THE WEB CONFERENCE 2023
AUSTIN, TEXAS, USA

THE WEB CONFERENCE ACM

Artifacts Available acm V1.1

Bad Apples: Understanding the Centralized Security Risks in Decentralized Ecosystems

Speaker: Kailun Yan

Kailun Yan[1]

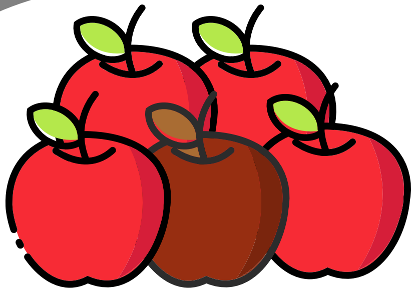
Jilian Zhang[2]

Xiangyu Liu[3]

Wenrui Diao[1] (✉)

Shanqing Guo[1]

1. Shandong University 2. Jinan University 3. Alibaba Group

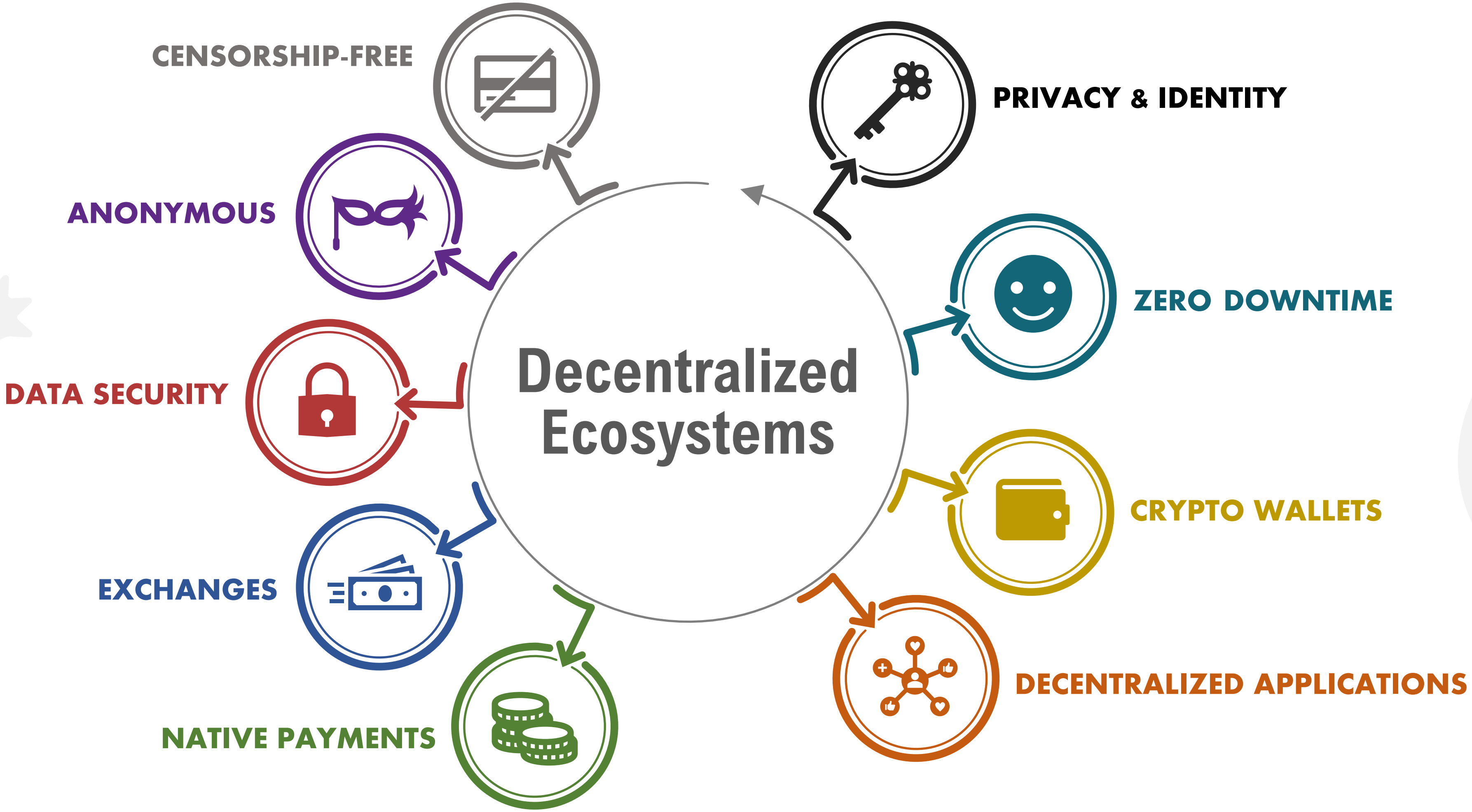


山东大学
SHANDONG UNIVERSITY

暨南大學
JINAN UNIVERSITY

Alibaba

● INTRODUCTION



Decentralized Ecosystems

CENSORSHIP-FREE

ANONYMOUS

DATA SECURITY

EXCHANGES

NATIVE PAYMENTS

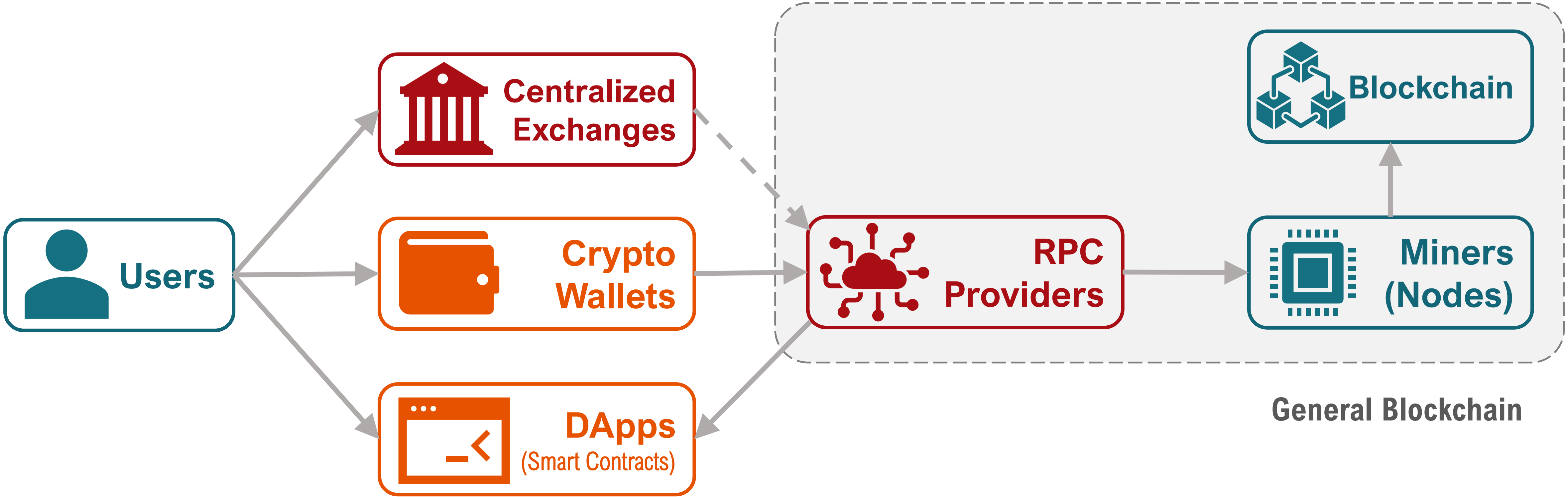
PRIVACY & IDENTITY

ZERO DOWNTIME

CRYPTO WALLETS

DECENTRALIZED APPLICATIONS

● INTRODUCTION



Basic components of a decentralized ecosystem

