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

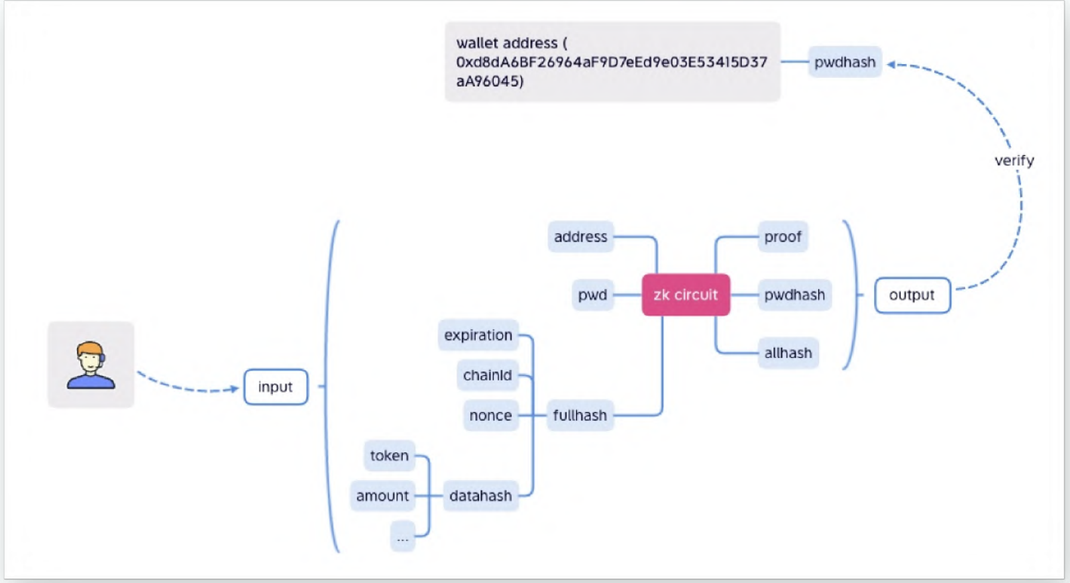
It needs not only Private key, but also a Password

1 Private key + 1 Password mutil-sign

ZKSAFE

How it works

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



We use Password to sign data as Private key

Base on Zero-knowledge proof

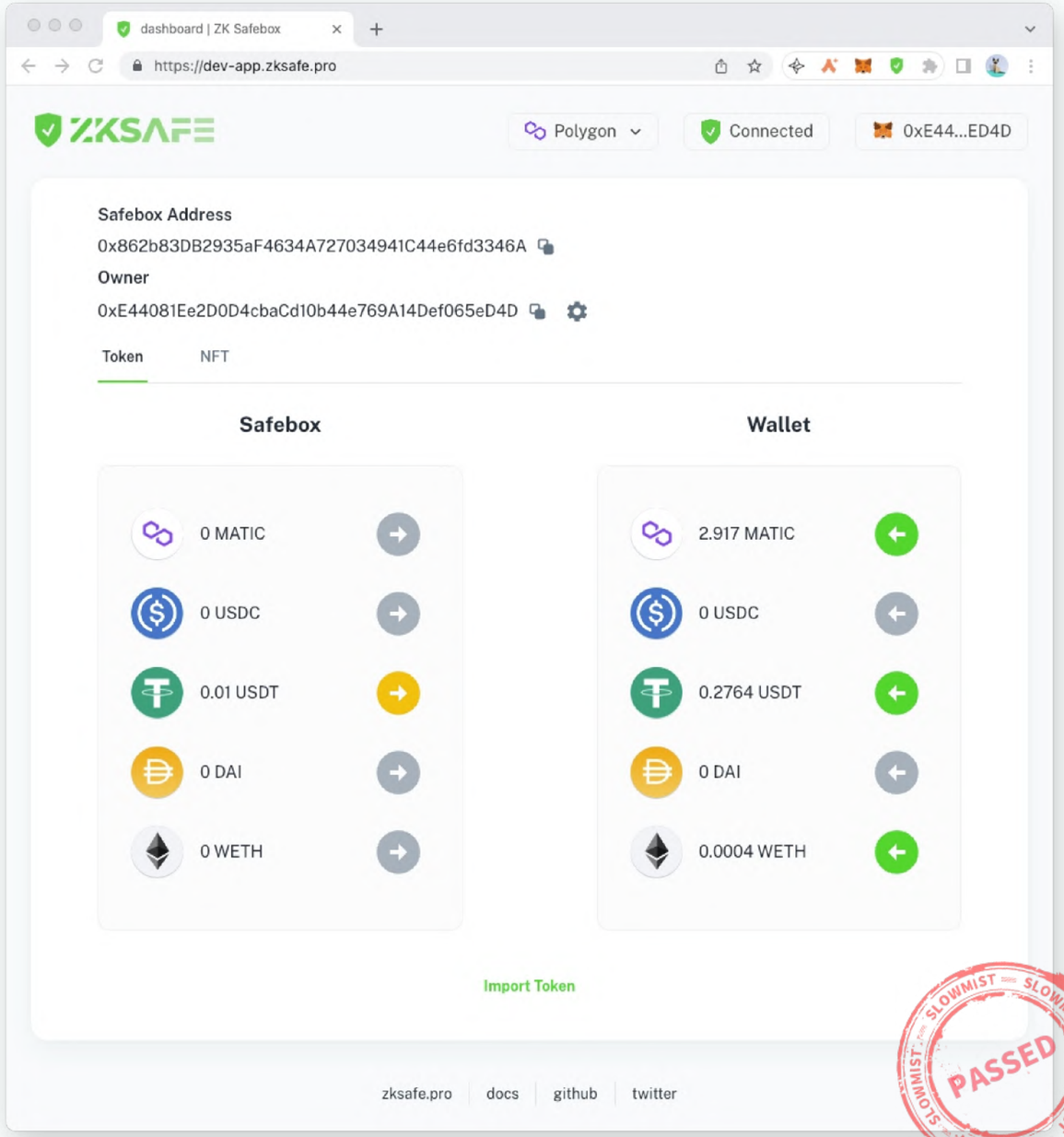
Sign data at front-end
Verify signature in smart contract
It's serverless (no storage, no risk to be stolen)

