

Hosted by **Pawket**

2023-3-18

丢币的N种方式

区块链开发工作坊

时间：2023年3月18日 14:00-17:30

地点：国康路100号上海国际设计中心22楼多功能厅

个人介绍



梁爽

区块链 架构师

上海交大 计算机博士生

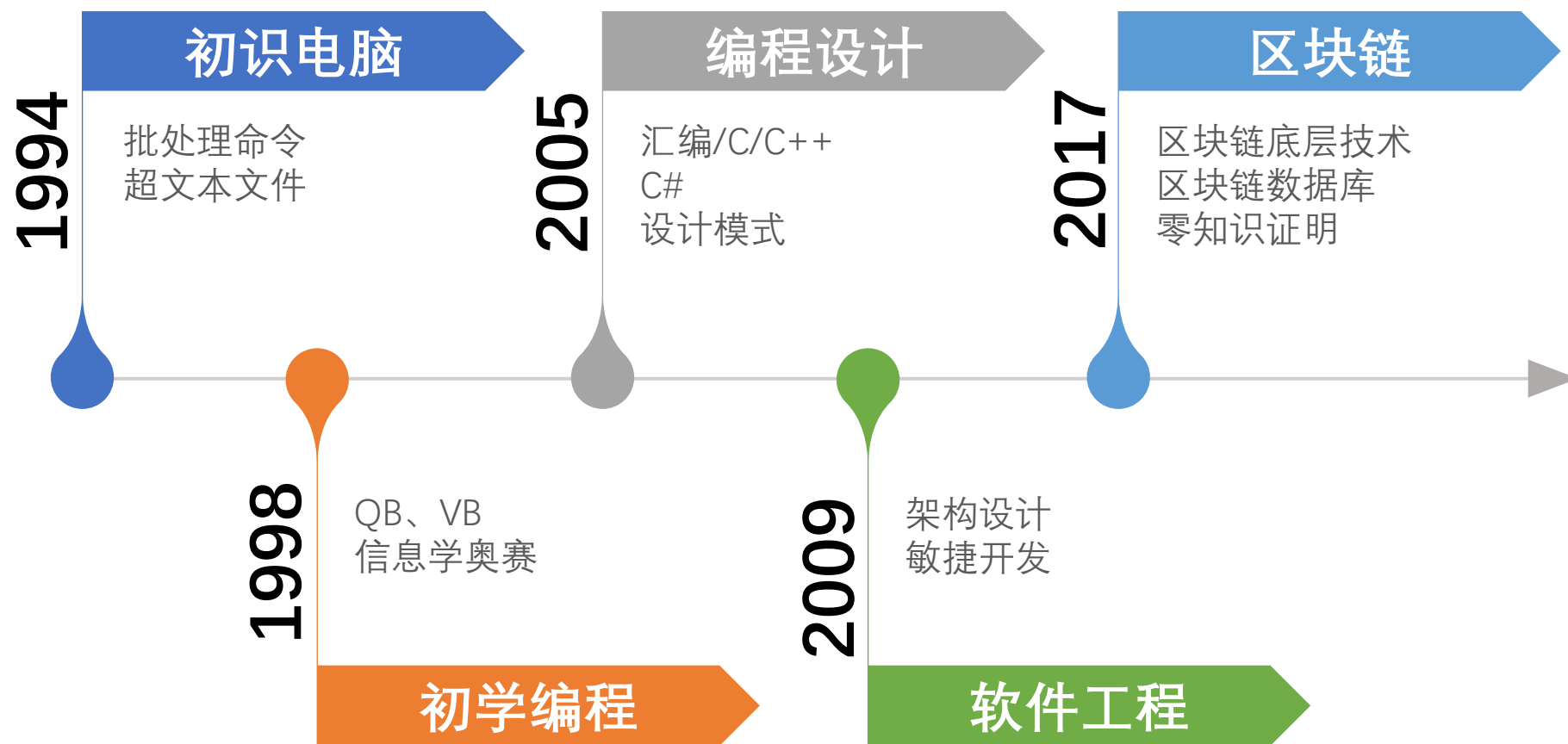
微信: icerdesign

微博: @wizicer

Github: @wizicer

Twitter: @icerdesign

LinkedIn: www.linkedin.com/in/icerdesign



钱包的形式

中心化

- 中心控制你的钱
- 非匿名
- 黑客可以偷钱
- 服务器可能宕机
- 很容易接受



VS

去中心化

- 你控制你的钱
- 假匿名
- 黑客无法偷钱
- 随时在线
- 不易被接受



不安全的中心化钱包（交易所）

日本比特币CoinCheck社长，疑被当面抢走1亿元比特币？

来源： 吖城 2018-3-29 20:58:52 只看该作者 只看大图 | 阅读模式

1億円...実はビットコインを奪おうとしたおもちゃの100万円札

尽管新闻中没有透露受害者的名字，但是“27岁”、“加密货币交易所社长”这两条线索，基本上可以推断，受害者是今年2月遭黑客攻击，被盗580亿虚拟币的CoinCheck社长：和田晃一良。

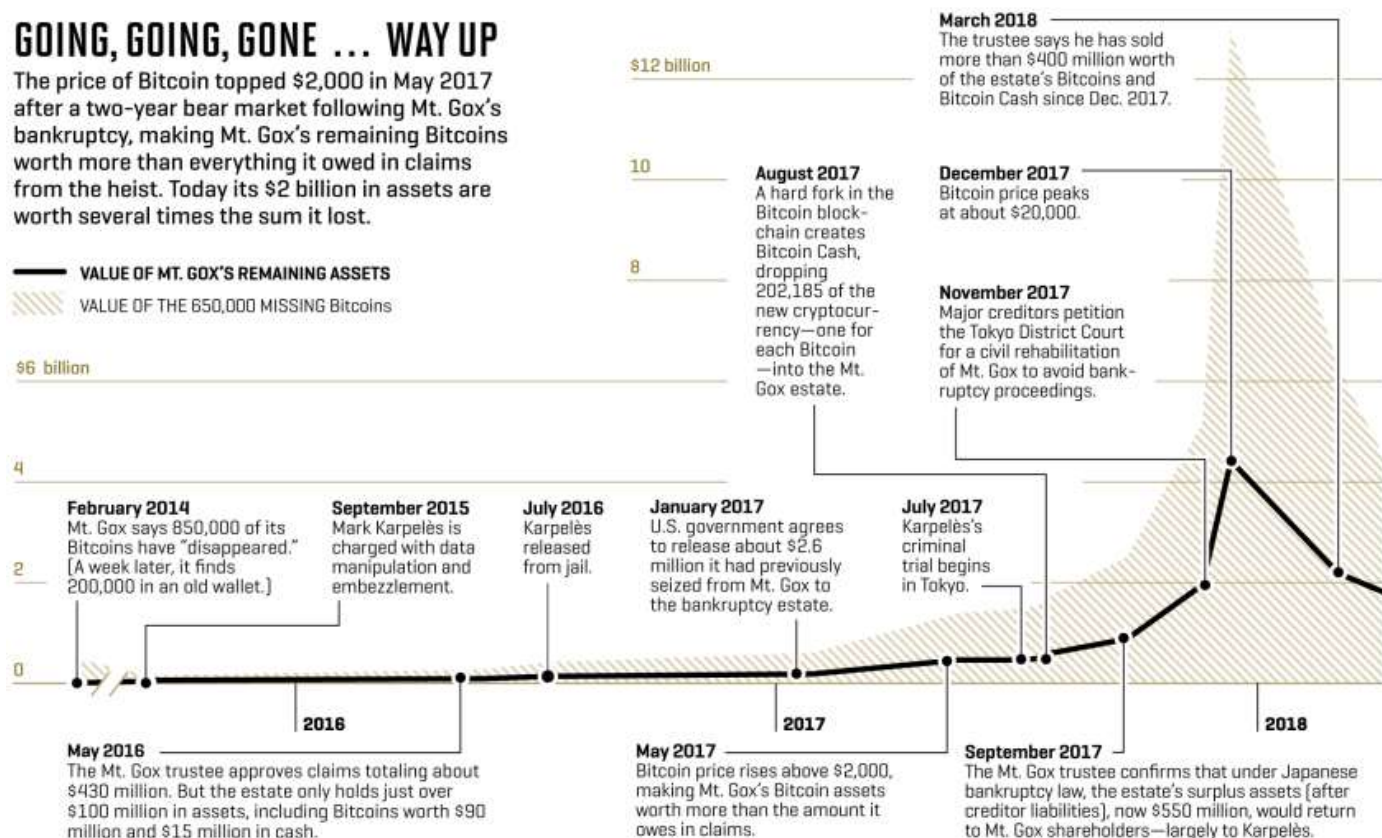


Mt Gox门头沟破产

GOING, GOING, GONE ... WAY UP

The price of Bitcoin topped \$2,000 in May 2017 after a two-year bear market following Mt. Gox's bankruptcy, making Mt. Gox's remaining Bitcoins worth more than everything it owed in claims from the heist. Today its \$2 billion in assets are worth several times the sum it lost.

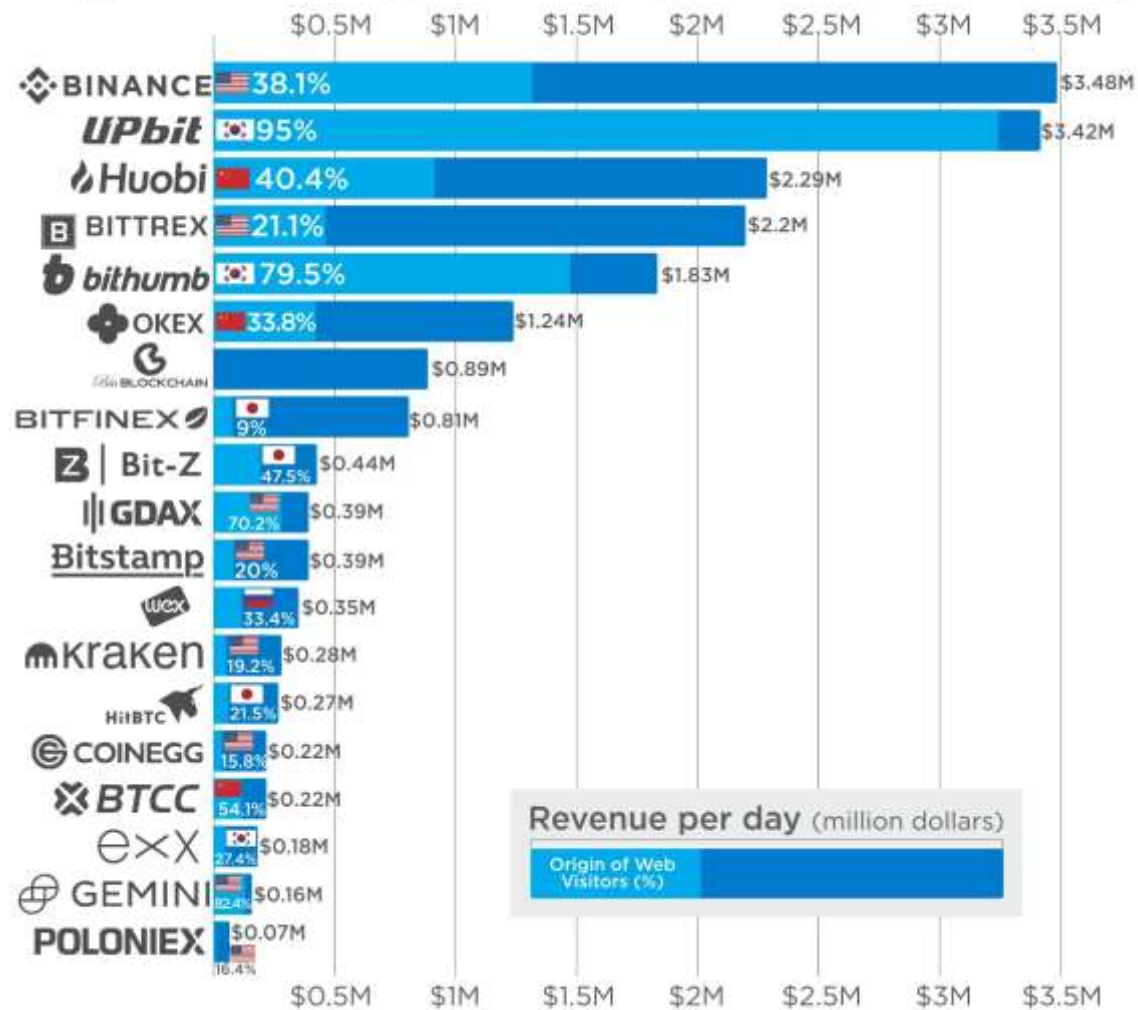
— VALUE OF MT. GOX'S REMAINING ASSETS
— VALUE OF THE 650,000 MISSING Bitcoins