● RESEARCH OBJECTS

CRYPTO WALLETS

DECENTRALIZED APPLICATIONS

CENTRALIZATION

● THREAT MODEL

Decentralized platforms are benign, miners will not collude with each other.

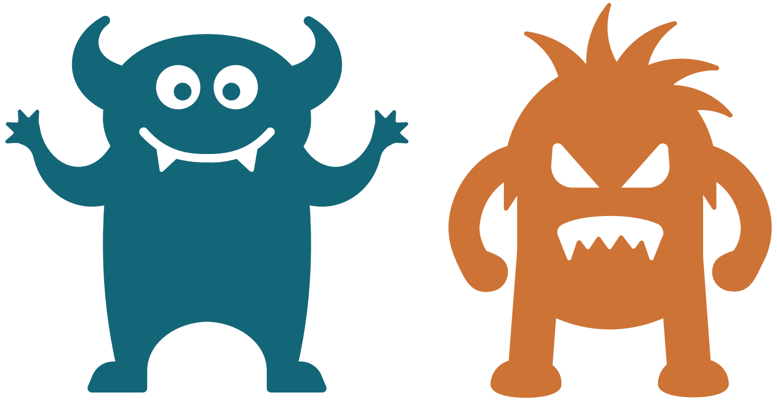
Decentralized service providers as adversaries.

- **First-party Centralization**

  The adversary integrates centralized services or backdoors into the decentralized service he developed.

- **Third-party Centralization**

  The adversary, as a third party, supplies centralized components for decentralized services to contaminate decentralized ecosystems.



● CRYPTO WALLETS

Slope Wallet Mobile Decentralized Exchange and Wallet

SENTRY Application Performance Monitoring and Error Tracking

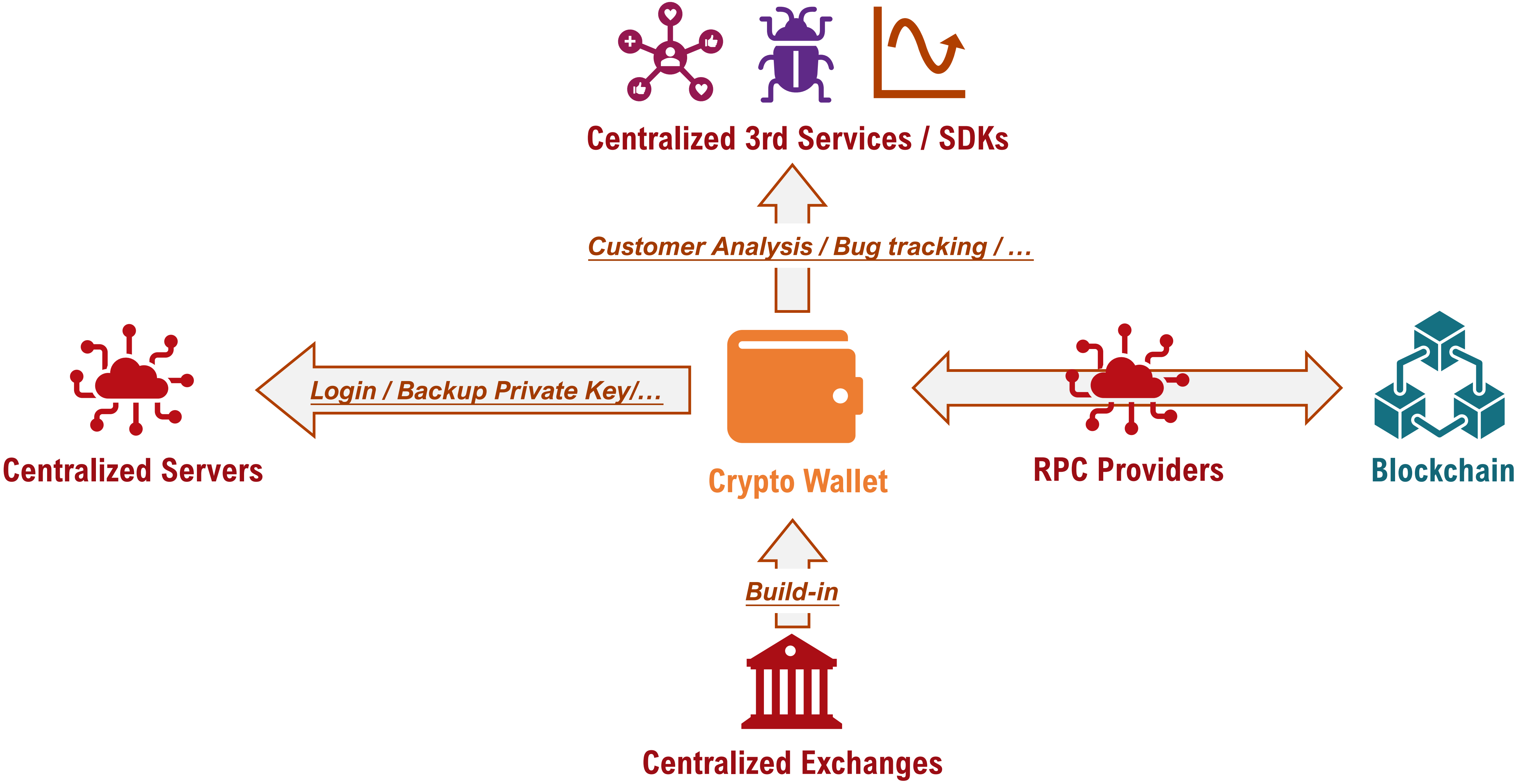
Slope used plaintext to transmit logs to Sentry!