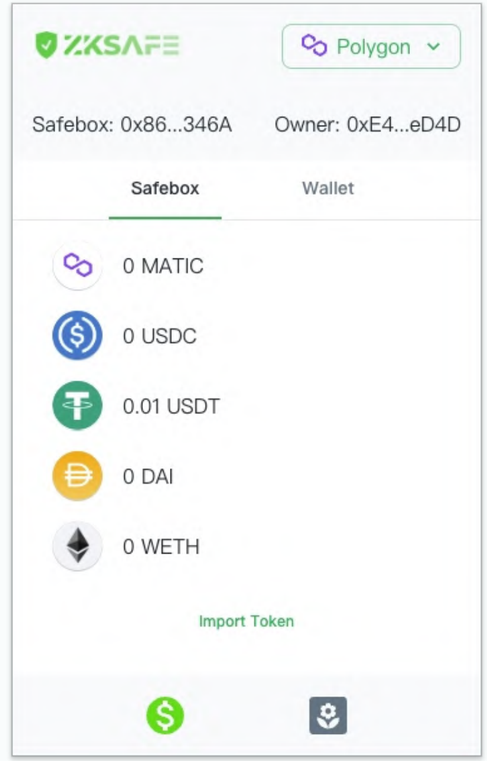
EIP-6237: Elastic Signature

eip	title	description	author	discussions-to	status	type	category	created
6327	Elastic Signature	Use password to sign data as privatekey	George (@JXRow)	https://ethereum-magicians.org/t/eip-6327-elastic-signature-es/12554	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