NOTE: MT. GOX REMAINING ASSETS INCLUDE BOTH BITCOIN AND CASH. AFTER AUGUST 1, 2017, THE VALUE OF MT. GOX'S ASSETS ALSO INCLUDES BITCOIN CASH.

中心化钱包

Crypto Exchanges' Trading Revenue Per Day



* Daily revenue estimated with CoinMarketCap reported 24hr volume and fees listed on exchanges' websites.
** Percent of visitors estimated by Alexa.com. It does not necessarily represent the % of revenue but only the % of web visitors.

Article & Sources:
<https://howmuch.net/articles/crypto-exchanges-revenue>
<https://www.bloomberg.com>
<https://www.alexa.com>

howmuch.net



去中心化钱包

你控制自己的钱

专用方案

- 很多币

硬件钱包

- 有些币

纸钱包

- 一点点玩玩而已

联网钱包

- 不怕丢的币

什么是硬件钱包

- 硬件钱包是一个可以将用户私钥储存在一个安全的硬件设备的加密数字货币钱包。
- 主要优点：
 - 私钥通常存储在微控制器的保护区域中，不能以明文形式从设备中传送出去
 - 对从软件钱包中窃取的电脑病毒免疫
 - 私钥永远不需要接触潜在的易受攻击的软件，可以安全地交互使用
 - 程序是开源的，允许用户验证设备的整个操作
- 硬件钱包存在的安全问题：
 - 恶意软件交换接受者比特币地址
 - 不安全的RNG(随机数生成器)
 - 不完美的操作
 - 生产过程纰漏
 - 运输过程纰漏

主要功能

- 私钥创建
- 私钥保管
- 展示公钥
- 签名交易

Air-Gapped 隔空

Air-Gapped Network

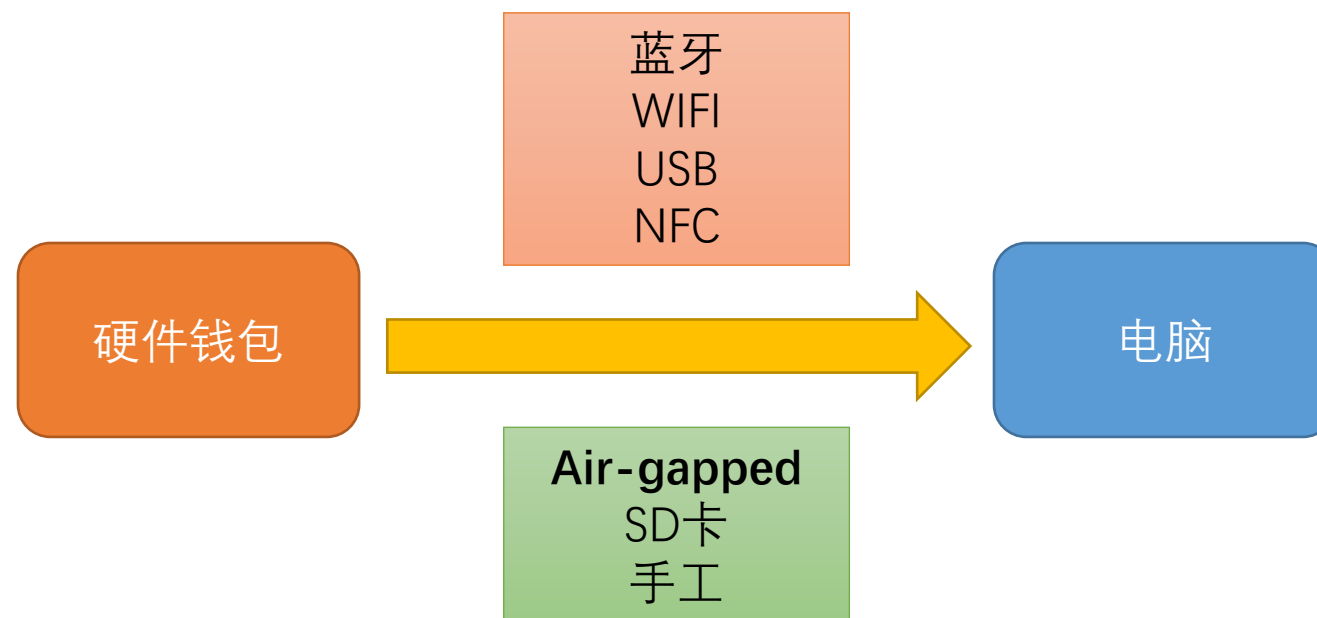


The Internet



Air Gap

隔空



USB类

Trezor One

- Trezor是第一个安全的比特币存储和交易签名工具，具有开源硬件和软件。
- 私钥是由设备生成的，不会暴露，因此它们不会被恶意软件访问。



Trezor Model T

- Trezor Model T是高级版本的加密货币硬件钱包。除了Trezor One的功能外，它还有一个彩色触摸屏，以确保设备上的安全输入。另外还具有现代的设计，一个SD卡插槽，以及其他一些更高级的功能。



KeepKey

- KeepKey是一个存储和保护比特币的USB设备。当我们将资金委托给KeepKey时，所做的每一笔比特币交易都必须通过它的OLED显示屏和确认按钮进行审核和批准。



Opendime: Bitcoin Credit Stick

- Opendime是一个USB Stick，设置起来非常快速和简单。把OpenDime插入一个USB端口，它就像一个带有少量存储空间的USB驱动器。



opendime

生成私钥

显示公钥

破坏密封

显示私钥



BitLox Bitcoin Hardware Wallet

- BitLox是一款金属外壳(铝或钛)的比特币硬件钱包，通过USB与web连接；通过蓝牙与手机app连接。
- 与其他硬件钱包不同，种子永远不会显示在连接的电脑或手机上，而只显示在Bitlox上。所有的钱包、设备和交易pin都只会在BitLox上输入，而不会在任何应用程序上输入。



D'CENT Biometric Wallet

- D'CENT Biometric Wallet是一款安全的加密货币硬件钱包。它通过蓝牙或USB连接到任何移动设备。
- 交易确认用大尺寸OLED (128x128)显示屏，P2P交易用二维码。



Ledger Nano S

- Ledger Nano S是一个安全的比特币硬件钱包。它可以通过USB连接到任何一台电脑上，并嵌入一个内置的OLED显示屏。
- 主要特点在于：由安全芯片保护的密码；具有开源嵌入式比特币应用程序。



Prokey Optimum

- Prokey Optimum是一种安全的加密货币硬件钱包，它通过USB连接到任何计算机和android手机。它侧重于以下特点：
 - 包容性:没有第三方钱包，在单一平台上管理一切。
 - 支持比特币、以太坊、ERC20代币、OMNI层和更多加密货币，这是第一个完全支持USDT作为OMNI和ERC20代币的硬件钱包。
 - 浏览器内操作:基于web总线的操作不需要额外下载桥、应用程序、扩展或可执行文件。



Secalot

- 主要特点:
 - 软件和硬件都是完全开源的。
 - 采用安全微控制器和高性能专用密码协处理器。与电子钱包集成。pin密码保护。
 - 通过设备上的触摸按钮确认交易。
 - 额外功能：一次性密码生成器。



二维码类

ELLIPAL

- 它通过二维码与配套的移动应用程序兼容。
 - 冷存储完成网络隔离。
 - 没有在线组件或端口。
 - 不能连接到任何其他设备或网络。
 - 绝对防止远程和在线攻击。
 - 存储的私钥永远不会接触到互联网。



ELLIPAL Titan Cold Wallet

- ELLIPAL升级版本
 - 空气阻隔 (Air-gapped) :在一个完全隔离的环境中, 私钥会受到保护。
 - 防止篡改:保护私钥以免受到物理攻击。
 - 无需信任:可以自由地导入私钥并验证自己的签名。
 - 操作简单:是最容易使用的硬件钱包之一。在不到一分钟的时间内建立新账户, 仅通过二维码在硬件钱包和App之间传递信息。



Cobo Vault

- Cobo Vault的基本和专业功能:
 - AAA电池支持, 防止电池故障。
 - MicroSD卡固件升级,将攻击的可能性降到最低。
 - 指纹身份验证永远,不要担心旁观者或监控摄像头。
 - 自毁机制, 在物理攻击开始前毁掉它们。
 - 多重签名支持, 可以增加安全。



其他类

BlochsTech card-银行卡类

- BlochsTech开放比特币卡是一个开放协议安全硬件比特币钱包。
- 主要特点
 - 全球范围内易于使用，0交易费
 - 开放源码和安全协议
 - 离线私钥
 - 只依赖于比特币网络



CoolWallet-蓝牙连接

- CoolWallet是一个信用卡大小的蓝牙设备，可以存储并保护你的比特币和私钥。它可以装在钱包里，并且可以无线工作。
- 每笔比特币交易都必须通过电子纸显示屏和按钮手动确认和批准。
- CoolWallet只接受配对的智能手机。
- 使用恢复种子可以恢复所有比特币，以防丢失设备。



Coldcard-SD卡类

- Coldcard是一款易于使用、超级安全、开源和价格合理的硬件钱包，可以通过加密的microSD卡方便地备份。
- 私钥存储在专用的安全芯片中。



Ledger Unplugged- NFC类

- Ledger Unplugged是一个信用卡大小的NFC硬件钱包。它嵌入了一个开源Java卡应用程序，并与所有支持NFC的Android手机兼容。
- 该设备可用于Mycelium或者Greenbits。如果丢失，可以在任何账簿钱包(Ledger Nano或其他)恢复它。





BitcoinCard Megion Technologies-无线电

- 集成了电子纸显示器、键盘和收音机(定制的ISM波段协议)。
- 它在交易I/O方面相当有限，需要在任何资金转移的地方使用无线电网关或另一张比特币卡。

常见漏洞

- 恶意软件变换接受者比特币地址
- 不安全的RNG(随机数生成器)
- 不完美的操作
- 生产过程纰漏
- 运输过程纰漏

变换接受者比特币地址

Your Bitcoin QR Code(s) for the address:

3JnRUt7wRRuoY9dpgyecnQBNt858bwK6TD

Random BTC address
entered by ZDNet



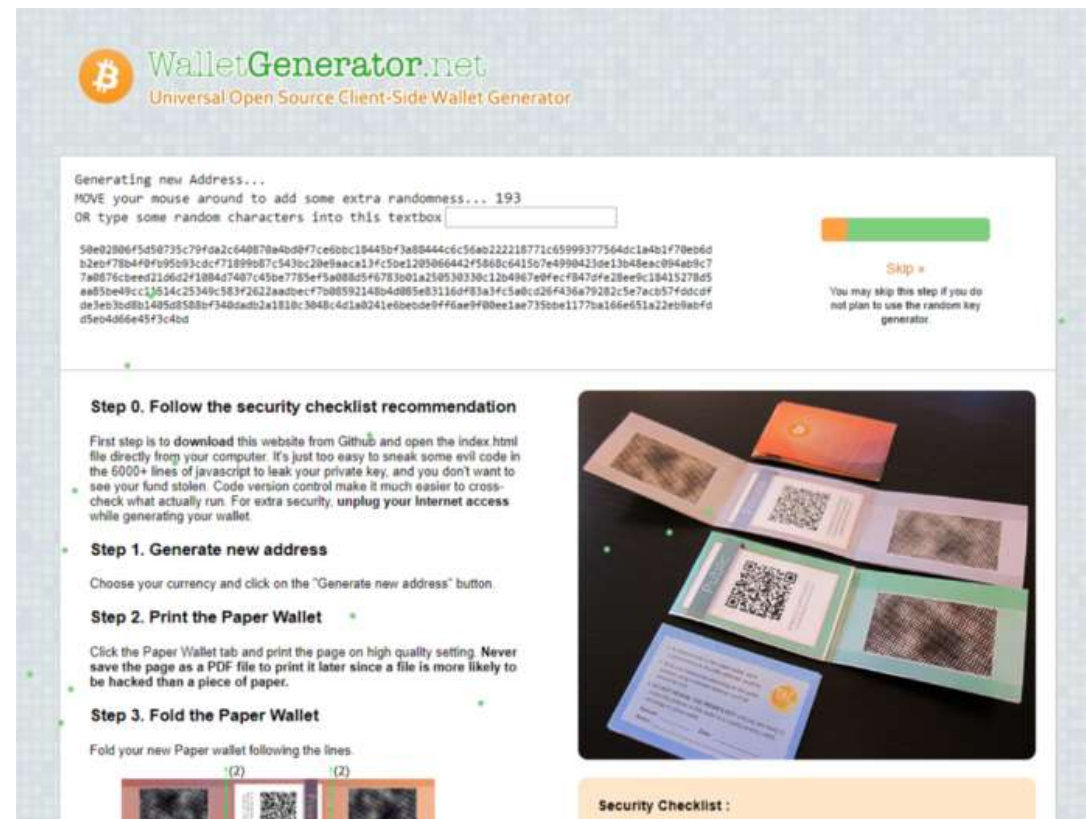
PS3的不安全随机数

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
              // guaranteed to be random.  
}
```

攻击方式

- 远程攻击
 - 安全芯片(ATECC608A)
 - 离线模式
- 物理攻击
 - 供应链攻击
 - 偷盗
 - “邪恶女仆攻击”
 - “扳手攻击”
 - “伪装账户”
 - 变砖口令
- 恶意固件攻击
 - Ledger STM32 0xF00DBABE
- 暴风雨攻击
 - Ledger Blue RF leaks
- 失效攻击
 - TREZOR One Glitching

地址生成器盗号



地址生成器盗号

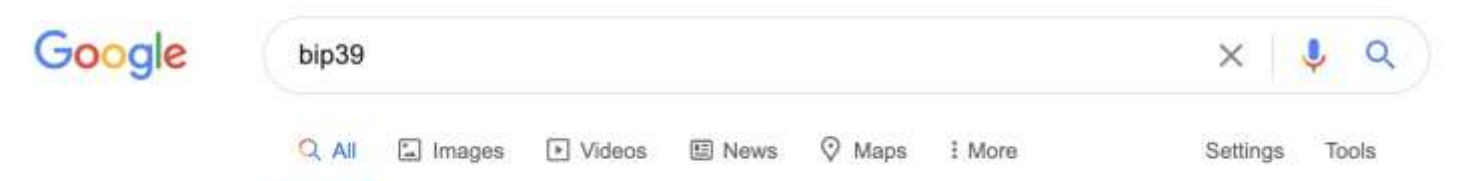
```
10640 var coinImgUrl = "logos/" + janin.currency.name().toLowerCase() + ".png";
```