9,231Wallets

$6,000,000

https://www.coindesk.com/business/2022/08/03/solanas-latest-6m-exploit-likely-tied-to-slope-wallet-devs-say/

● CRYPTO WALLETS


Centralized 3rd Services / SDKs
Customer Analysis / Bug tracking / …
Centralized Servers
Login / Backup Private Key/…
Crypto Wallet
RPC Providers
Blockchain
Build-in
Centralized Exchanges

● CRYPTO WALLETS

SR#1 Anonymity Loss

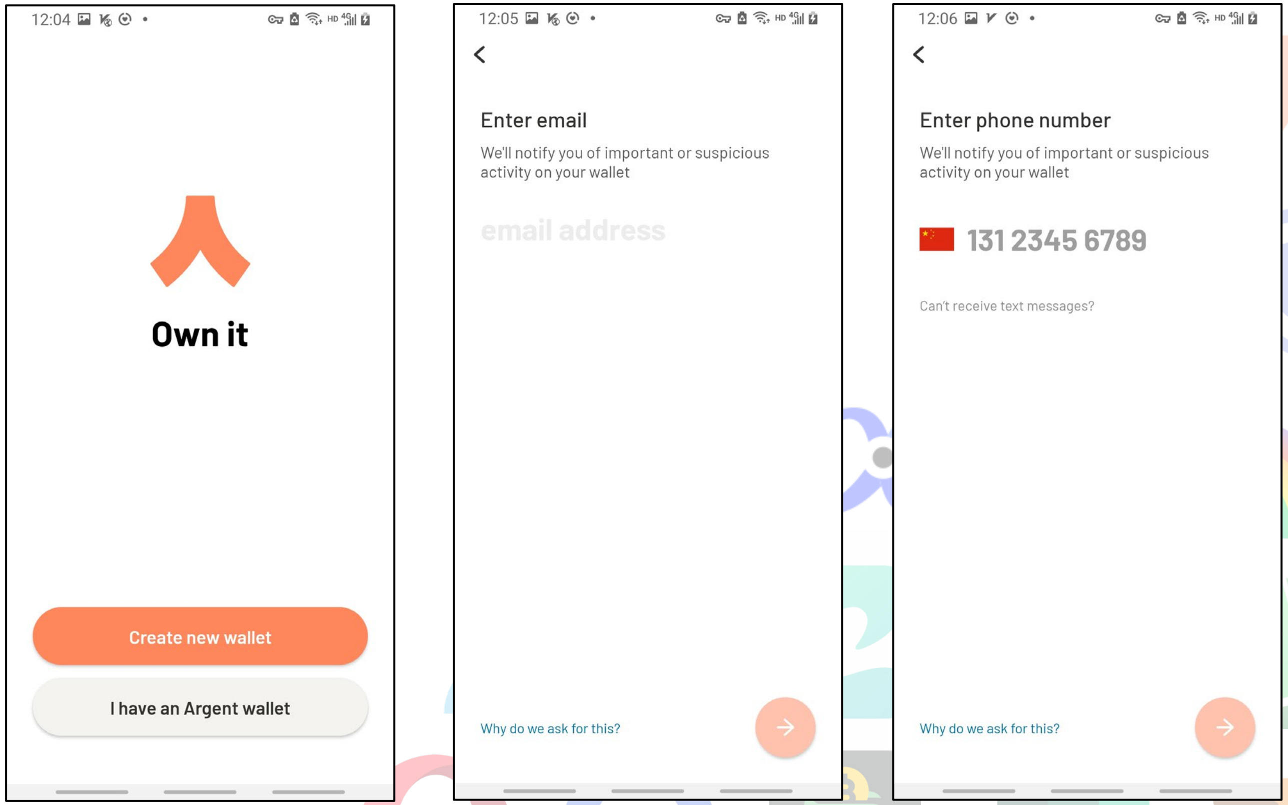
SR#2 Private Key Leakage

SR#3 Built-in Centralized Services

SR#4 RPC Services

SR#5 Third-Party SDKs

CENTRALIZED SECURITY RISKS



12:04

Own it

Create new wallet

I have an Argent wallet

12:05

Enter email

We'll notify you of important or suspicious activity on your wallet

email address

Why do we ask for this?

12:06

Enter phone number

We'll notify you of important or suspicious activity on your wallet

131 2345 6789

Can't receive text messages?

Why do we ask for this?