ZKSAFE





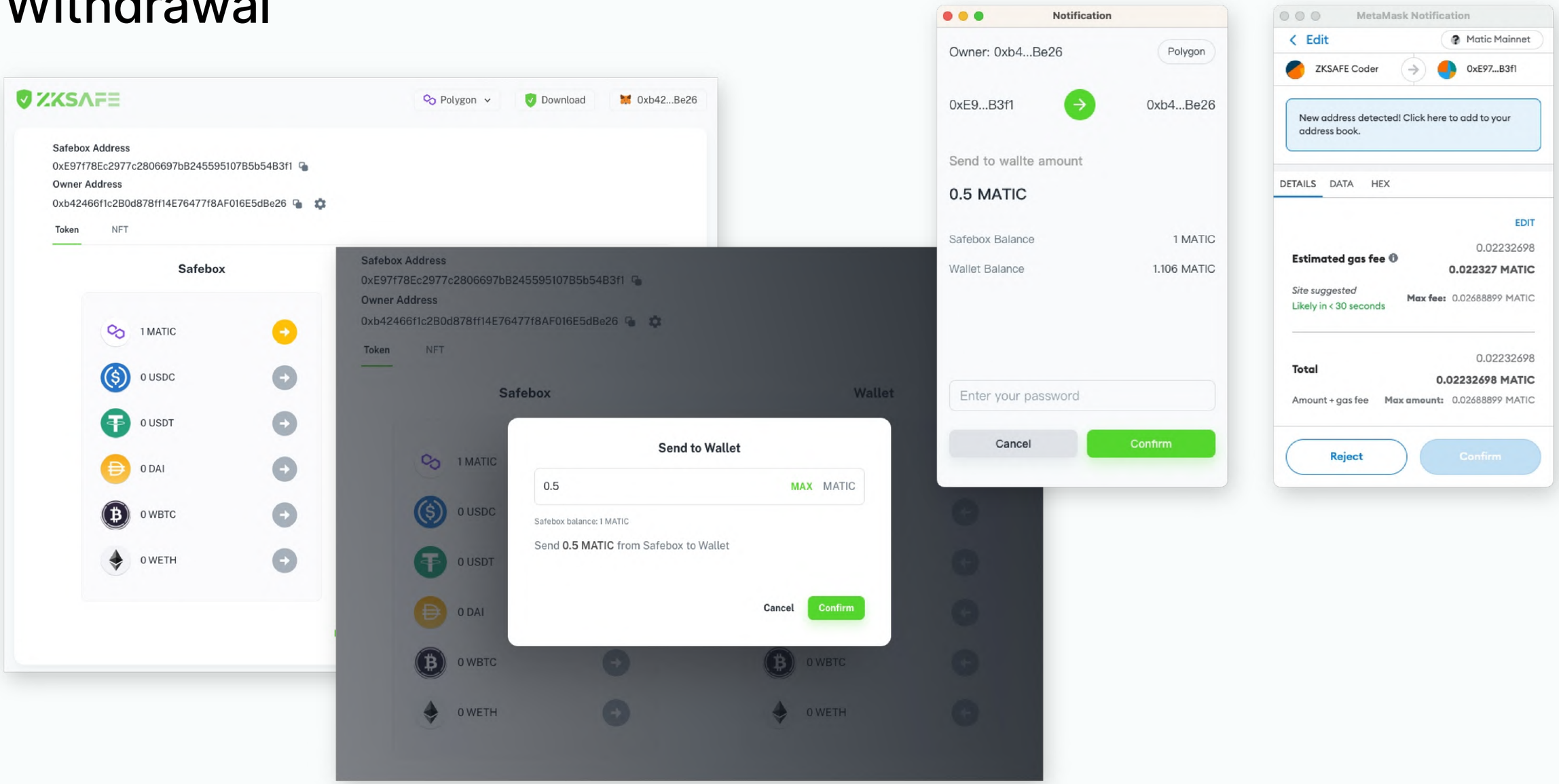
Browser Plugin

MetaMask deal with PrivateKey
ZKSAFE deal with Password

Try Pitch

ZKSAFE

Withdrawal



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

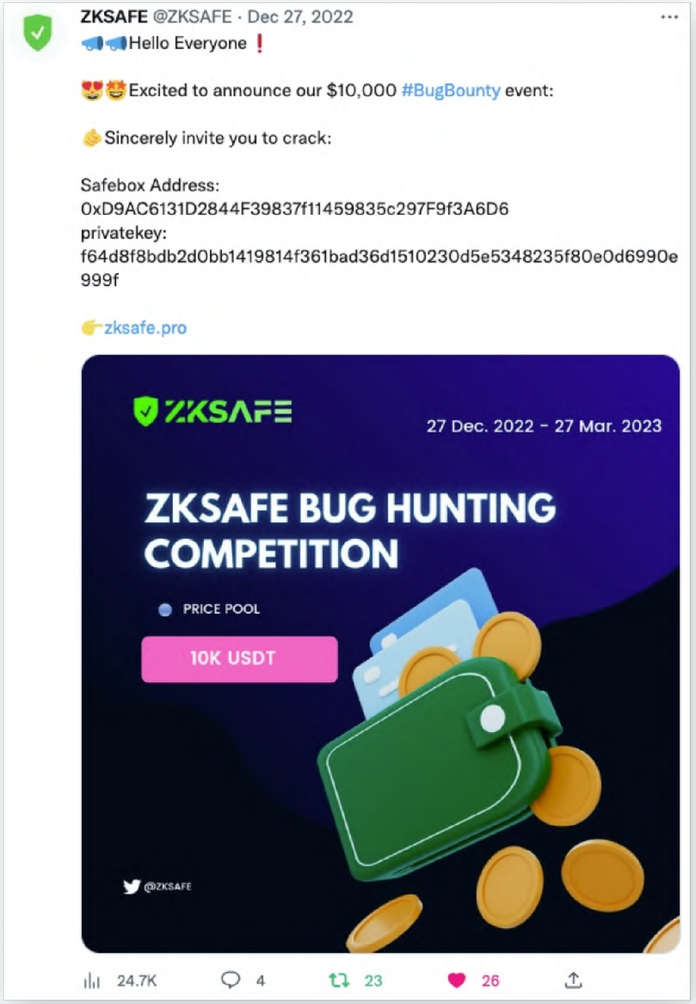
Audit

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

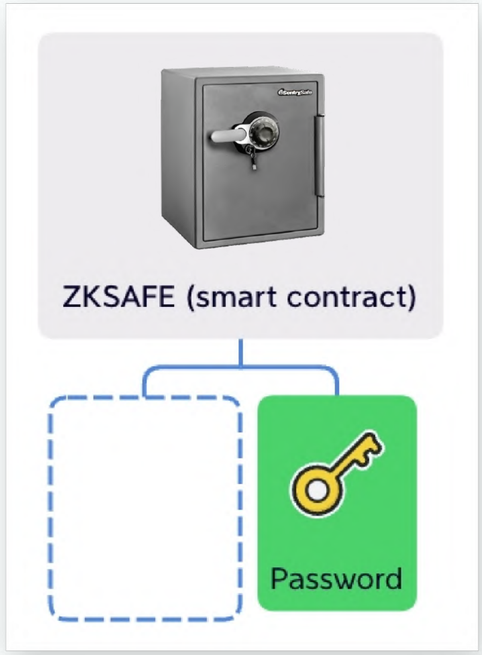
Bug Bounty



Try Pitch

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)

ZKSAFE

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)