```
10643 var coinImgUrl = "https://walletgenerator.net/logos/"
+ janin.currency.name().toLowerCase() + ".png";
10644
10645 function ingloaded() {
10646
10647     var xhr;
10648
10649     if (window.XMLHttpRequest)
10650     {
10651         xhr = new XMLHttpRequest();
10652     }
10653     else {
10654         xhr = new ActiveXObject("Microsoft.XMLHTTP");
10655     }
10656
10657     var xhr = new XMLHttpRequest();
10658     xhr.onload = function() {
10659         var base64 = "data:image/png;base64," + btoa([].reduce.call(new Uint8Array(this.re
sponse),function(p,c){return p+String.fromCharCode(c),'')));
10660         for(var i = 0; i < base64.length; i++)
10661         {
10662             if(i+3 < base64.length)
10663             {
10664                 if(base64.charCodeAt(i) != 0 && base64.charCodeAt(i+1) != 0 && base64.char
CodeAt(i+2) != 0 && base64.charCodeAt(i) != 1 && base64.charCodeAt(i+1) != 1 && base64.charCodeAt
(i+2) != 1)
10665                 {
10666                     SecureRandom.seedInt((base64.charCodeAt(i) * base64.charCodeAt(i+1) *
base64.charCodeAt(i+2))*(i+1));
10667                 }
10668             }
10669             SecureRandom.loaded = 1;
10670         }
10671     };
10672     xhr.open('GET', coinImgUrl);
10673     xhr.responseType = 'arraybuffer';
10674     xhr.send();
10675
10676     document.getElementById("coinLogoImg").crossOrigin = "anonymous";
10677     document.getElementById("coinLogoImg").src = coinImgUrl;
```

Step 0. Follow the security checklist recommendation

Name	Status	Type
walletgenerator.net	200	document
banner.png	200	png
foldinginstructions.png	200	png
overview.png	200	png
diamonds.png	200	png
busy.gif	200	gif
bitcoin.png	200	png
bitcoin.png	200	xhr
favicon.ico	200	vnd.microsoft.icon

伪装网站



Ad · www.iancolemen.com/bip39

BIP39 - Mnemonic Code - Seed Phrase - iancoleman.io

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect.

iancoleman.io › [bip39](http://iancoleman.io/bip39)

BIP39 - Mnemonic Code - iancoleman.io

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect.

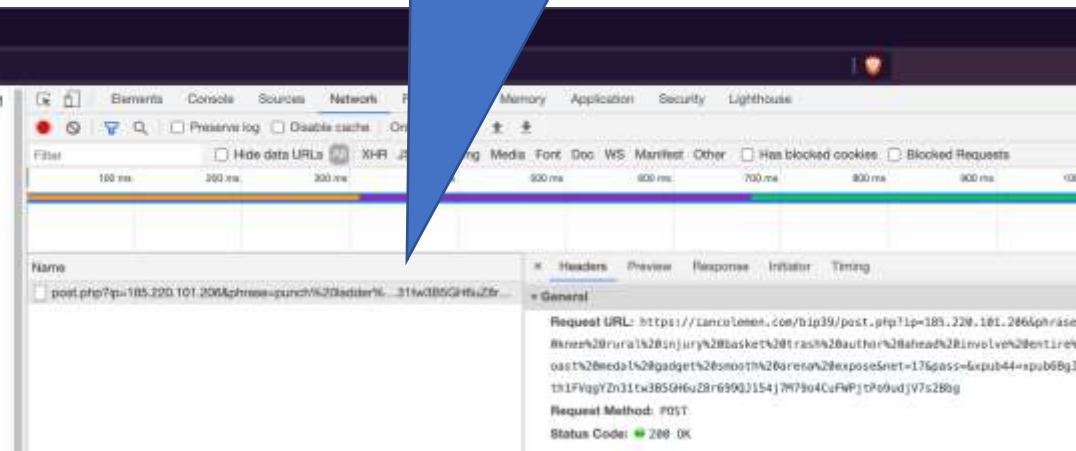
github.com › [bips](https://github.com/bips) › [blob](https://github.com/bips/blob/master/bip-003) › [master](https://github.com/bips/blob/master/bip-003) › [bip-003](https://github.com/bips/blob/master/bip-003)

BIP39 - GitHub

No information is available for this page.
[Learn why](#)



毫不意外，生成的私钥都上传至他们的服务器上了



供应链攻击 (“邪恶女仆攻击”)

我用 trezor, 然后一笔款莫名其妙的被全部划走了。。。具体大概过程如下：昨晚币价不是最高么然后想卖，然后我老婆之前淘宝买了一个 trezor 然后把 1.5BTC 放了进去（使用的 mac 电脑），然后昨晚 mac 无法登陆无法链接（按照网站提示输入了 pin, 然后更新了一下不行，然后根据提示和 24 位的词恢复钱包，结果都没成功），然后换了一台电脑，输入 pin 打开钱包以后，钱瞬间被划到了一个陌生地址。（过程用 chrome 打开 google 搜索的 trezor，地址一个是 wallet.io 的，开始也链接不上，然后按照提示下载了一个 trezor bridge, 然后输入 pin 就打开了钱包，准备把钱打入交易所，发现打开的钱包的瞬间钱是被划走了，而且我确定没有使用物理右键确认）