Argent Wallet

● CRYPTO WALLETS

SR#1 Anonymity Loss

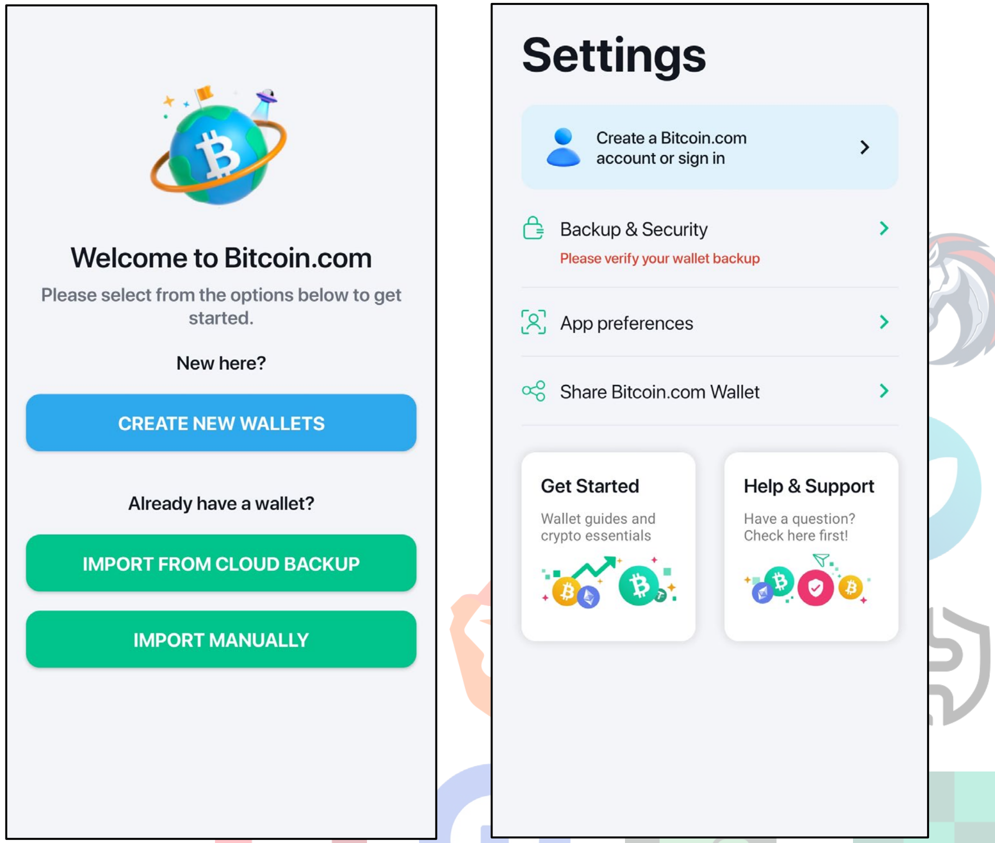
SR#2 Private Key Leakage

SR#3 Built-in Centralized Services

SR#4 RPC Services

SR#5 Third-Party SDKs

CENTRALIZED SECURITY RISKS



Welcome to Bitcoin.com

Please select from the options below to get started.

New here?

CREATE NEW WALLETS

Already have a wallet?

IMPORT FROM CLOUD BACKUP

IMPORT MANUALLY

Settings

Create a Bitcoin.com account or sign in

Backup & Security

Please verify your wallet backup

App preferences

Share Bitcoin.com Wallet

Get Started

Wallet guides and crypto essentials

Help & Support

Have a question? Check here first!

Bitcoin.com Wallet

● CRYPTO WALLETS

SR#1 Anonymity Loss

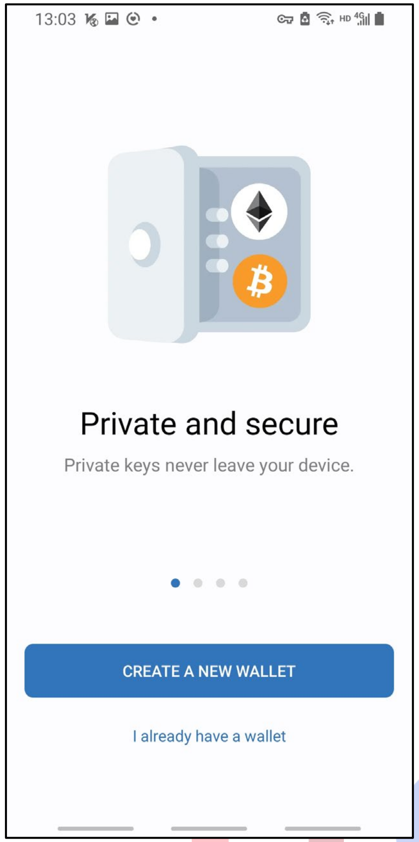
SR#2 Private Key Leakage

SR#3 Built-in Centralized Services

SR#4 RPC Services

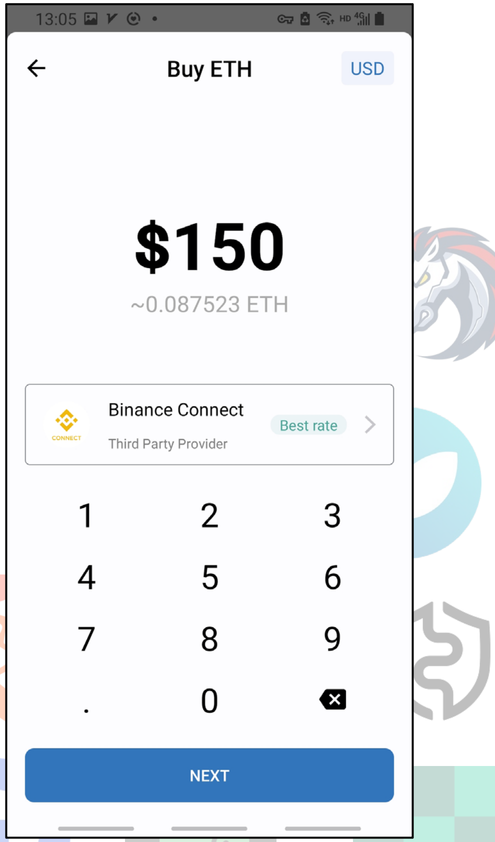
SR#5 Third-Party SDKs

CENTRALIZED SECURITY RISKS



Private and secure

Private keys never leave your device.



