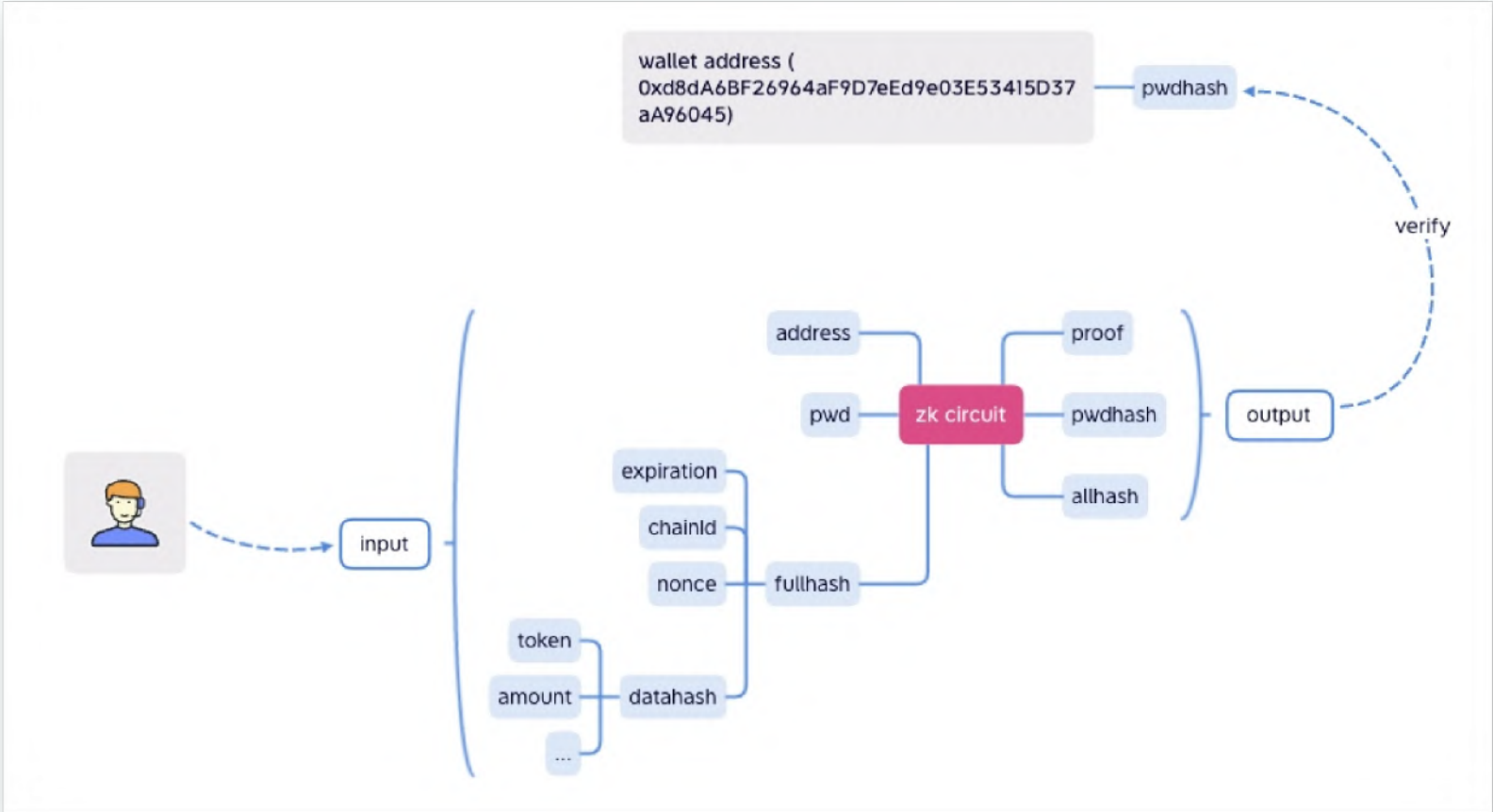
It needs not only **Private key**, but also a **Password**