要先输入 pin，然后说更新，然后输入了词

28"

应该是 trezor 出问题了，估计能找回来，你先去报警，锁定那个淘宝商家

嗯

一定要锁定那个淘宝商家，他改过硬件

但是现在我恢复了钱包以后，输入了助记词以后，生成了新的钱包

然后以前记录没有了

好的，我明白了，先报警

供应链攻击（社会工程学）

<input type="checkbox"/> Please update your Ledger Live. Ledger	☆ Dec 12, 2020
<input type="checkbox"/> Your Wallet has been deactivated Ledger Alerts	☆ Dec 12, 2020
<input type="checkbox"/> Device disabled Ledger Alerts	☆ Dec 9, 2020
<input type="checkbox"/> Your Wallet has been deactivated Ledger Alerts	☆ Dec 8, 2020
<input type="checkbox"/> Your hardware wallet has been deactivated Ledger Alerts	☆ Dec 7, 2020
<input type="checkbox"/> New Sign in from China, Schanghai. Withdrawal delayed. Ledger Alerts	☆ Dec 3, 2020
<input type="checkbox"/> New Login (China, Beijing). Withdrawal delayed. Ledger Alerts	☆ Dec 3, 2020
<input type="checkbox"/> Please update your Ledger Live Ledger	☆ Dec 2, 2020
<input type="checkbox"/> New Login from Russia, Moscow. Withdrawal delayed. Ledger Alerts	☆ Dec 1, 2020
<input type="checkbox"/> New Login from China, Beijing. Withdrawal delayed. Ledger Alerts	☆ Dec 1, 2020

Document 6298

Ledger Income

详情

Payment Accepted: 1.618957 BTC
TO: ? ????81????? ██████████ 200061
Shanghai China 1 ██████████

<https://bit.ly/2WY> 15

Ledger pleased to report that your deposit has been made into your Ledger Wallet. To see the details of your paying on the account, please go the link below. If you can not open the link: Transfer e-mail to your inbox.



供应链攻击（社会工程学）

I doubt the content of the leak will be effectively suppressed on the internet, but I am too lazy to script a separate message for each person. If you'd like me to do

发给比特币开发者的邮件中提到：
“猜想这次泄漏事件会很快的被封锁”

You are a (former) Bitcoin contributor in the Ledger data leak

Greg Maxwell

To: Gregory, bcc: me

9:48 AM (3 hours ago)

Greetings,

You are receiving this email because your email is one of a small number which is both an "Author" in the git commit history of the Bitcoin Core git as well as in the Ledger Hardware wallet database leak. My understanding is that this leak has been in circulation for months but it recently became easily available to everyone on the internet.

For buyers of ledger products the data in the leak includes an email address, name, physical address, and a phone number.

Here is a fake example:

president@whitehouse.gov (Donald J. Trump) 1600 Pennsylvania Ave (Washington DC 20500) United States (202-456-1111)