Buy ETH

$150

~0.087523 ETH

Binance Connect

Third Party Provider

Best rate

Trust Wallet

● CRYPTO WALLETS

SR#1 Anonymity Loss

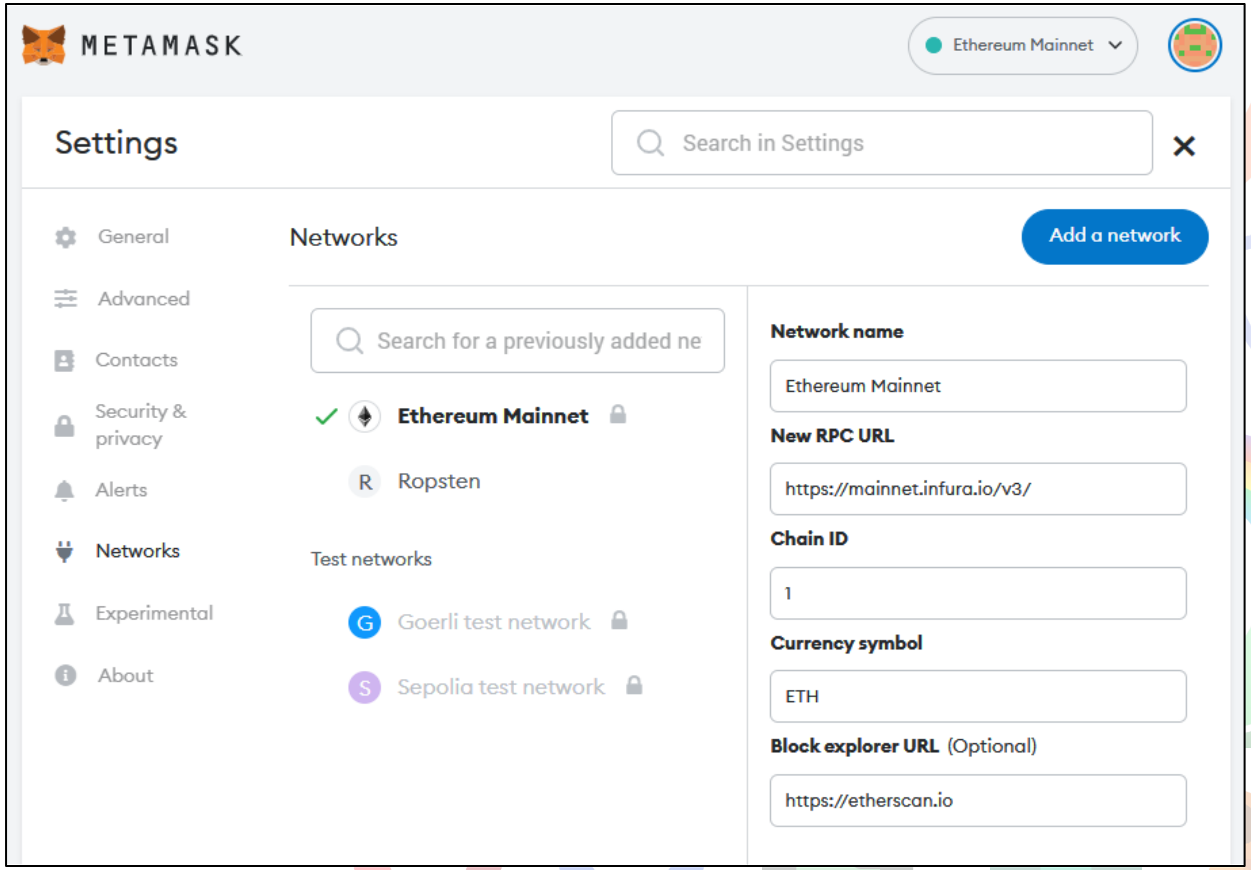
SR#2 Private Key Leakage

SR#3 Built-in Centralized Services

SR#4 RPC Services

SR#5 Third-Party SDKs

CENTRALIZED SECURITY RISKS



Network name
Ethereum Mainnet

New RPC URL
https://mainnet.infura.io/v3/

Chain ID
1

Currency symbol
ETH

Block explorer URL (Optional)
https://etherscan.io

Metamask Wallet

● CRYPTO WALLETS

SR#1 Anonymity Loss

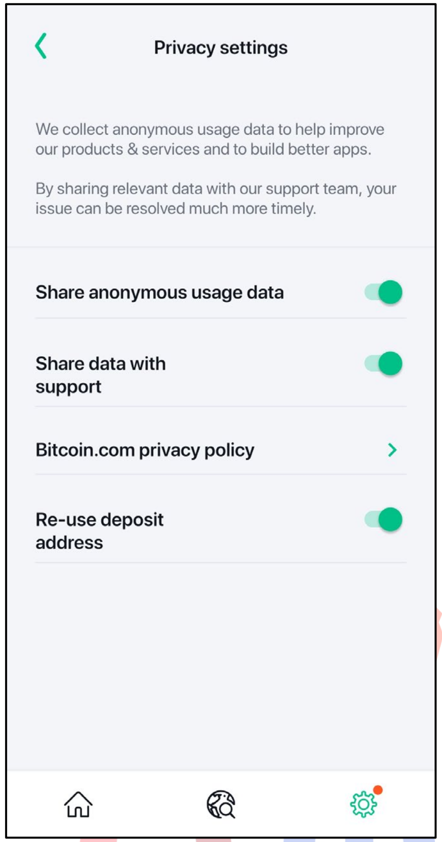
SR#2 Private Key Leakage

SR#3 Built-in Centralized Services

SR#4 RPC Services

SR#5 Third-Party SDKs

CENTRALIZED SECURITY RISKS



Privacy settings

We collect anonymous usage data to help improve our products & services and to build better apps.

By sharing relevant data with our support team, your issue can be resolved much more timely.