1 Private key + 1 Password **mutil-sign**



# How it works

<https://docs.zksafe.pro/zkpass/zkpass>



We use Password to sign data as Private key

Base on Zero-knowledge proof

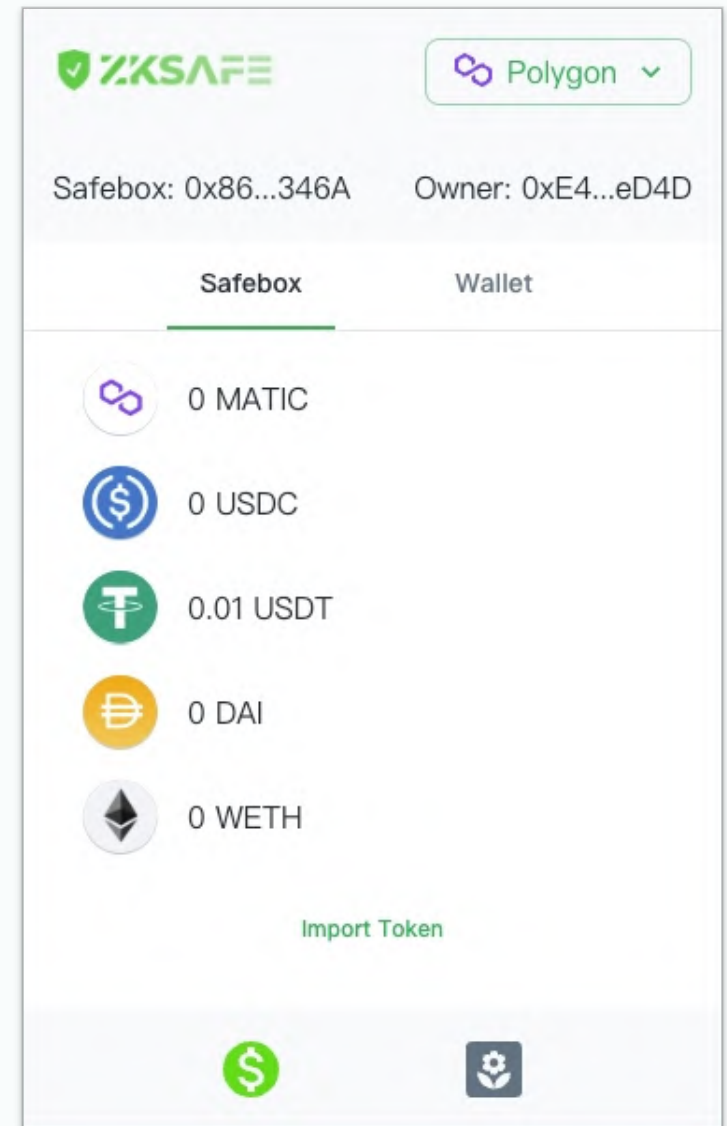
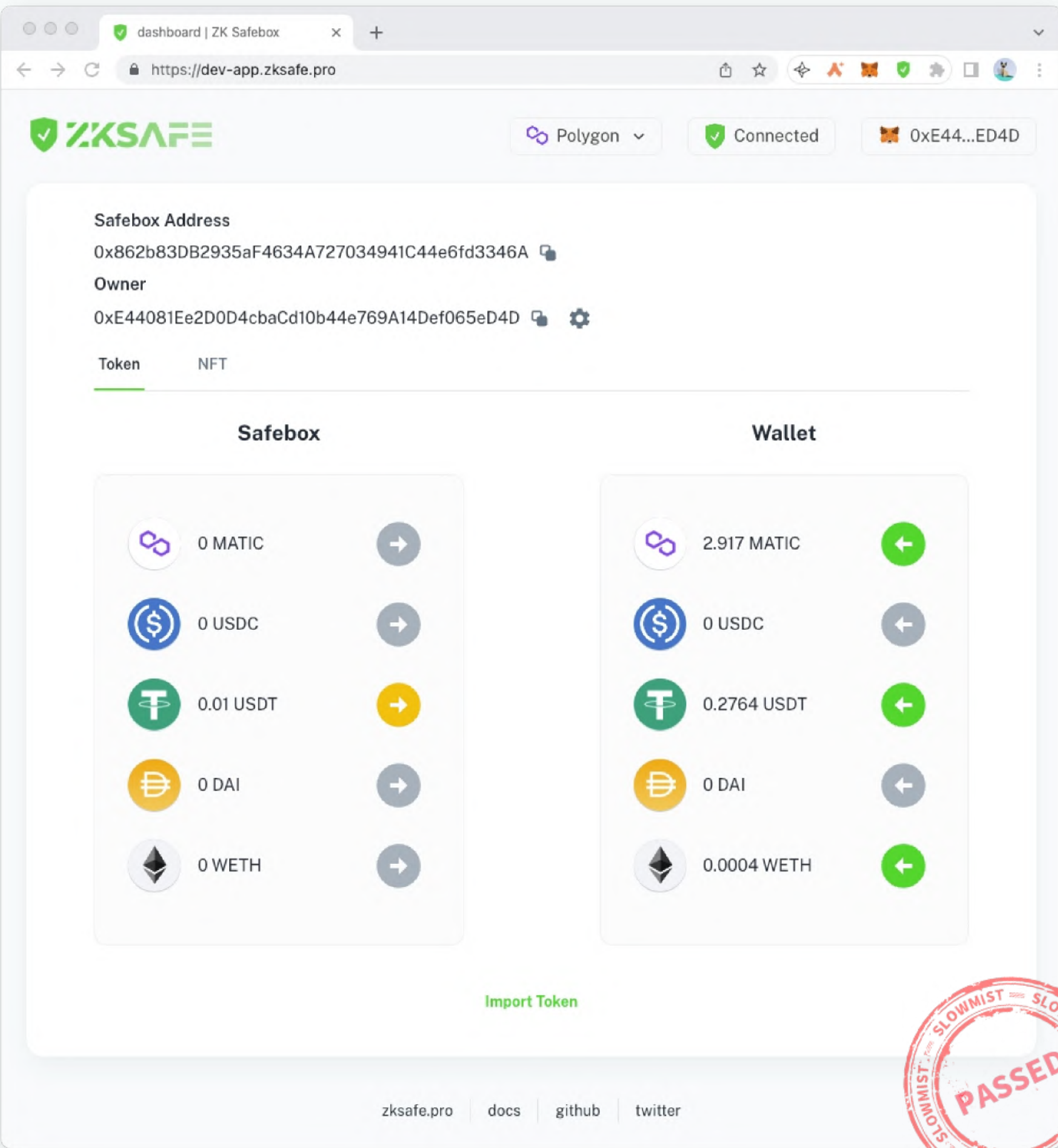
Sign data at front-end  
Verify signature in smart contract  
It's serverless (no storage, no risk to be stolen)