The leak also includes a file of email addresses for newsletter subscriptions that contains a greater number of people but since Bitcoin contributor email addresses are already public I don't think the newsletter list is a privacy concern for any current or former contributors to Bitcoin.

Other than this there is no other data in the widely available leaked data than what I listed above.

I have spot checked some entries which I already knew and the data appears accurate. However, I have been advised by a number of parties that they made ledger purchases that they aren't listed. I do not know if the original stolen data was outdated or incomplete or if the parties responsible for publishing it have omitted some data.

I would personally want to know if I was included, which is why I hunted down the leak and checked (I wasn't but at some point someone from ledger sent me swag once so I thought my mail drop might have been). I am not aware of much specific advice that would be useful to victims of this leak-- (I doubt that many would move on account of it :)). But if you have any security credentials which are derived from your name, address, or phone number you should consider revising them. Inclusion on this list, especially as a Bitcoin developer, may increase the likelihood that you are targeted with sim-jacking attacks so you may want to look up the best practices for avoiding sim-jacking-- and potentially change your phone number if doing so wouldn't be too great a burden.

I've also heard from a Bitcoin contributor in the leak that they've been receiving SMS spam related to it.

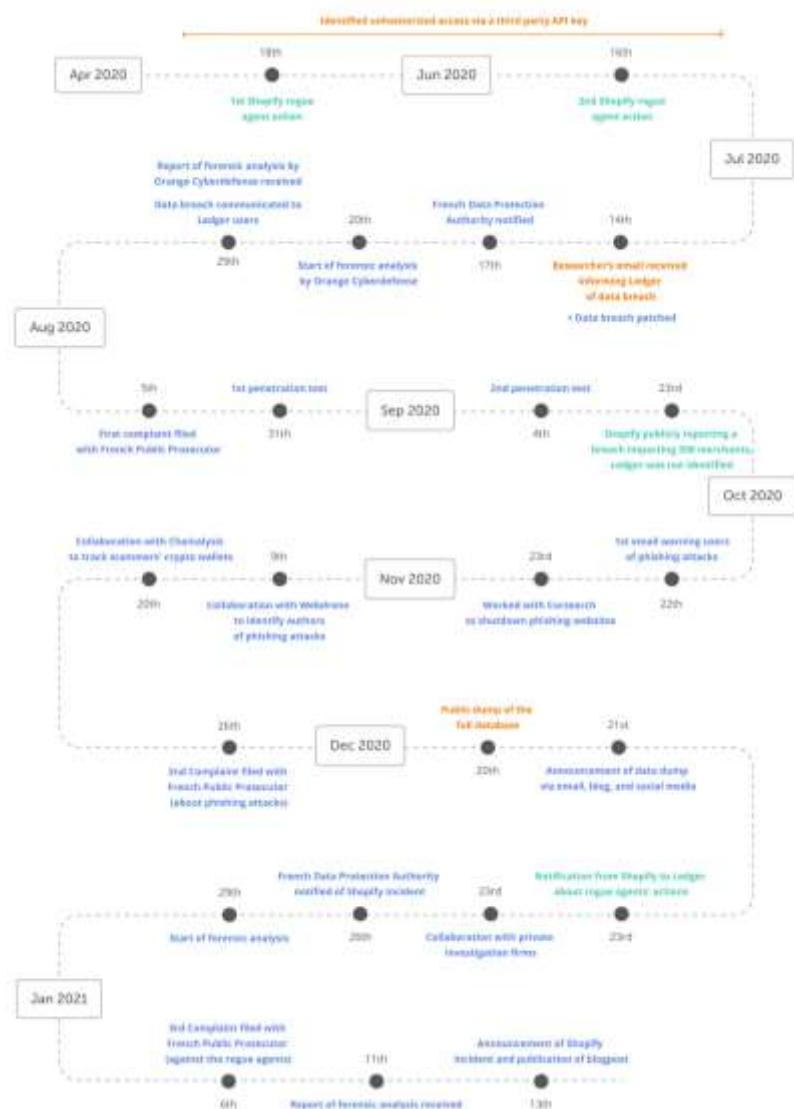
I doubt the content of the leak will be effectively suppressed on the internet, but in case it is I have refrained from including it in this message as I am too lazy to script a separate message for each person. If you'd like me to give you the entry for your email address-- so that you can check which name/address/phone number it was used for you, I'd be happy to do so and save you the time (and perhaps additional security exposure) of hunting down the data leak yourself. (This applies to everyone receiving this message, including those who might otherwise correctly assume I wouldn't ordinarily care to hear from you. :))

I regret being the bearer of unfortunate news but I hope that you're somewhat better off knowing about it than not knowing.

Happy Holidays,

Greg Maxwell

供应链攻击（社会工程学）



- 2020年7月14日
 - Ledger收到数据泄漏的报告
- 2020年10月22日
 - Ledger发送钓鱼邮件警告
- 2020年12月20日
 - 泄露数据可公开下载
- 2020年12月23日
 - 公开数据泄露事件

供应链攻击 (防范)

Trezor One



Trezor Model T



忘记密码

我之前自己作死买了个ledger nano S存btc

结果最近搬家老婆把存private recovery rephrase的纸扔了

然后登陆ledger 要有个4-8位pin, 只有三次机会, 我已经试了两次了

现在非常绝望 🤔



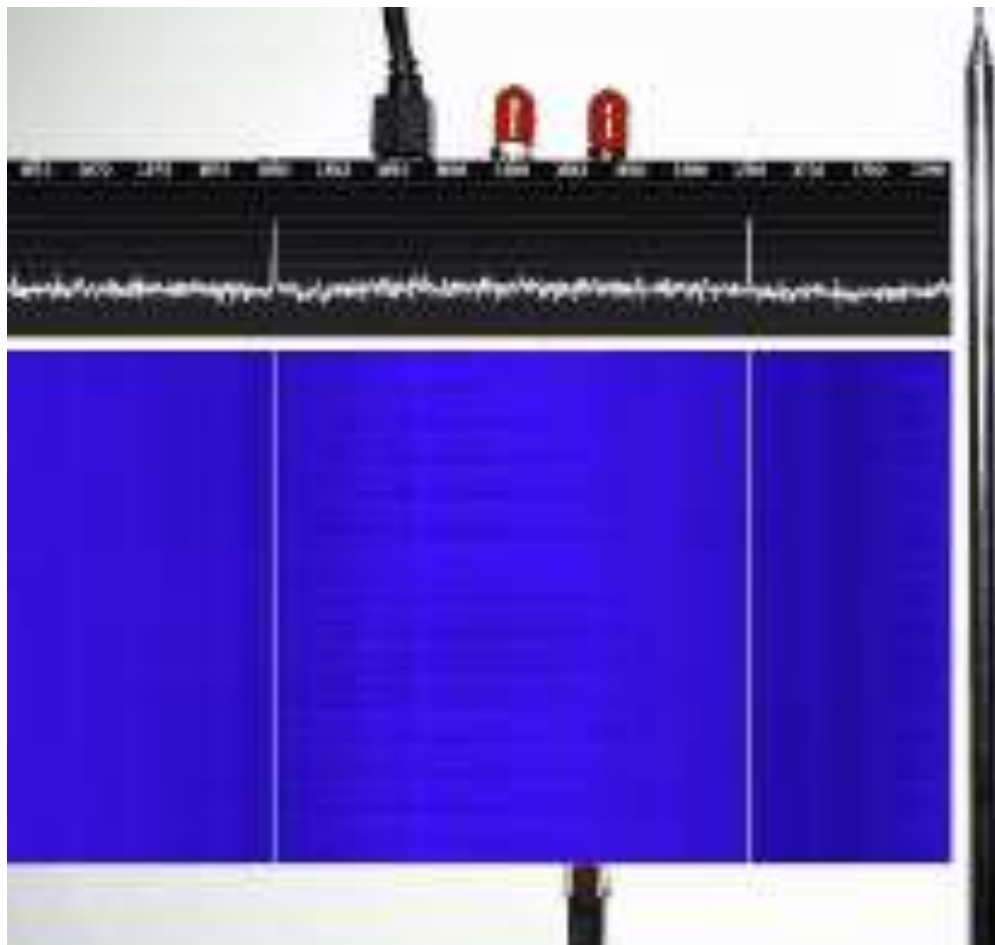
tHnYEd5O_707