Share anonymous usage data ●

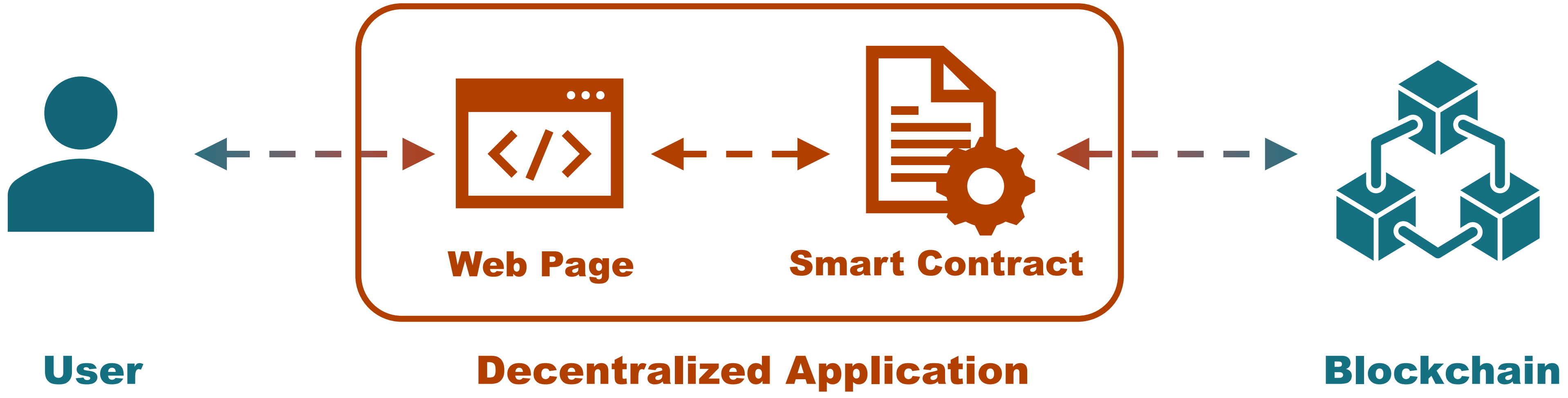
Share data with support ●

Bitcoin.com privacy policy >

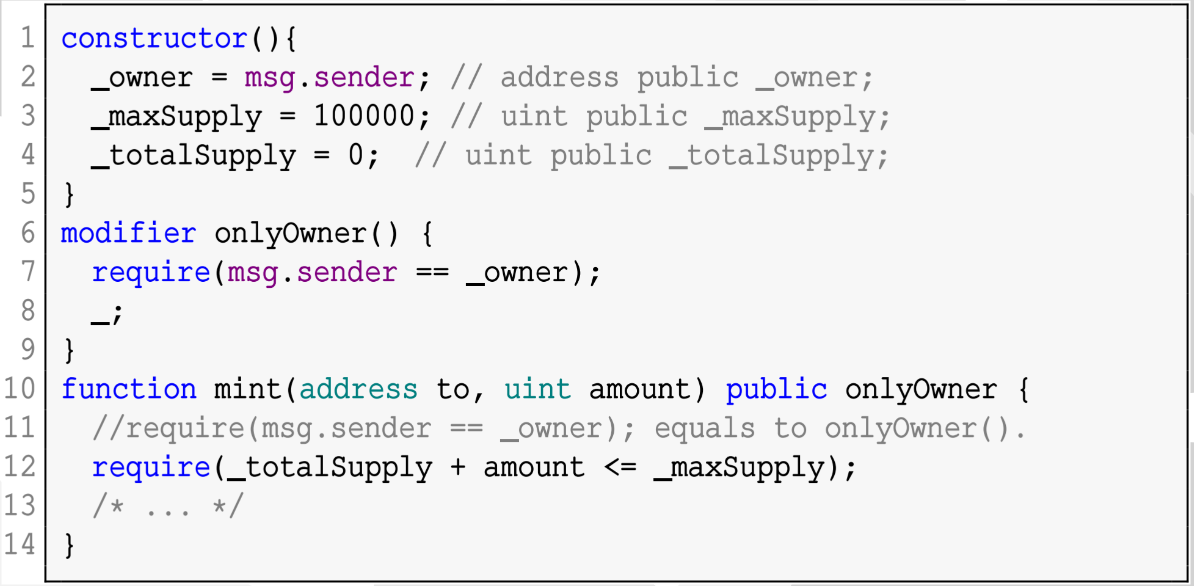
Re-use deposit address ●

Bitcoin.com Wallet

● DAPPS


Web Page
Smart Contract
User
Decentralized Application
Blockchain

● SMART CONTRACTS



```
constructor(){
  _owner = msg.sender; // address public _owner;
  _maxSupply = 100000; // uint public _maxSupply;
  _totalSupply = 0;  // uint public _totalSupply;
}
modifier onlyOwner() {
  require(msg.sender == _owner);
  _;
}
function mint(address to, uint amount) public onlyOwner {
  //require(msg.sender == _owner); equals to onlyOwner().
  require(_totalSupply + amount <= _maxSupply);
  /* ... */
}
```

Access Control

● SMART CONTRACTS

SR#6 Overpowered Owner

(a) Limited Liquidity

(b) Vulnerable Scarcity

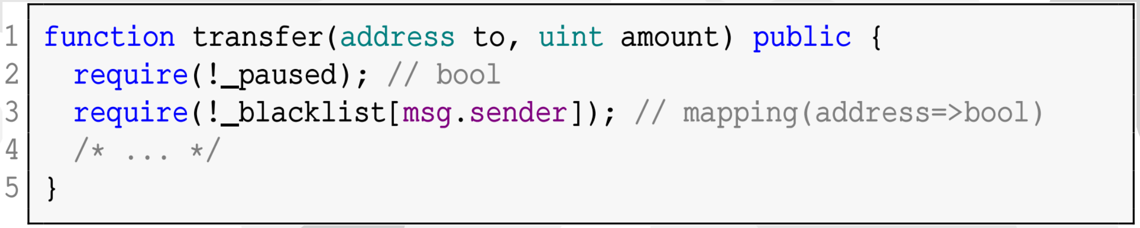
(c) Mutable Metadata

(d) Mutable Parameters

SR#7 Missing Events

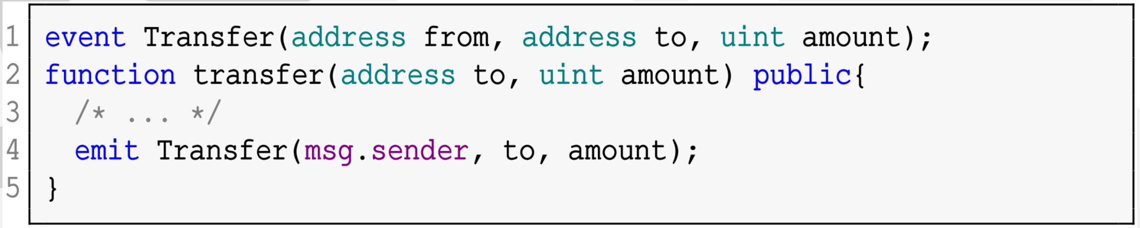
CENTRALIZED SECURITY RISKS

● SMART CONTRACTS



```
function transfer(address to, uint amount) public {
  require(!_paused); // bool
  require(!_blacklist[msg.sender]); // mapping(address=>bool)
  /* ... */
}
```

Limited Liquidity



```
event Transfer(address from, address to, uint amount);
function transfer(address to, uint amount) public{
  /* ... */
  emit Transfer(msg.sender, to, amount);
}
```

Event

SR#6 Overpowered Owner

- (a) Limited Liquidity
- (b) Vulnerable Scarcity
- (c) Mutable Metadata
- (d) Mutable Parameters

SR#7 Missing Events

CENTRALIZED SECURITY RISKS

● DETECTION APPROACHES

✓ Function Check. (SR#1~4)