## EIP-6237: Elastic Signature

eip	title	description	author	discussions-to	status	type	category	created
6327	Elastic Signature	Use password to sign data as privatekey	George (@JXRow)	<a href="https://ethereum-magicians.org/t/eip-6327-elastic-signature-es/12554">https://ethereum-magicians.org/t/eip-6327-elastic-signature-es/12554</a>	Draft	Standards Track	ERC	2023-01-13

<https://github.com/ethereum/EIPs/pull/6327>  
<https://github.com/JXRow/EIPs/blob/master/EIPS/eip-6327.md>





Browser Plugin

MetaMask deal with PrivateKey  
ZKSAFE deal with Password



# Withdrawal

ZKSAFE

Polygon

Download

0xb42...Be26

Safebox Address

0xE97f78Ec2977c2806697bB245595107B5b54B3f1

Owner Address

0xb42466f1c2B0d878ff14E76477f8AF016E5dBe26

Token

NFT

Safebox

1 MATIC

0 USDC

0 USDT

0 DAI

0 WBTC

0 WETH

Safebox Address

0xE97f78Ec2977c2806697bB245595107B5b54B3f1

Owner Address

0xb42466f1c2B0d878ff14E76477f8AF016E5dBe26

Token

NFT

Safebox

1 MATIC

0 USDC

0 USDT

0 DAI

0 WBTC

0 WETH

Wallet

0 WBTC

0 WETH

Send to Wallet

0.5

MAX MATIC

Safebox balance: 1 MATIC

Send 0.5 MATIC from Safebox to Wallet

Cancel

Confirm

Notification

Owner: 0xb4...Be26

Polygon

0xE9...B3f1

0xb4...Be26

Send to wallet amount

0.5 MATIC

Safebox Balance

1 MATIC

Wallet Balance

1.106 MATIC

Enter your password

Cancel

Confirm

MetaMask Notification

Edit

Matic Mainnet

ZKSAFE Coder

0xE97...B3f1

New address detected! Click here to add to your address book.

DETAILS

DATA

HEX

Estimated gas fee

0.02232698

0.022327 MATIC

Site suggested

Likely in < 30 seconds

Max fee: 0.02688899 MATIC

Total

0.02232698

0.02232698 MATIC

Amount + gas fee

Max amount: 0.02688899 MATIC

Reject

Confirm

Try Pitch

ZKSAFE



# Security

Since the pwdhash is public, it is possible to be crack the password.  
We estimate the Poseidon hash rate of RTX3090 would be 100Mhash/s,  
this is the estimate of crack time:

- 8 chars (number + english) : 25 days
- 8 chars (number + english + symbol) : 594 days
- 12 chars (number + english) : 1023042 years
- 12 chars (number + english + symbol) : 116586246 years

# Audit

Audit Number	Audit Team	Audit Date	Audit Result
0X002211290001	SlowMist Security Team	2022.11.22 - 2022.11.29	Low Risk

Summary conclusion: The SlowMist security team use a manual and SlowMist team's analysis tool to audit the project, during the audit work we found 2 low risk, 4 suggestion vulnerabilities.

<https://www.zksafe.pro/audit/SlowMistAuditReport-ZKSAFE.pdf>

# Bug Bounty

ZKSAFE

@ZKSAFE · Dec 27, 2022

Hello Everyone !