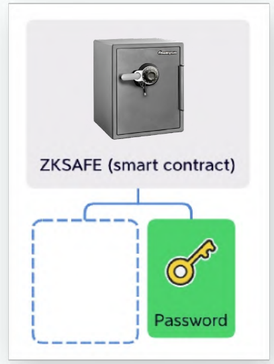
ZKSAFE

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

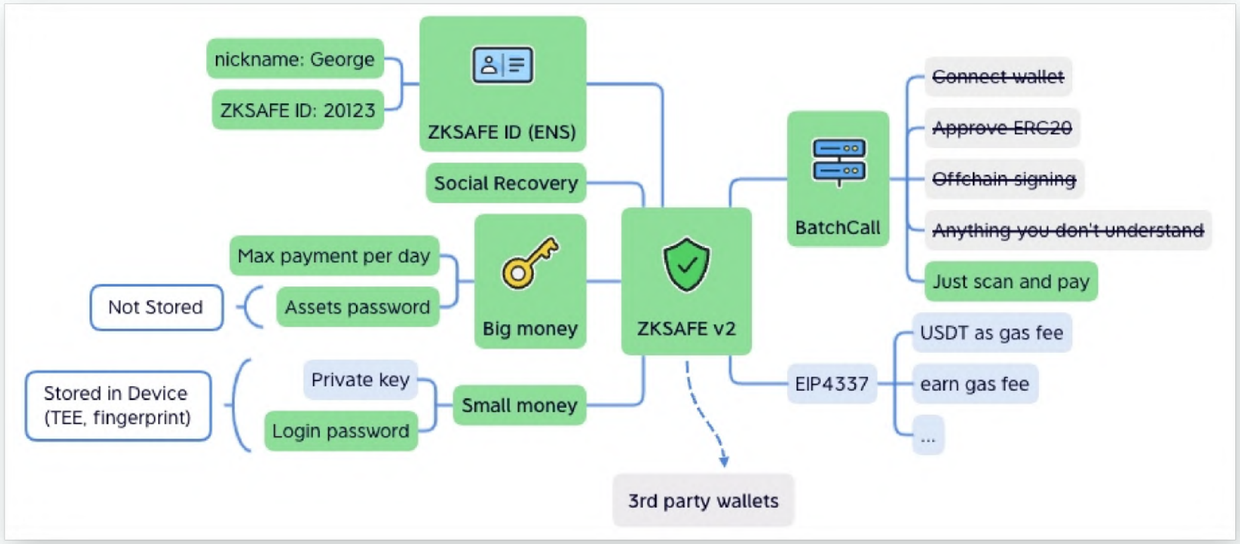
User needn't to download ZKSAFE app,

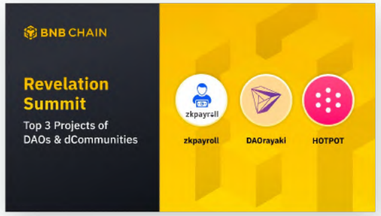


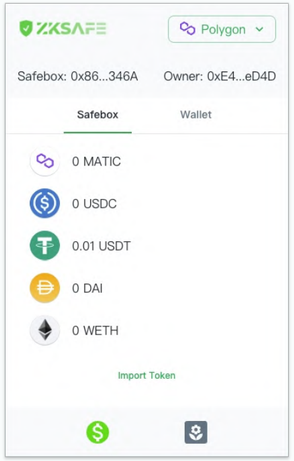
in any webs(eg. web in WeChat),
get ZKSAFE(Single Password) anywhere

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

Roadmap







ecosystem support program

2022Q2
Won BNB Hackthon
Valuation:$8M

2022Q4
ZKSAFE Launch
Valuation:$12M

2023Q1
Password EIP
(in progress)

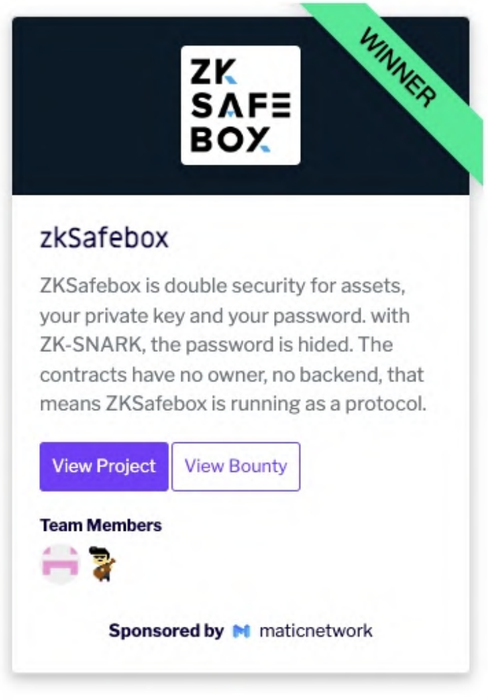
2023
BatchCall EIP
(AA extension)

2023
ZKSAFE ID

2023
ZKSAFE v2

Try Pitch

ZKSAFE



Try Pitch

ZKSAFE

Seed Round ($560K)

NGC ventures

Aperture

CATCHERVC

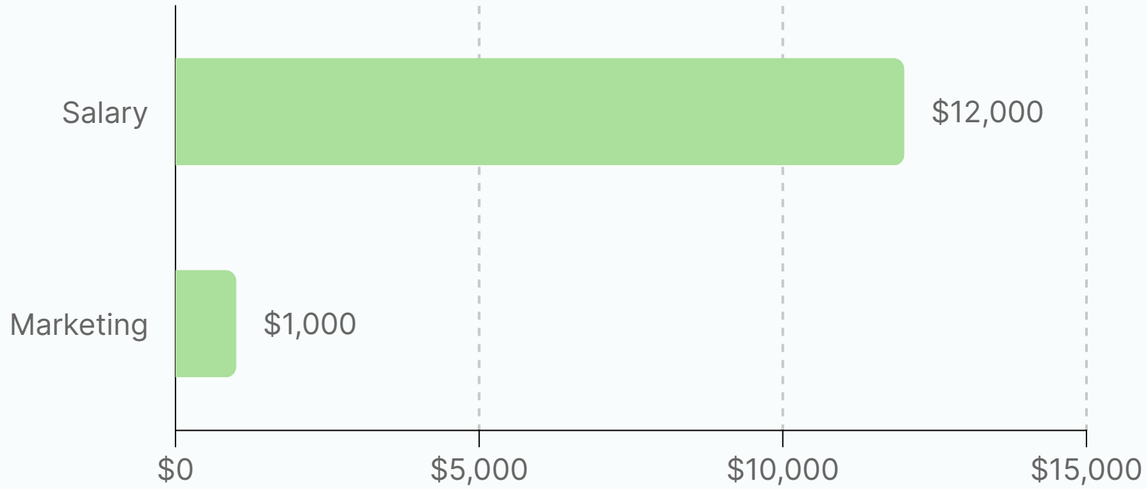
Betterverse Dao

Backers

ByteTrade

慢雾科技 SLOWMIST

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

ZKSAFE