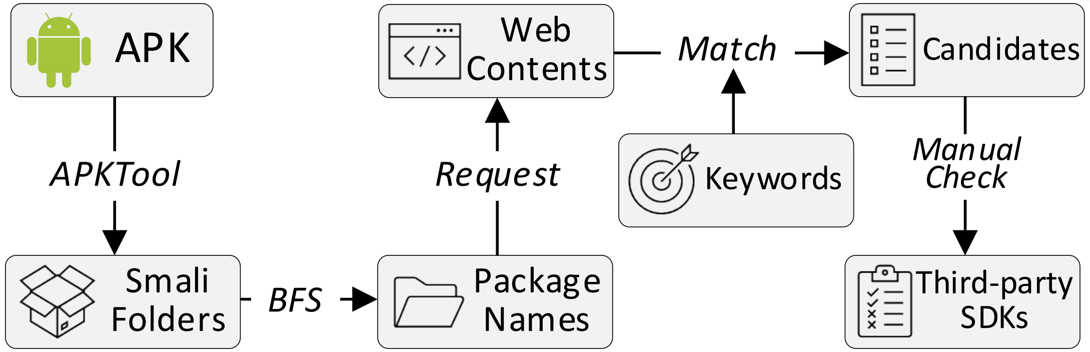
RQ1 Does the wallet require users to register or provide additional information before use? (**SR#1**)

RQ2 Does the wallet recommend users back up their private keys to the cloud? (**SR#2**)

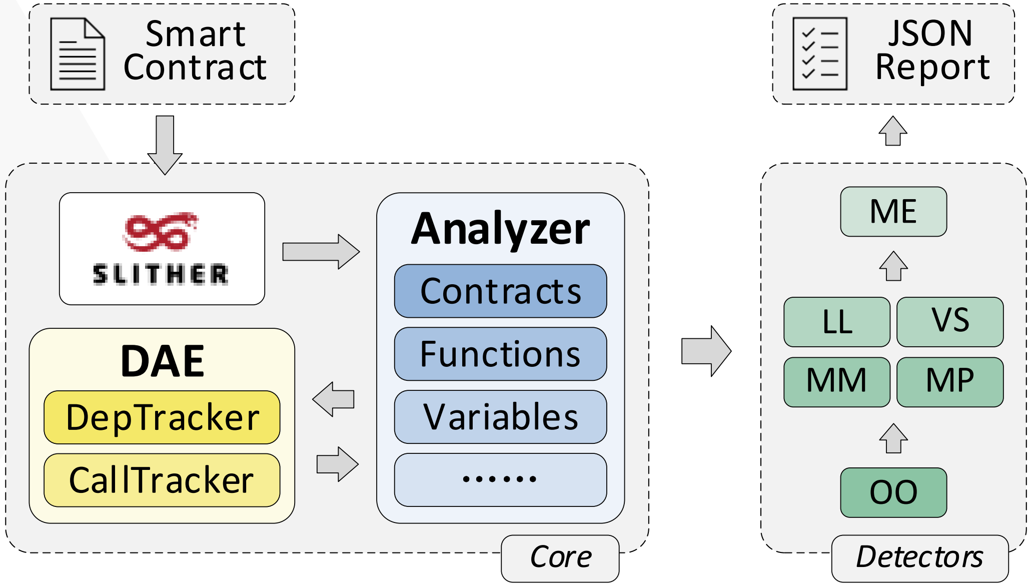
RQ3 Whether the wallet has built-in centralized services and reminds users that these services are not decentralized. (**SR#3**)

RQ4 Can users modify RPC providers in the wallet? (**SR#4**)

✓ Semi-Automated Detection. (SR#5)



✓ Automated Tool. (SR#6, SR#7)



NAGA

● DATASETS

28

Ethereum website recommended wallets

131M Downloads

Google Play

110,506

Ethereum on-chain contracts

11,753 High-value contracts

Total market cap exceeds **310B**

Etherscan

Ethereum Wallets: https://ethereum.org/en/wallets/find-wallet/
Contracts Dataset: https://github.com/d0scoo1/naga_contracts
Etherscan Token Tracker: https://etherscan.io/tokens
Smart Contract Sanctuary: https://github.com/tintinweb/smart-contract-sanctuary-ethereum