🥰🥰

Excited to announce our \$10,000 #BugBounty event:

💰

Sincerely invite you to crack:

Safebox Address:

0xD9AC6131D2844F39837f11459835c297F9f3A6D6

privatekey:

f64d8f8bdb2d0bb1419814f361bad36d1510230d5e5348235f80e0d6990e999f

zksafe.pro

ZKSAFE

27 Dec. 2022 – 27 Mar. 2023

ZKSAFE BUG HUNTING

COMPETITION

PRICE POOL

10K USDT

@ZKSAFE

24.7K

4

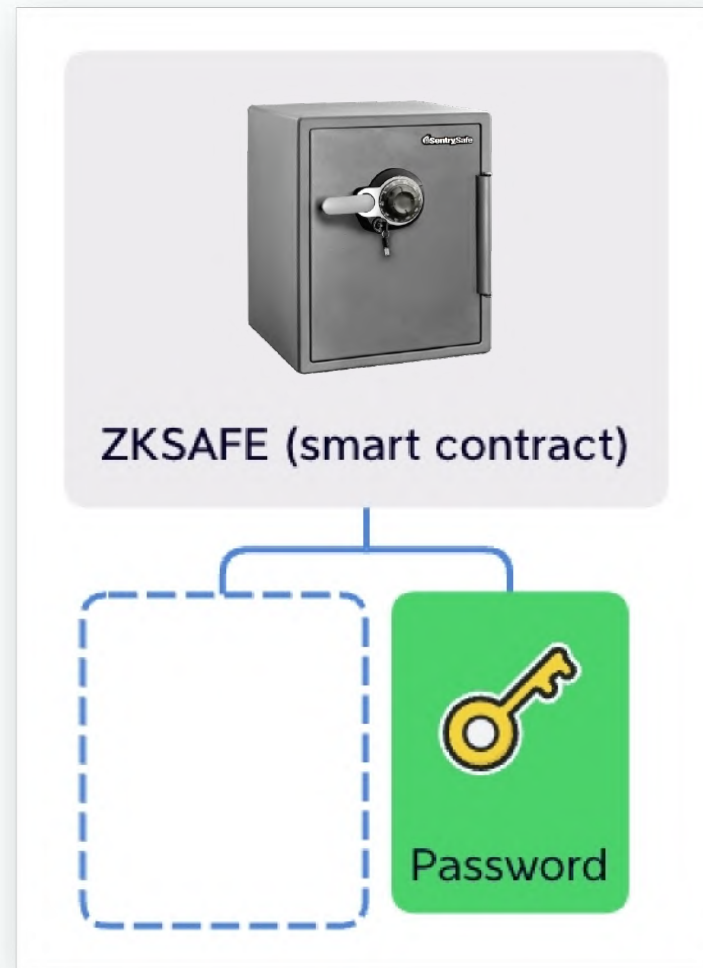
23

26



# ZKSAFE v2 (building)

implements ERC4337



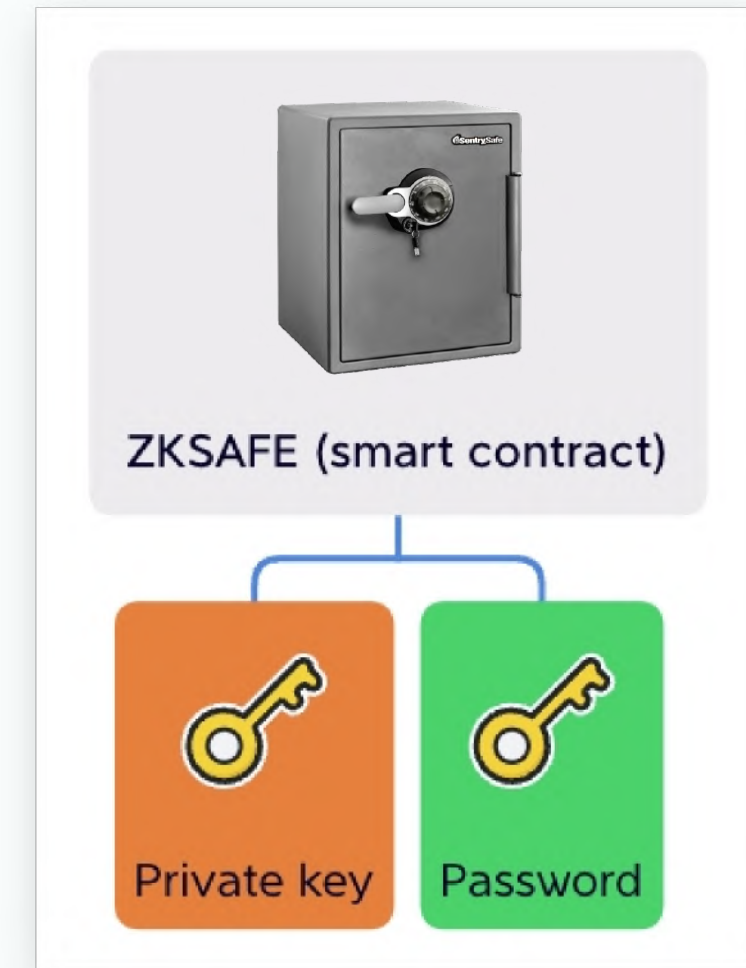
## Single Password

for new user get into Web3 (from WeChat eg.)