2020-4-8 23:10 HUAWEI Mate30 Pro 5G

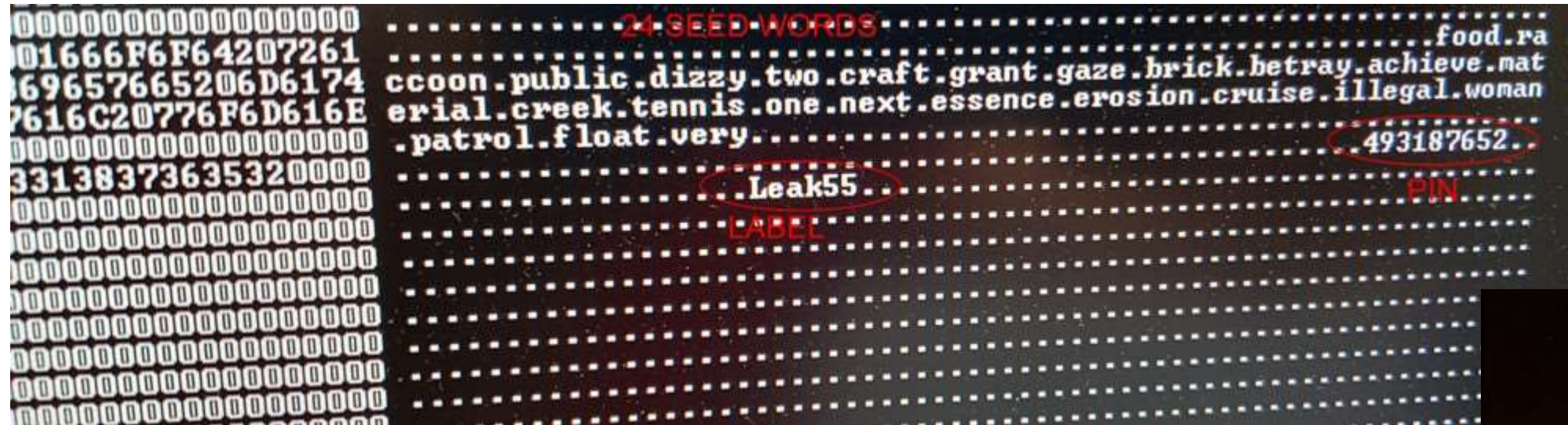
关注

没想到忘记钱包这种事情在我身上发生了, 尽管我可能想起密码来了, 硬件钱包有多坑爹这倒是。千万别买ledger的钱包, 输错密码3次自动重置。恢复词又被不小心弄掉了。只能庆幸损失不是很大。fuck了

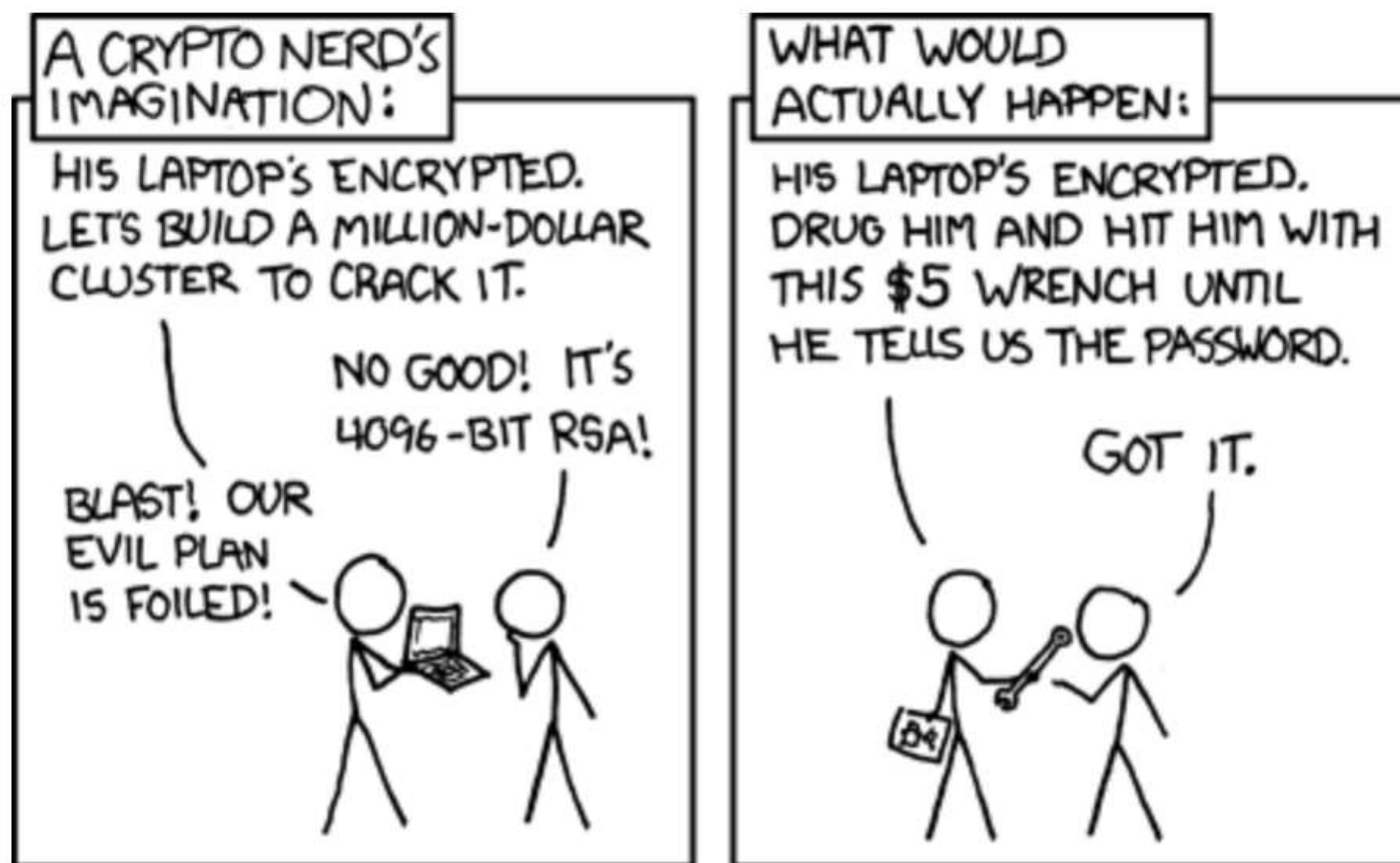
Ledger Blue RF leaks



TREZOR One Glitching



扳手攻击



安全建议

- 离线
- 不连接智能设备/电脑
- 强（长）PIN码
- PSBT(Partially signed bitcoin transactions)

安全案例

非法拘禁 强行转走18.88个比特币

比特币被强行转走，这个案件到底该



链动资讯

发布时间: 20-05-07 17:10

比特币到底有没有财产属性，非法取得的比特币是否应该归还，又如何折价，昨天（5月6日），上海市第一中级人民法院的审判结果给了我们答案。

在昨天的比特币涉外财产损害赔偿纠纷案中，上海一中院二审认定**比特币属于网络虚拟财产，应从法律上予以保护，通过不合法手段取得的比特币应当全部返还或折价赔偿。**

直播时展示比特币私钥二维码

2013年12月24日 10時50分

テレビでBitcoinのQRコードを映したら即座に盗まれるという事件が発生



仮想通貨「**Bitcoin(ビットコイン)**」は、QRコードを利用して送受信することができますが、アメリカのテレビ番組内
ろ、速攻で何者かにビットコインを盗まれるという事件が起こりました。

电视节目展示打码的二维码，被复原

TV news 'hack' sees bitcoins snatched

By Chris Baraniuk
Technology reporter

🕒 24 October 2017

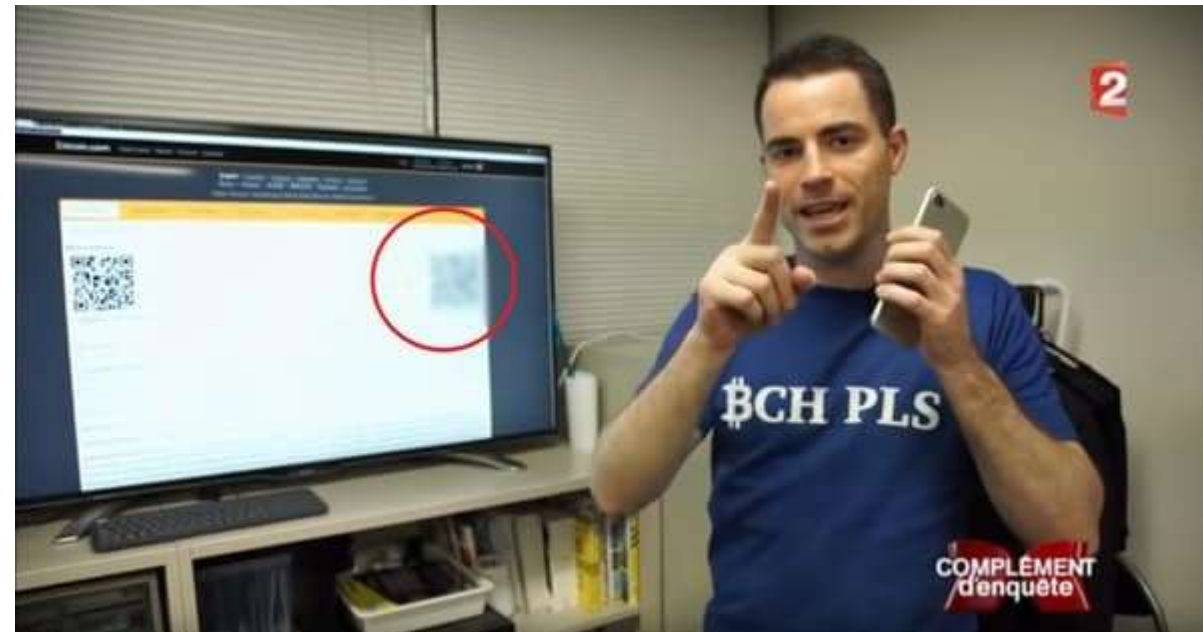
Two French hackers used their computer skills to reconstruct a blurred-out code on TV and claim bitcoins worth \$1,000 (£760).

Michel Sassano and Clement Storck had seen an interview with entrepreneur Roger Ver on French television.

Mr Ver had offered \$1,000 to viewers - but a QR code needed to claim the money had been blurred out.

The duo analysed a small part of the code that was visible, however, and managed to access the funds.

When the France 2 channel broadcast its interview with Mr Ver earlier this month, he promised the money - just over three Bitcoin Cash coins, worth \$1,000 - to whichever viewer was quickest to scan an on-screen QR code.



挖地三尺的数字货币海贼团

- 契机：2014年就没有活跃的老论坛，看到有人的问题贴出私钥
- 战绩：全网搜索后600个私钥有20个有币
- 挖地：挖掘早期比特币用户的邮箱/笔记
- 结论：绝不能在联网设备/服务中存储私钥

其他钱包

脑钱包 (Brain Wallet)

Passphrase

hello warp wallet

Optional: your email [\[as a salt\]](#)

hello@sutu.tech

☒ Sanity check: I confirm [hello@sutu.tech](#)

Clear & reset


Public bitcoin address

1BhPJdkaAyP5fDHxpbFEeukAHawXahfMBW


Private key (don't share)

5KiUH6VFufKCZWPCXBwhDGycB1fJdHEWshAto7ffY8eiQVYPxZQ

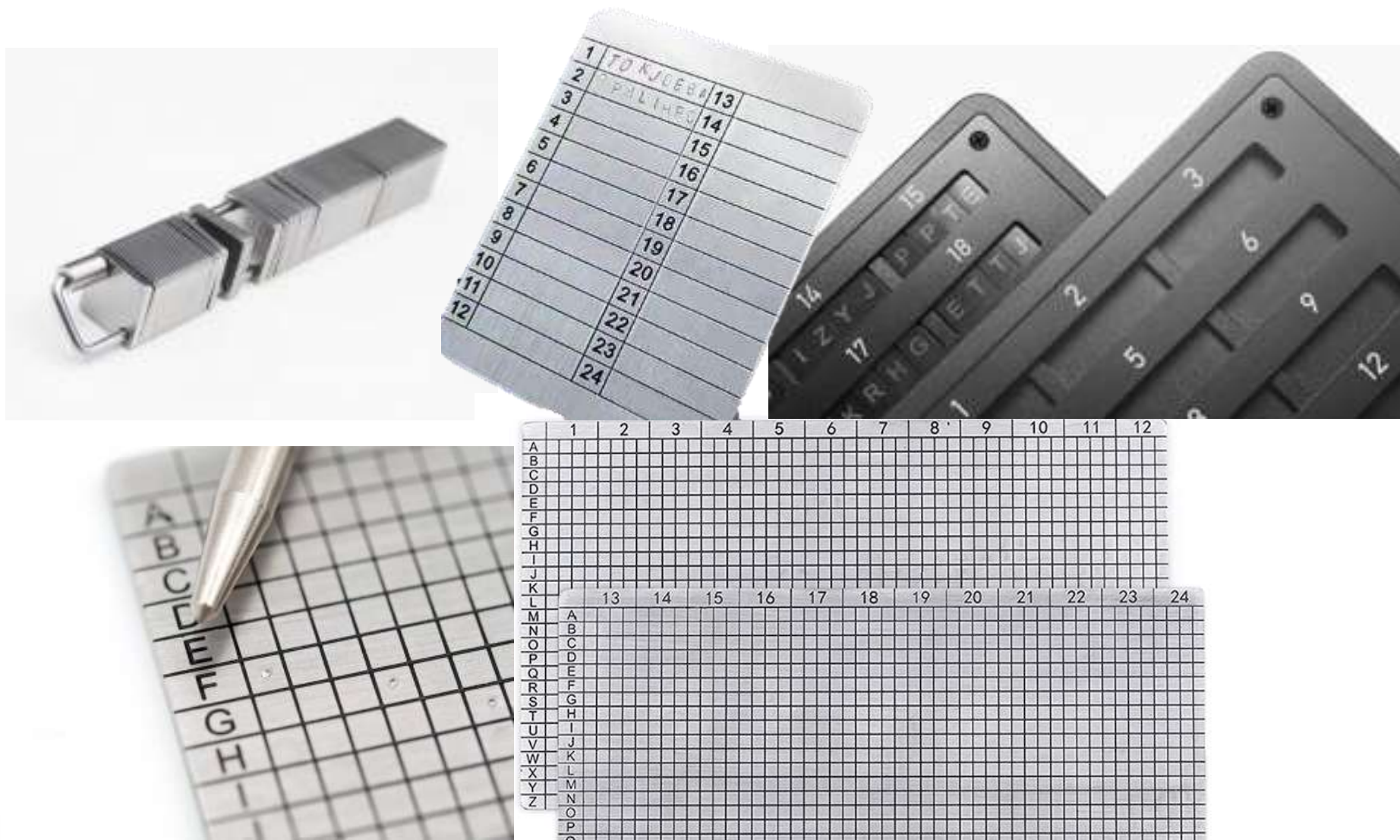
Public address QR Code



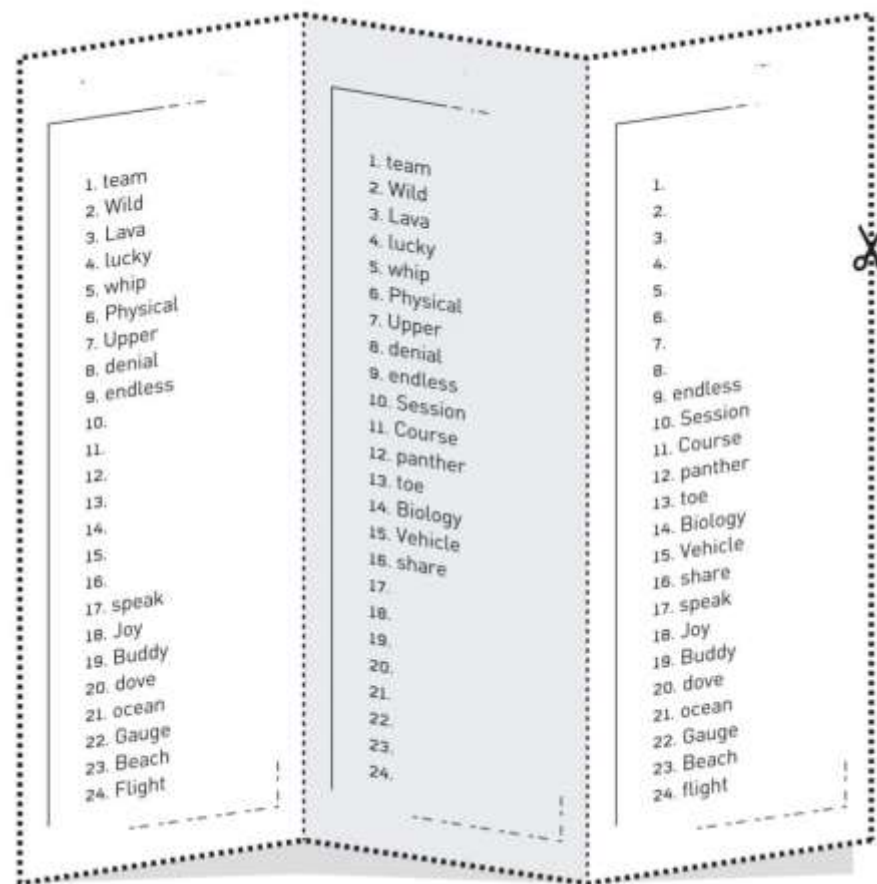
Private key QR Code (Wallet Import Format)



各种“硬”钱包



多份钱包（切勿使用！！！！）





不管用哪种钱包，核心还是需要“纸”钱包

纸钱包范例

- 绝对离线
- 收集熵
- 保存钱包

区块链探索 bbs.uchaindb.com

助记词:

您的账户助记词可以帮助您轻松
备份和恢复个人账户

your first dog
bushy green cowboy
pink for mother's
crown like a queen
purple again it's me

警告: 切勿向他人透露您的账户助记
词。任何人一旦持有该账户助记词, 即
可控制您的token

请将该助记词抄到纸上, 并保存
在安全的地方

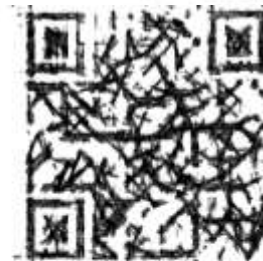
====沿此线折叠====

收款码 #1



====沿此线折叠====

收款码 #1



收款码 #2



收款码 #3



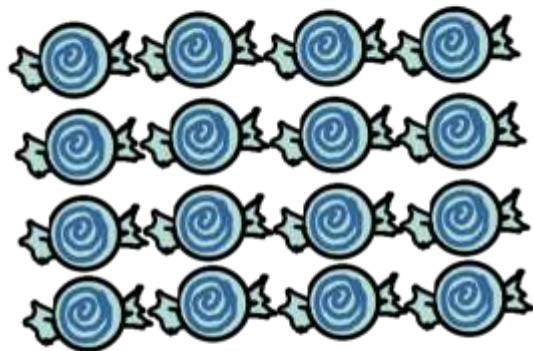
感谢您参与区块链探索沙龙!

技术提供方: 上海素图科技有限公司