● FINDINGS

CRYPTO WALLETS

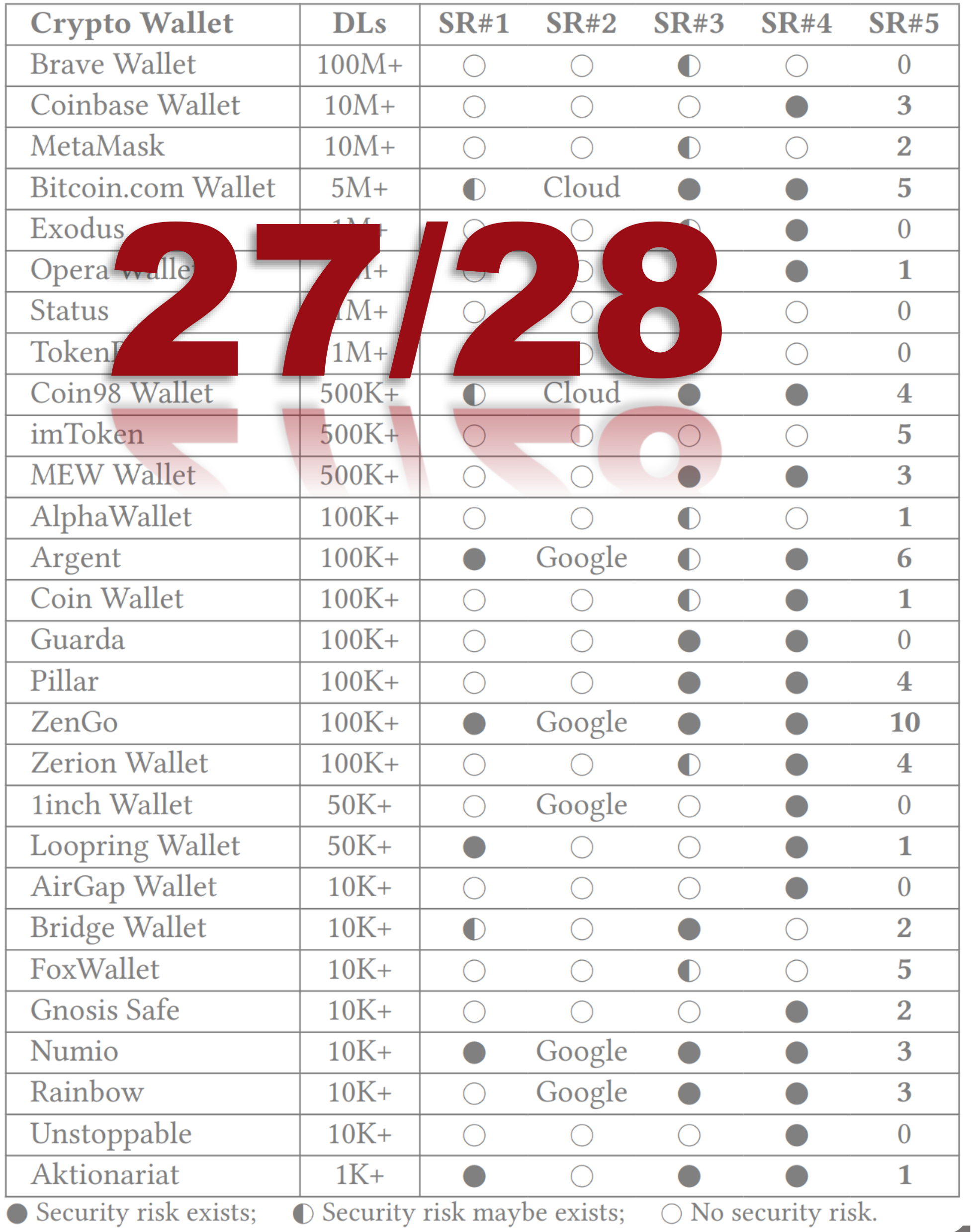
SR#1 Anonymity Loss (AL) **8/28**

SR#2 Private Key Leakage (PL) **7/28**

SR#3 Built-in Centralized Services (BS) **19/28**

SR#4 RPC Services (RS) **20/28**

SR#5 Third-Party SDKs (TS) **20/28**



27/28

Crypto Wallet	DLs	SR#1	SR#2	SR#3	SR#4	SR#5
Brave Wallet	100M+	○	○	◐	○	0
Coinbase Wallet	10M+	○	○	○	●	3
MetaMask	10M+	○	○	◐	○	2
Bitcoin.com Wallet	5M+	◐	Cloud	●	●	5
Exodus	1M+	○	○	◐	●	0
Opera Wallet	1M+	○	○	[illegible]	●	1
Status	1M+	○	○	[illegible]	○	0
TokenP[illegible]	1M+	[illegible]	○	[illegible]	○	0
Coin98 Wallet	500K+	◐	Cloud	●	●	4
imToken	500K+	○	○	○	○	5
MEW Wallet	500K+	○	○	●	●	3
AlphaWallet	100K+	○	○	◐	○	1
Argent	100K+	●	Google	◐	●	6
Coin Wallet	100K+	○	○	◐	●	1
Guarda	100K+	○	○	●	●	0
Pillar	100K+	○	○	●	●	4
ZenGo	100K+	●	Google	●	●	10
Zerion Wallet	100K+	○	○	◐	●	4
1inch Wallet	50K+	○	Google	○	●	0
Loopring Wallet	50K+	●	○	○	●	1
AirGap Wallet	10K+	○	○	○	●	0
Bridge Wallet	10K+	◐	○	●	○	2
FoxWallet	10K+	○	○	◐	○	5
Gnosis Safe	10K+	○	○	○	●	2
Numio	10K+	●	Google	●	●	3
Rainbow	10K+	○	Google	●	●	3
Unstoppable	10K+	○	○	○	●	0
Aktionariat	1K+	●	○	●	●	1

● Security risk exists; ◐ Security risk maybe exists; ○ No security risk.

FINDINGS

83.5%

SMART CONTRACTS

11,419

high value contracts

260 well-known contracts

$98B

Overpowered Owner

88.0%

Token contracts

MITIGATIONS

USERS

- Choose wallets with large downloads
- Not provide any information to wallets
- Hide the actual IP address by use onion routing
- Run own blockchain nodes

SR#1 Anonymity Loss
SR#2 Private Key Leakage
SR#4 RPC Services

DEVELOPERS

- Use decentralized services
- Fulfill obligation to inform users
- Connect to multiple RPC services simultaneously
- Multi-signature contract as the owner

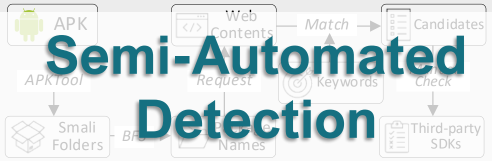
SR#3 Built-in Centralized Services
SR#5 Third-Party SDKs
SR#7 Missing Events
SR#4 RPC Services
SR#6 Overpowered Owner

● SUMMARY

1st
centralization

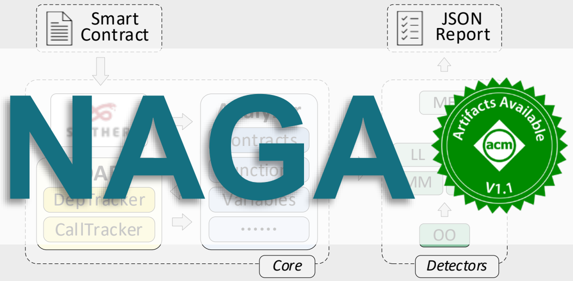
3rd
centralization

Function Check



Semi-Automated Detection

Centralized Security Risks in Decentralized Ecosystems



NAGA

SMART CONTRACTS

27/28
Crypto Wallets

83.5%
Smart Contracts

110,506
11,753
$98B
260 well-known token

Mitigation

Community Contributions

Bad Apples: Understanding the Centralized Security Risks in Decentralized Ecosystems

Kailun Yan, Jilian Zhang, Xiangyu Liu, Wenrui Diao, Shanqing Guo

Thanks!

Speaker: Kailun Yan

kailun@mail.sdu.edu.cn

https://dos.cool/

NAGA: https://github.com/d0scoo1/Naga

Contract Dataset: https://github.com/d0scoo1/naga_contracts