## Double Password

small money: login pwd  
big money: login pwd + secure pwd



## Double Security

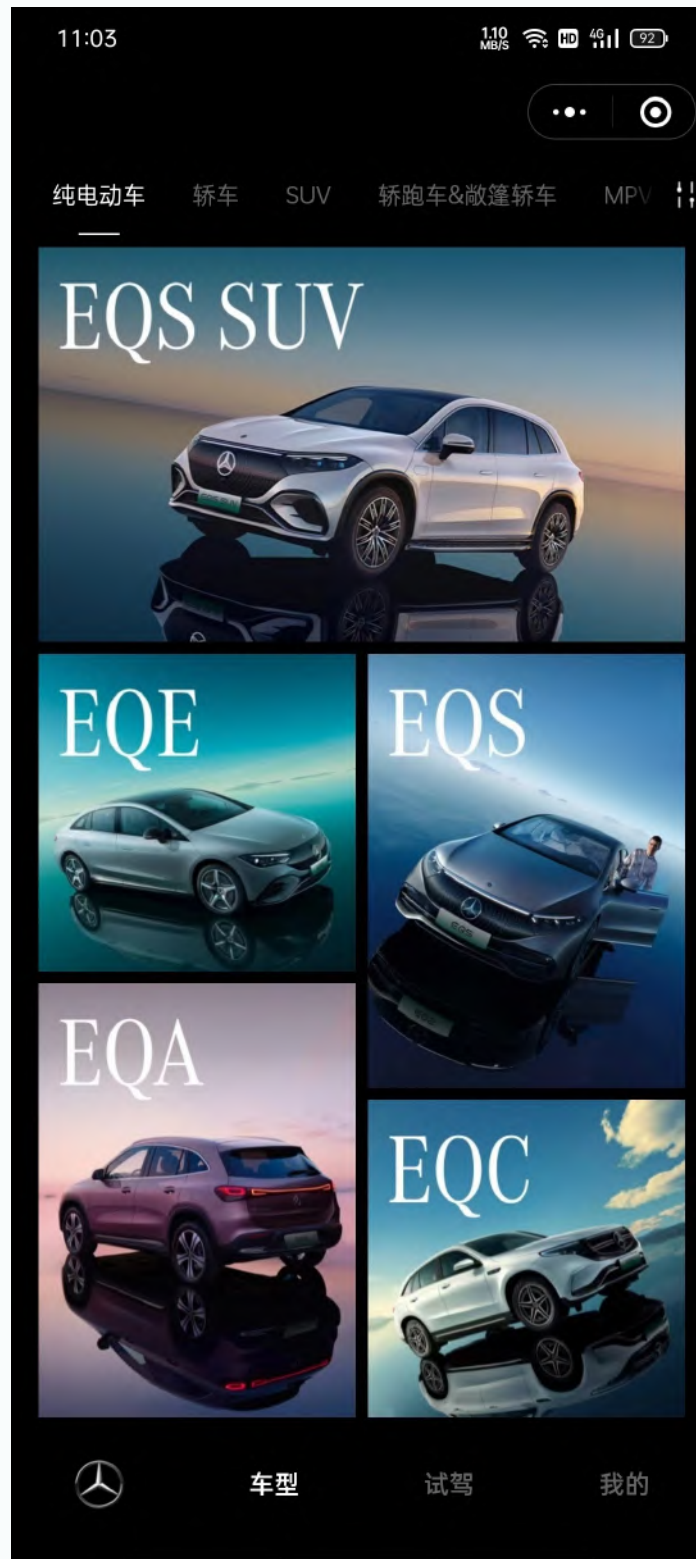
small money: private key  
big money: private key + secure pwd  
(done by v1)



# MPC VS ZKSAFE

	EOA	MPC	ZKSAFE
Verify	Private key	Password	Password
Key stored	User's device	Servers	User's mind
Serverless	Yes	No	Yes
Seedless	No	Seed in servers	Yes
Security	Decentralized	Centralization risk	Decentralized
Complex	Simple	Complex	Simple
Gas cost	Low	Low	High (Low in L2)