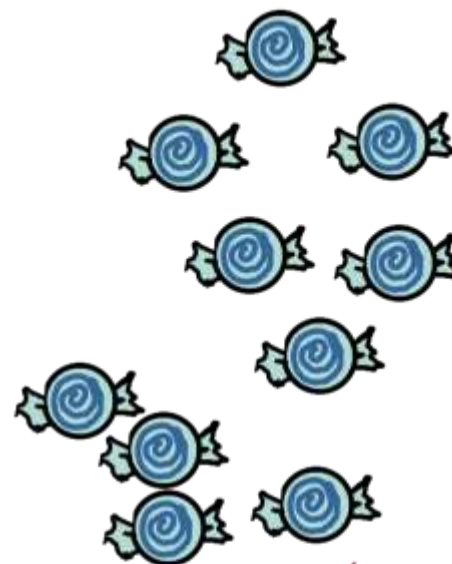
熵

有序：低熵

无序：高熵

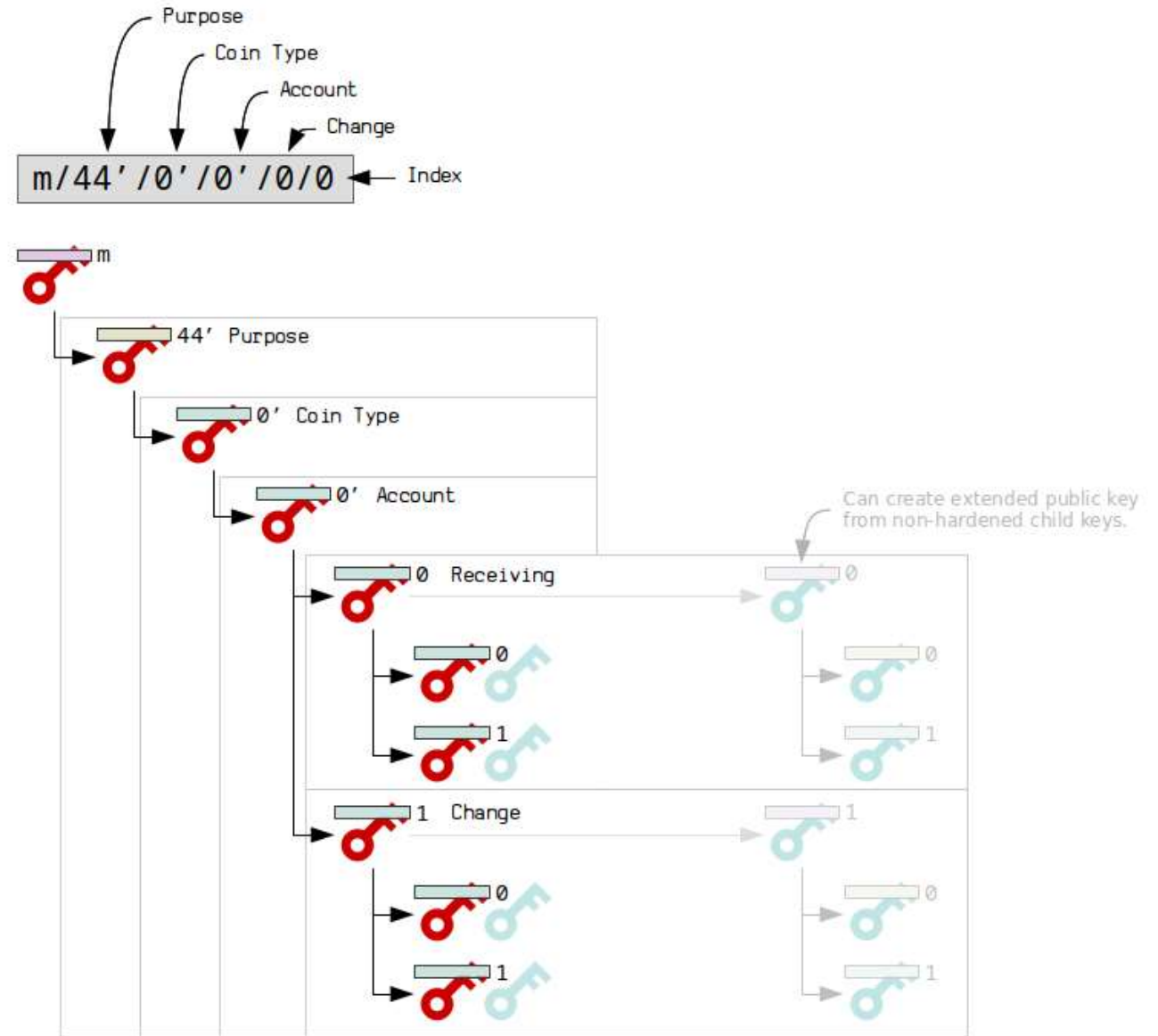


Low Entropy
order



High Entropy
disorder

BIP44



生成纸钱包

素图科技——纸钱包

生成新的钱包

密码（可选）：

通过您的声音来提高熵：

英文

生成新的钱包

密码（可选）：

canyon join charge style ceiling message wise whip
alone train muscle grow

打印

英文

再谈安全

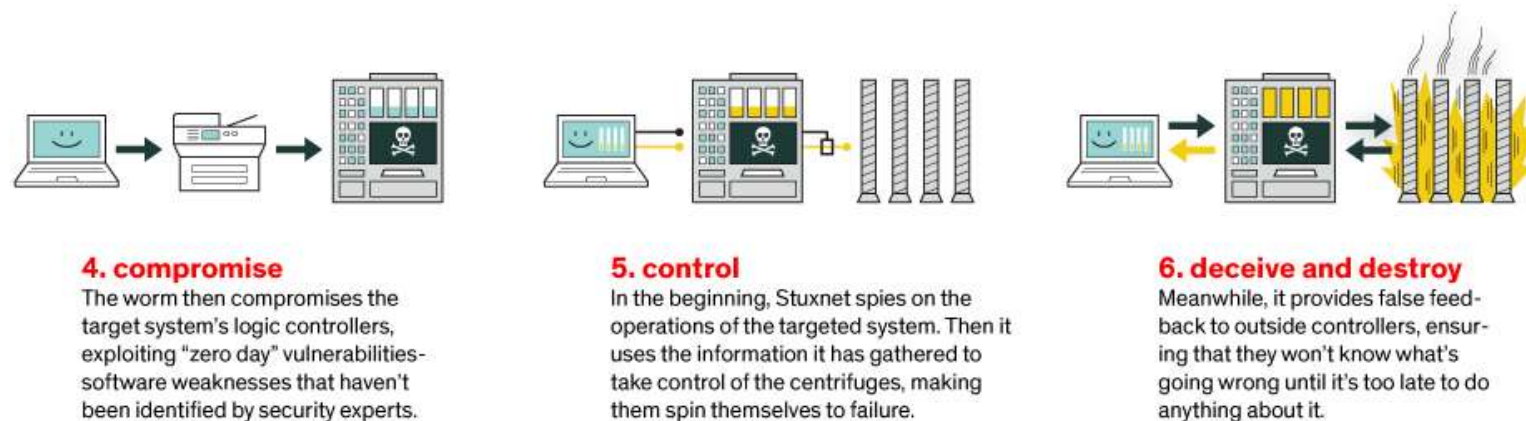
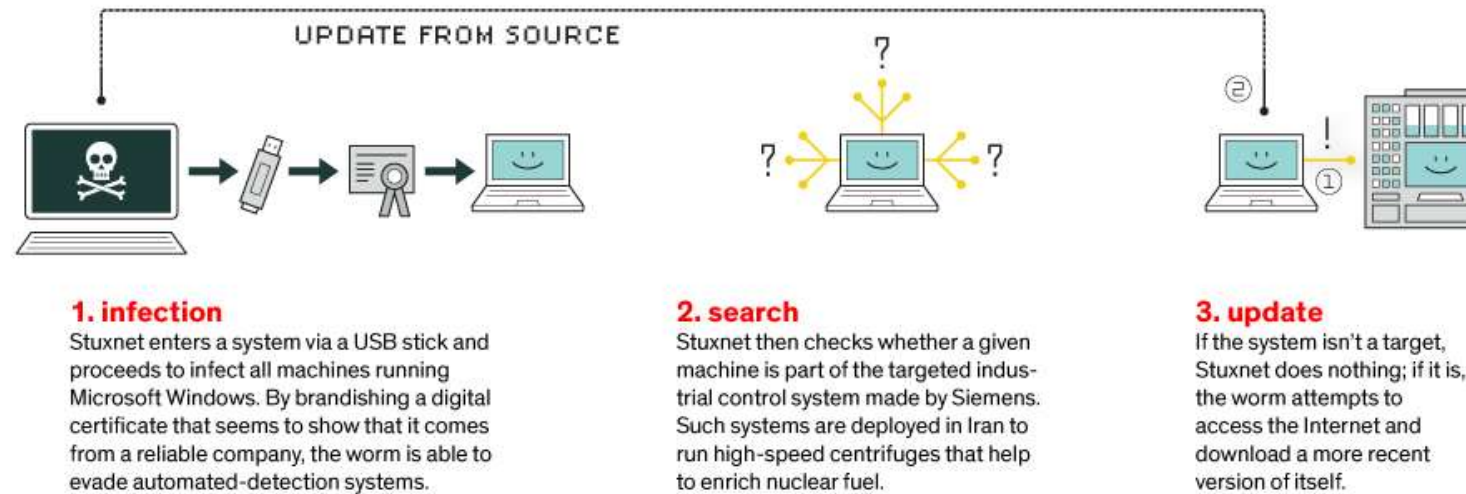
Hack of Jeff Bezos's iPhone

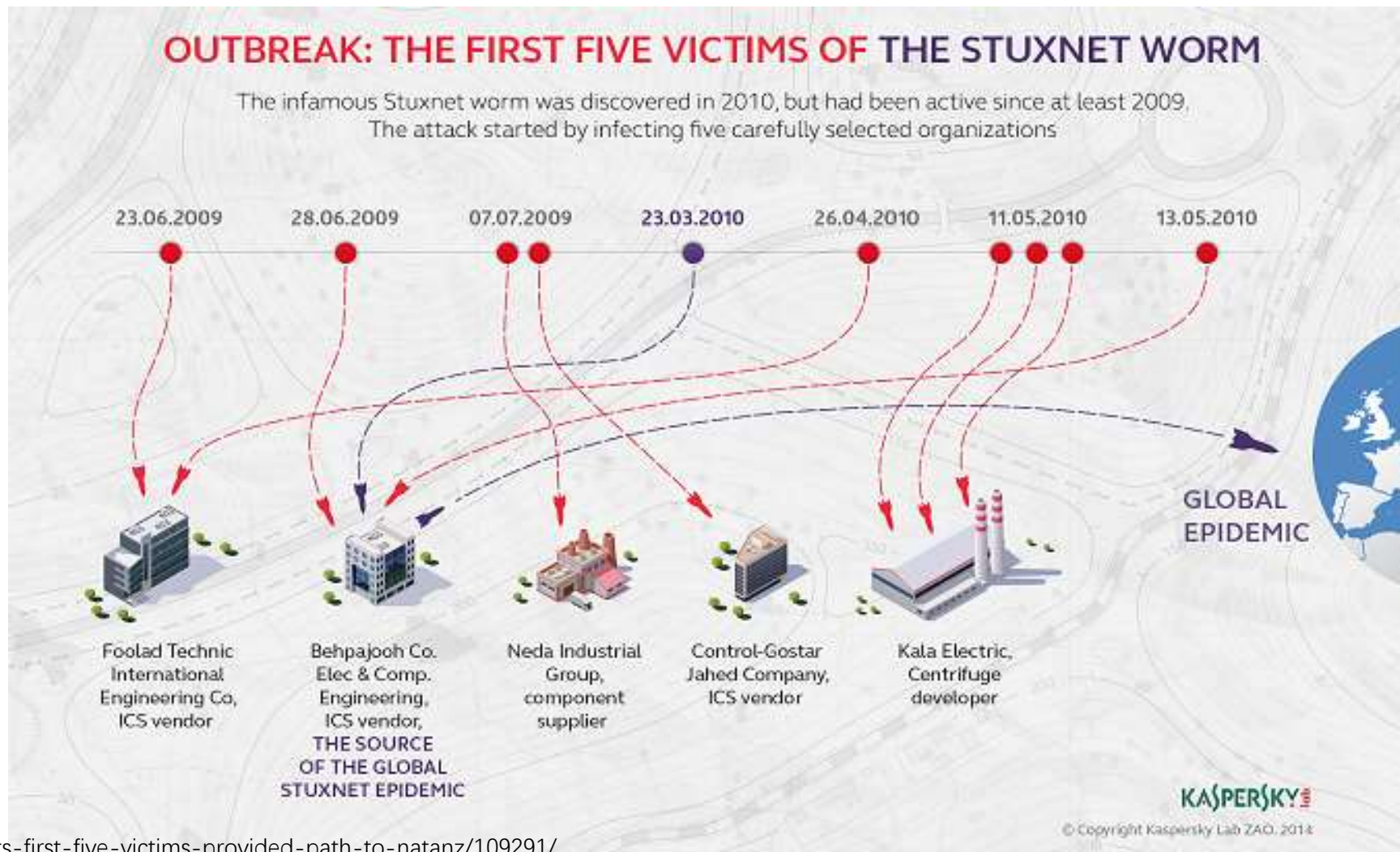


Figure 2: *Texts between Bezos and MBS.*
Source: Bezos' iPhone, WhatsApp application

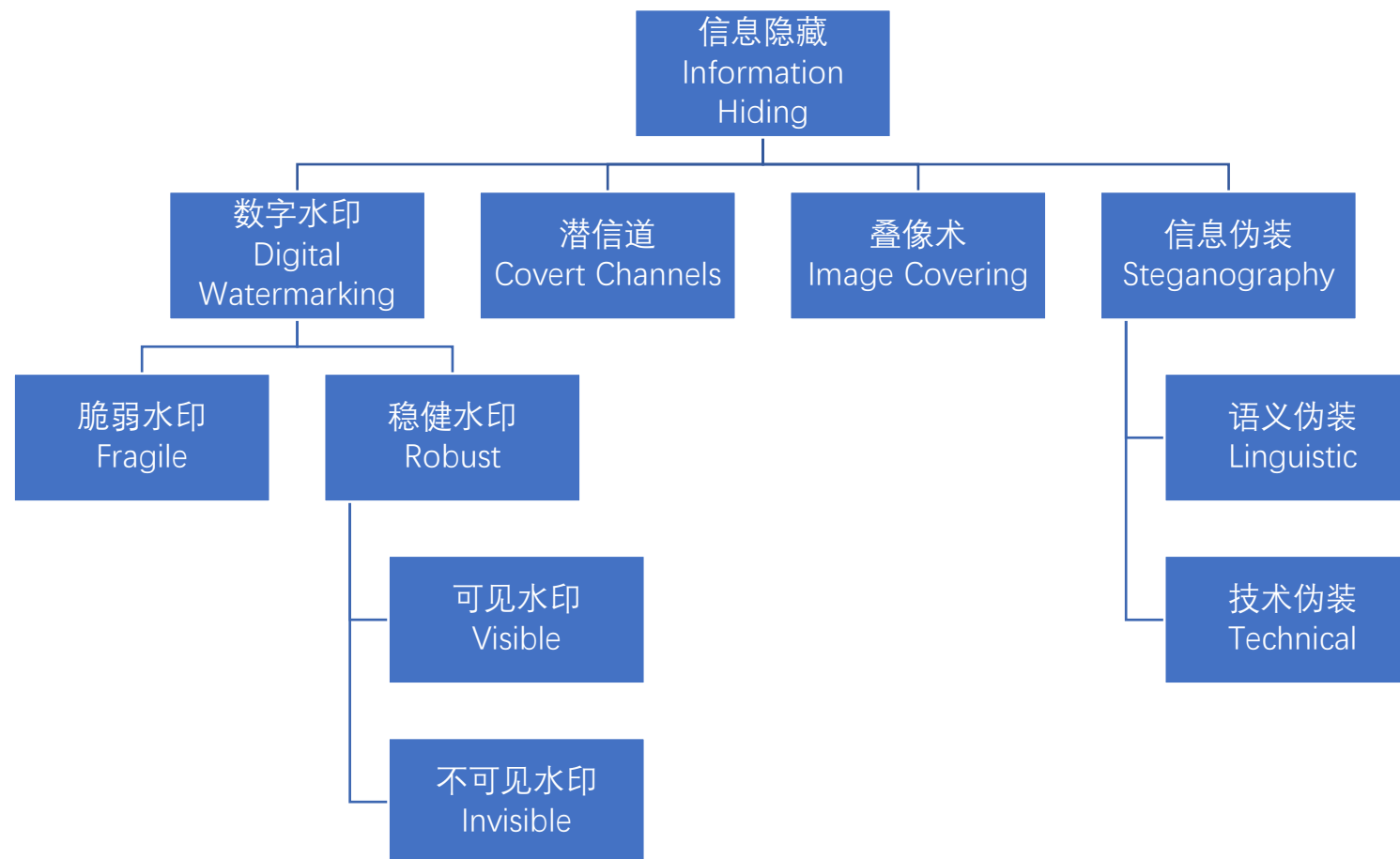


Stuxnet

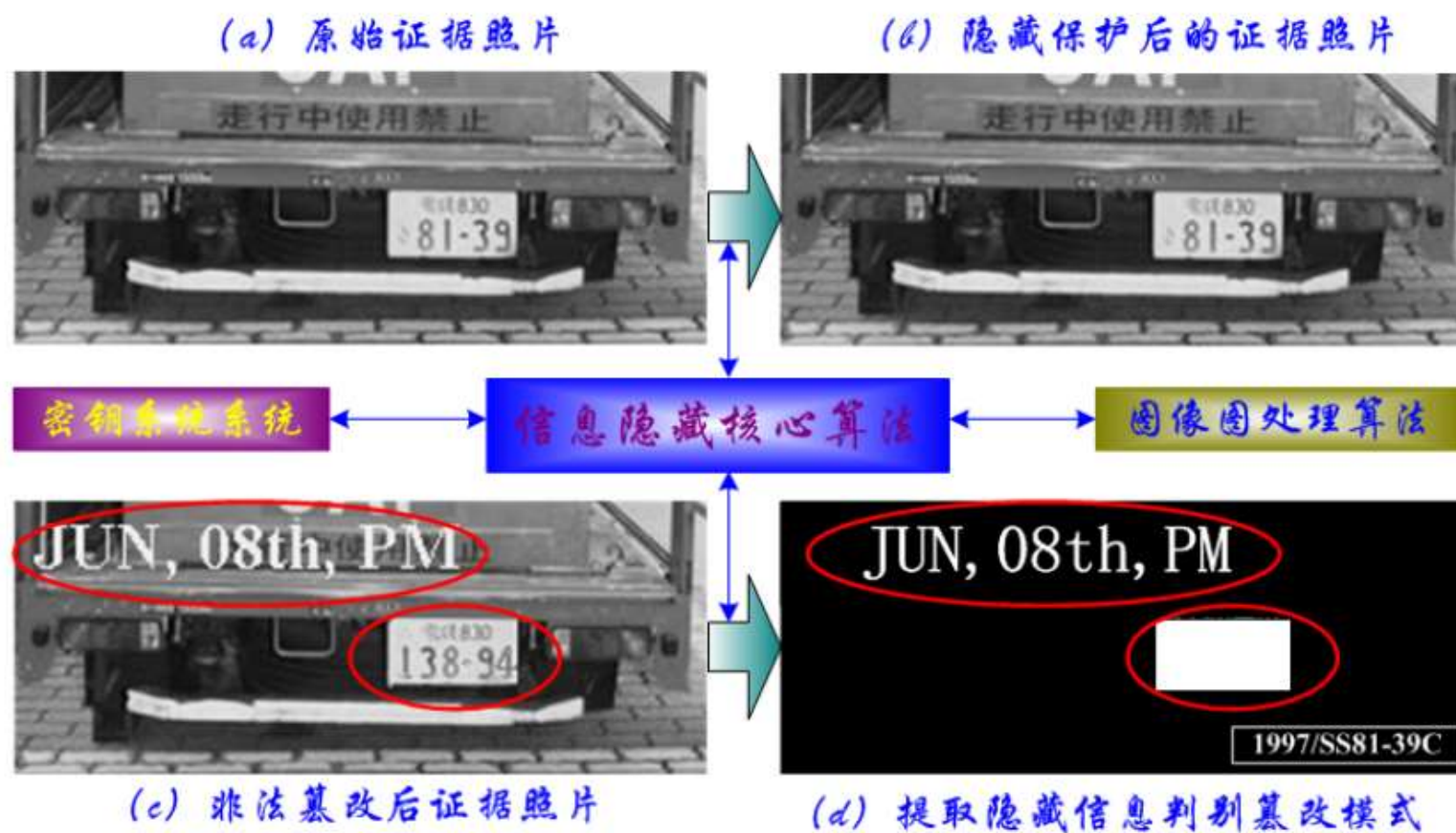




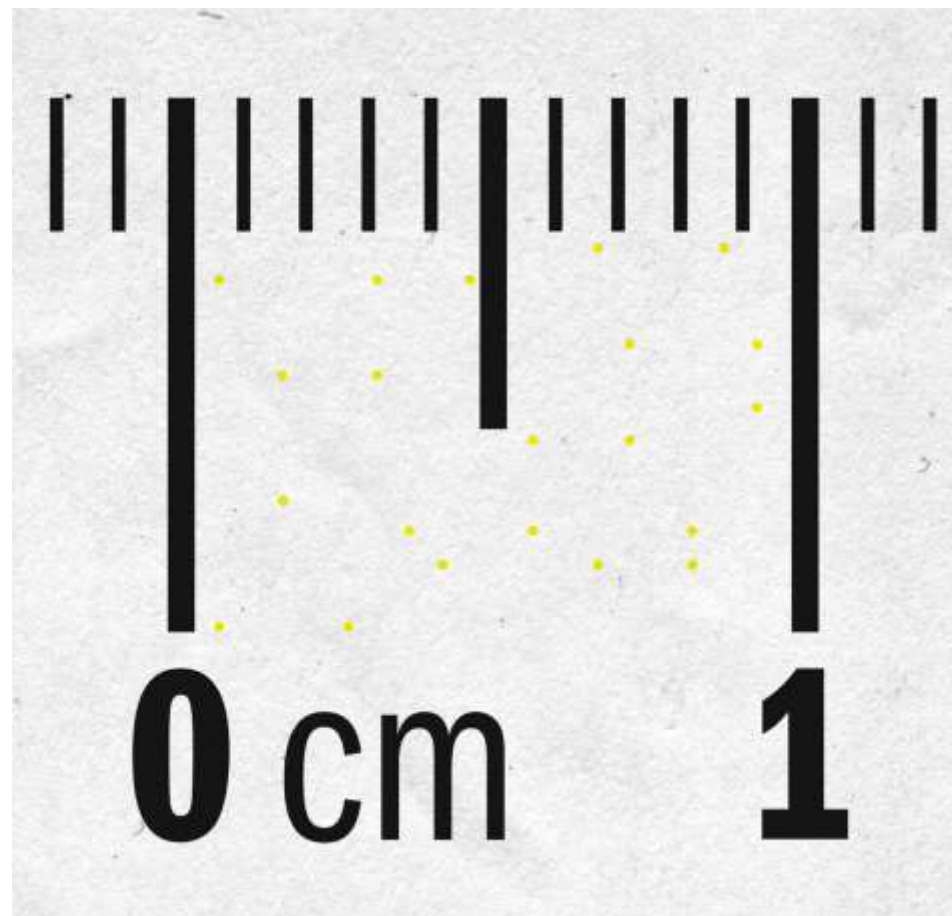
Steganography 信息伪装技术



数字水印



打印机的特殊印记



藏头诗

1 2 3
SALUDOS LOVED ONE
4 5 1 2 3 4 5 ...
SO TODAY I HEARD FROM UNCLE MOE OVER THE PHONE. HE TOLD
ME THAT YOU AND ME GO THE SAME BIRTHDAY. HE SAYS YOUR TIME THERE
TESTED YOUR STRENGTH SO STAY POSITIVE AT SUCH TIMES. I'M FOR ALL THAT
CLEAN LIVING! METHAMPHETAMINES WAS MY DOWN FALL. THE PROGRAM I'M
STARTING THE NINTH IS ONE I HEARD OF A COUPLE WEEKS BEFORE SEPTEMBER
THROUGH MY COUNSELOR BARRIOS. BUT MY MEDICAL INSURANCE COVERAGE
DENIES THEY COVER IT. I'M USING MY TIME TO CHECK AND IF THE INSURANCE
AGENT DENIES STILL MY COVERAGE I'M GETTING TOGETHER PAPERWORK
SAYING I TESTED FOR THIS TREATMENT REQUIRED ON THE CHILD CUSTODY.
THE NINTH WILL MEAN I HAVE TESTED MY DETERMINATION TO CHANGE. ON
THE NEXT FREE WEEKEND THE KIDS ARE COMING, BUT FIRST I GOTTA SHOW
CAROLINA I'M STAYING OUT OF TROUBLE WAITING TO GET MYSELF ADMITTED
ON THE PROGRAM. THE SUPPORTING PAPERWORK THAT THE FAMILY COURTS
GOT WILL ALSO PROVE THERE'S NO REASON NEITHER FOR A WITNESS ON MY
CHILDREN'S VISITS. OF COURSE MY BRO HAS HIS MIND MADE UP OF RECENT
THAT ALL THIS DRUG USAGE DON'T CONCERN OUR VISITS. I THINK THAT MY
KIDS FEEL I NEED THEIR LOVE IF I'M GONNA BE COOL. GUILTY FEELINGS RISE ON
ACCOUNT OF THE MISTAKES I COULD WRITEUP. FOR DAYS I'M HERE. HE GOT A
GOOD HEART. SHOULD YOU BE HAVING PROBLEMS BE ASSURED THAT WHEN
YOU HIT THE STREETS WE'LL BE CONSIDERING YOU.....

信息伪装与密码学

- 柯克霍夫原则
 - 除了私钥之外的信息都是公开的，系统依旧是安全的
- 大密钥空间原则

安全建议

- 确保助记词均来自设备屏幕
- 确保单词拼写和单词顺序没错
- 确保记录介质安全，不会丢也不会意外损毁
- 在不同的安全位置存储多份

影子钱包（哨兵钱包）

- 助记词不含密码的版本中含有小量资金
- 如果被转走，说明助记词已经泄漏
- 真正的资金是在含密码的助记词中的

保管建议

- 绝不要存在联网的电脑里
- 绝对不要把助记词部分单词分开存放
- 简单地把其他单词加到助记词中间，可能很难提高安全性
- 小心使用脑钱包，很容易丢
- 小众币记得把钱包的名字记下来

Chialisp SH Workshop

区块链开发工作坊

时间: 3月18日 14:00-17:30

地点: 国康路100号上海国际设计中心22楼多功能厅

2023 Mar 18th, 14:00-17:30



议程:

14:00-14:20 从B到C, 区块链的发展史

14:20-15:00 Chia的技术路线图

15:00-15:40 丢币的N种方式 (如何保障钱包安全?)

15:40-16:00 茶歇

16:00-16:40 Chialisp开发入门

16:40-17:00 Chia NFT介绍

17:00-17:30 现场提问时间