# Application Scenario



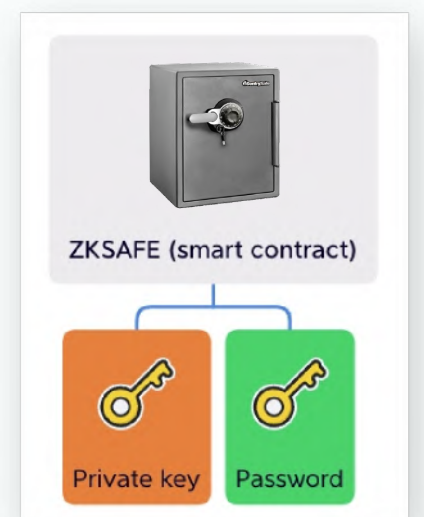
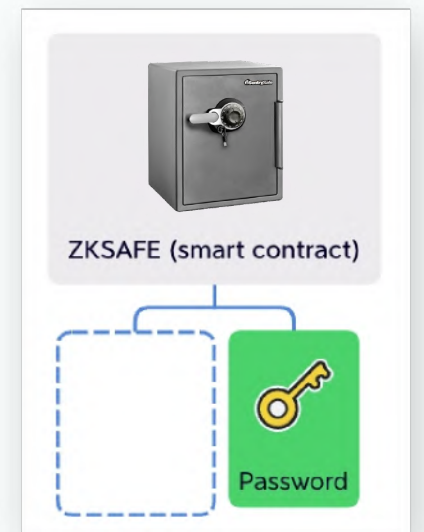
How can Benz mint NFT to its users ?

- Ask them to write down the seed? **NO**
- Use centralized scheme ? **NO**
- Seedless and serverless, **Yes**, that's **ZKSAFE**

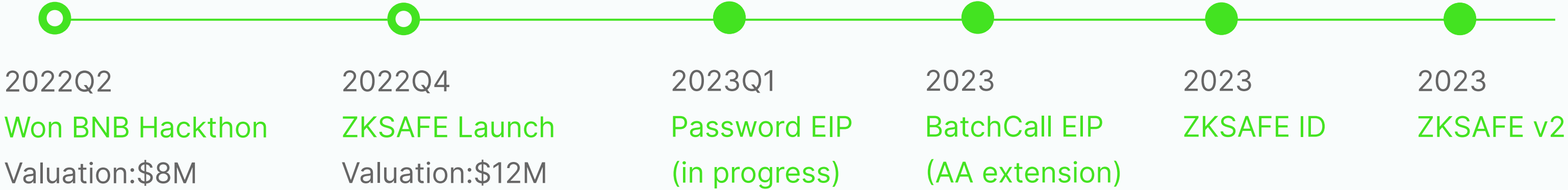
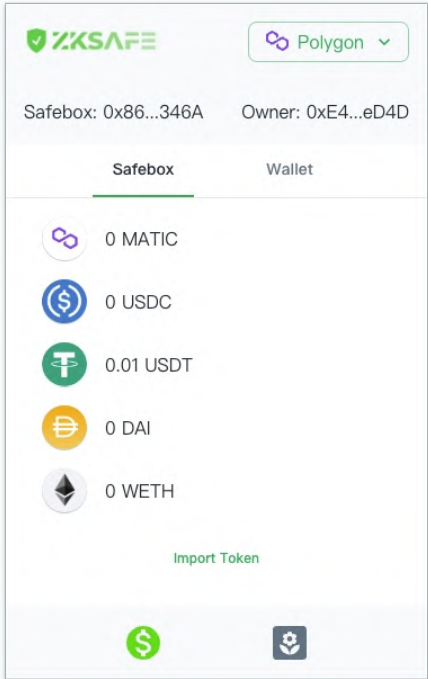
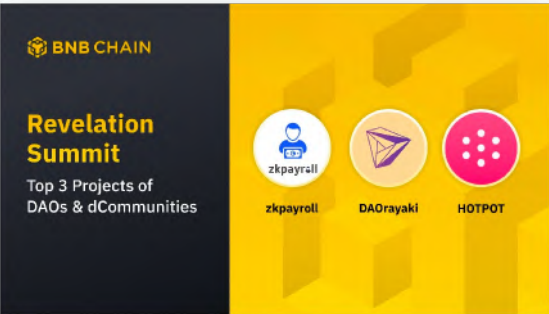
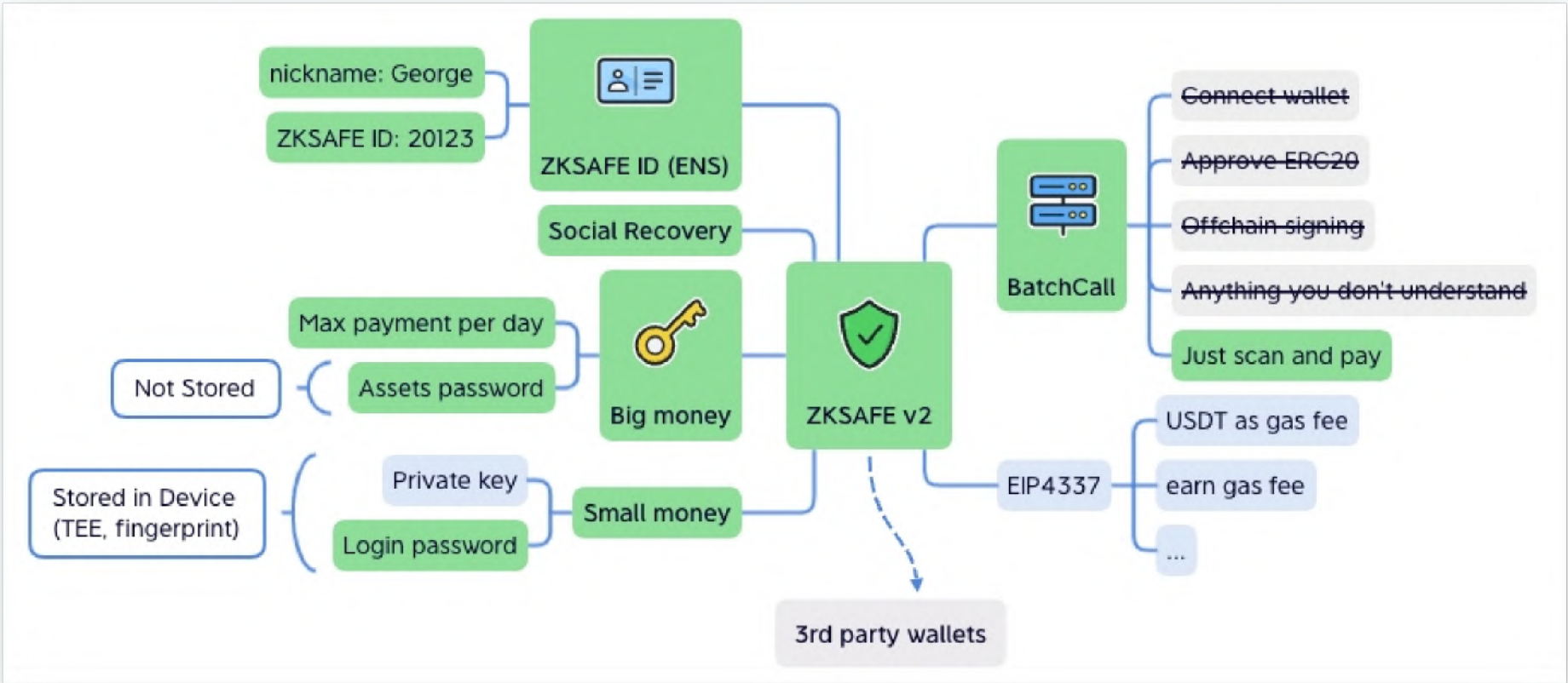
User needn't to download ZKSAFE app,

in any webs(eg. web in WeChat),  
**get ZKSAFE(Single Password) anywhere**

in any wallets(eg. imToken), open ZKSAFE Dapp,  
**get ZKSAFE(Double Security) anywhere**



# Roadmap





**BNB CHAIN**

# Revelation Summit

Top 3 Projects of DAOs & dCommunities

zkpayroll

DAOrayaki

HOTPOT

**Hacker Dōjō**

# ETH Research Grant

**ROUND 1 GRANTEE DEMO**
18TH JAN 9PM EST

## ZKSAFE Password

Cryptography Research

ZKSAFE Password is a great cryptography system which can be expanded to support not only ZKSAFE, but also various asset management platforms, and even private key-less wallets.

Nov 28th, 2022 - Jan 18th, 2023
Round-2

# BNB GRANT DAO

## Round 1 Winners Joining Voting

Ark Rivals

Metaverse / Gaming / Music/NFT

BetaMars

Metaverse / Gaming / Music/NFT

Cryptosat

Frontier technology

DAOrayaki

DAOs / Communities

Velvet Capital

DeFi

InsurAce

DeFi

Astar

Crypto Twitter & Social

Zecrey

Public Goods (Web3 Infra & Tooling)

ZKSAFE

ZK projects

BNB Grant DAO Round2 Details  
<https://dora hacks.io/bnb/2>

WINNER

## zkSafebox

ZKSafebox is double security for assets, your private key and your password. with ZK-SNARK, the password is hided. The contracts have no owner, no backend, that means ZKSafebox is running as a protocol.

View Project

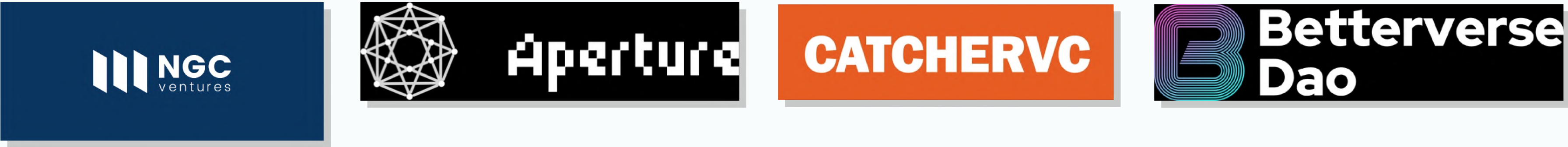
View Bounty

### Team Members

Sponsored by maticnetwork



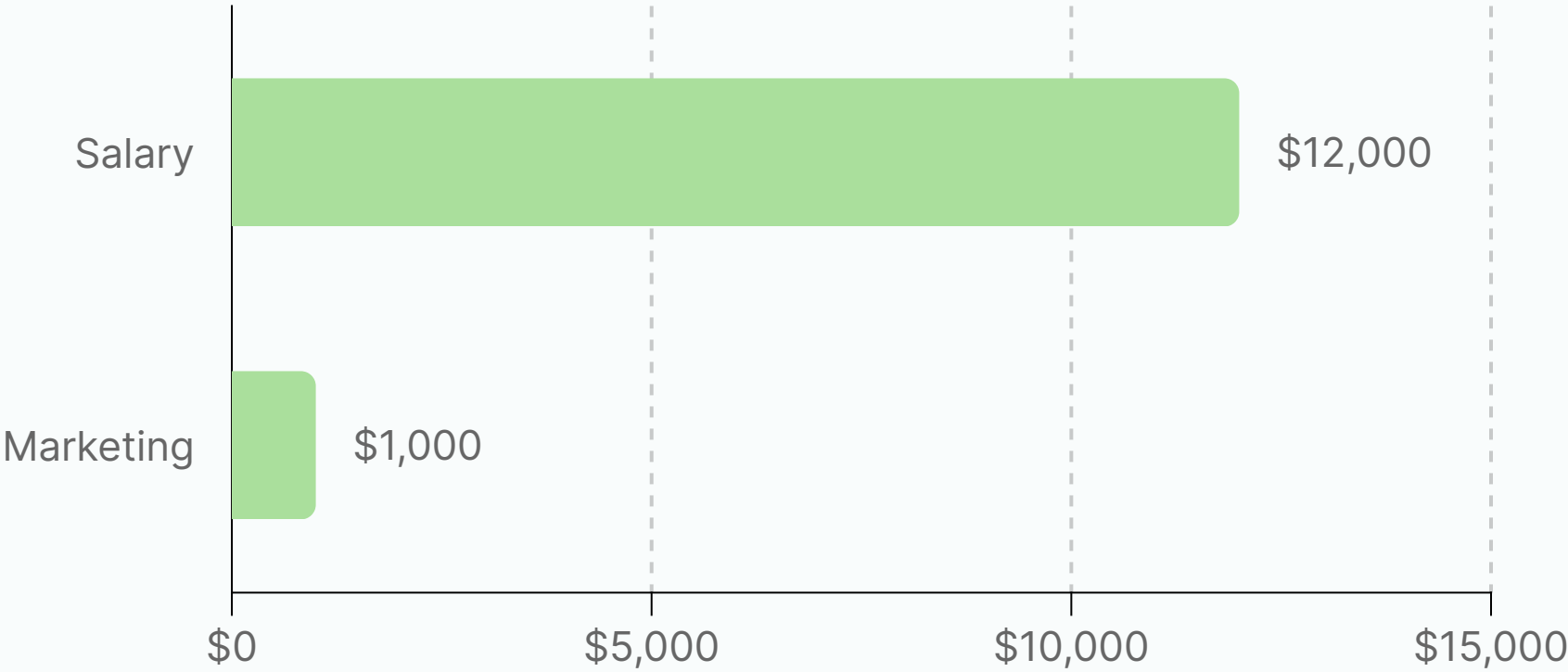
# Seed Round (\$560K)



Backers



## Use of Proceeds (per month)



# Thanks!

## We'd love to hear your feedback

ZKSAFE is a decentralized asset security product based on Zero-knowledge Proof. Even if private key is stolen, asset is still safe. The team is made up of a small group of aspiring crypto geeks, innovation is what drives us, and more incredible products are in the pipeline.

ZKSAFE是基于零知识证明的去中心化资产安全产品，即使私钥被盗，资产依然安全。团队由一小撮志向远大的加密极客们组成，创新是我们的驱动力，更多不可思议的产品正在开发中。

Related Links

Website: <https://www.zksafe.pro>

Twitter: <https://twitter.com/ZKSAFE>

Medium: <https://medium.com/@ZKSAFE>

GitHub: <https://github.com/ZKSAFE>

## Contacts

Shawn

COO

Telegram @Shawn\_zkSafe

twitter @ZKSAFE

shawn@zksafe.pro

