P.O.D · New Block Trend

新区势

2018 WISE

P.O.D · New Block Trend
新区势 2018 WISE

区块链安全风险

彭峙酿@360核心安全

区块链安全是跟风吗？

数字货币，已经改变了我们的生活。

数字货币安全事件频发

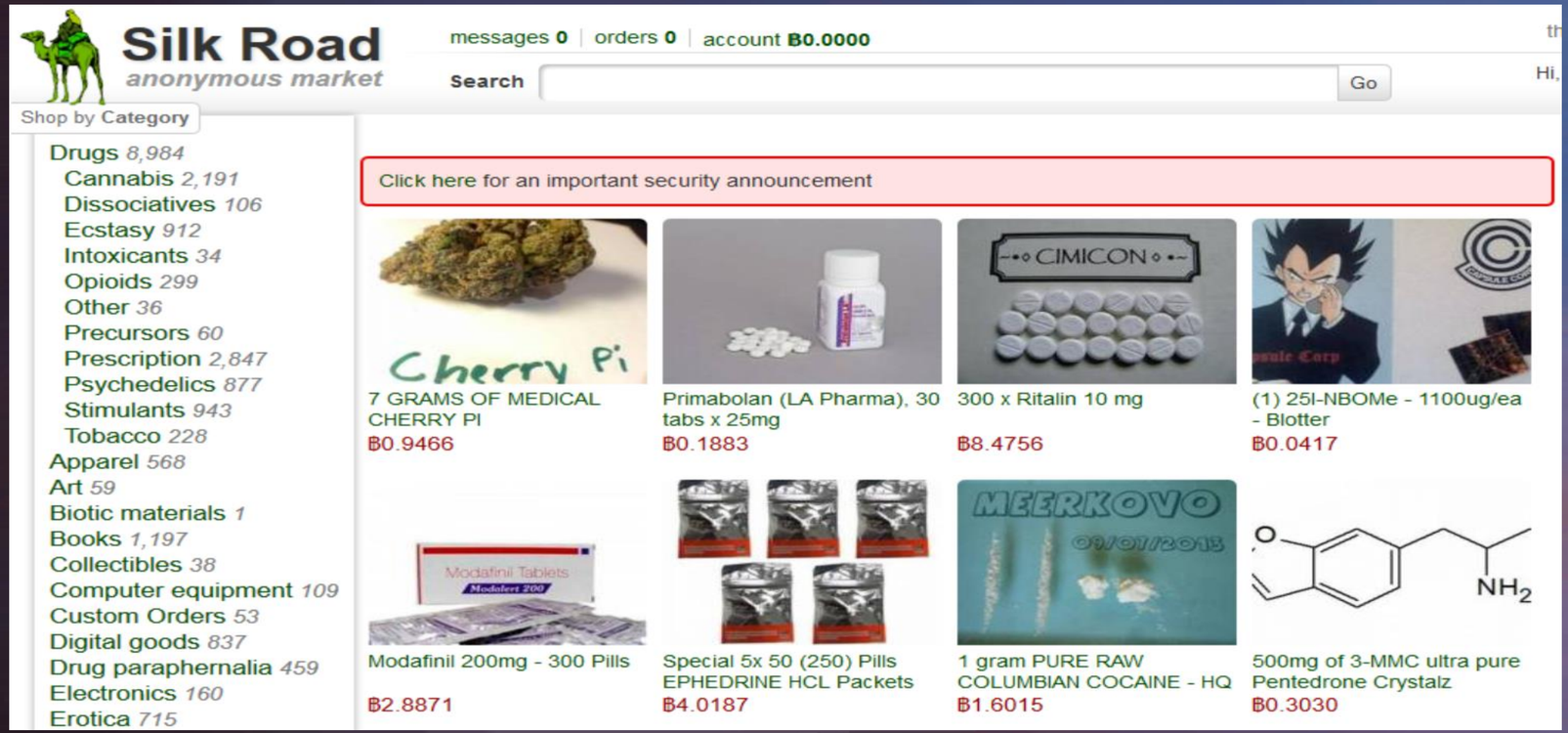
2013-2018： 至少54起严重安全事件
2018上半年： 安全事件引起27亿美元损失

案例：Mt.gox被盗案

85万枚比特币被盗

数字货币世界已成为法外之地

案例：丝绸之路


Silk Road
anonymous market
messages 0 | orders 0 | account ฿0.0000
Search
Go
Hi,
Shop by Category
Drugs 8,984
Cannabis 2,191
Dissociatives 106
Ecstasy 912
Intoxicants 34
Opioids 299
Other 36
Precursors 60
Prescription 2,847
Psychedelics 877
Stimulants 943
Tobacco 228
Apparel 568
Art 59
Biotic materials 1
Books 1,197
Collectibles 38
Computer equipment 109
Custom Orders 53
Digital goods 837
Drug paraphernalia 459
Electronics 160
Erotica 715
Click here for an important security announcement
Cherry Pi
7 GRAMS OF MEDICAL CHERRY PI
฿0.9466
Primabolan (LA Pharma), 30 tabs x 25mg
฿0.1883
CIMICON
300 x Ritalin 10 mg
฿8.4756
(1) 25I-NBOMe - 1100ug/ea - Blotter
฿0.0417
Modafinil Tablets
Modalert 200
Modafinil 200mg - 300 Pills
฿2.8871
Special 5x 50 (250) Pills EPHEDRINE HCL Packets
฿4.0187
MEERKOVO
1 gram PURE RAW COLUMBIAN COCAINE - HQ
฿1.6015
O
NH2
500mg of 3-MMC ultra pure Pentedrone Crystalz
฿0.3030

新技术：进一步助长黑市交易

匿名币：　无迹可寻
智能合约：　犯罪智能合约

案例：WannaCry

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (simpl
我的电脑出了什么问题？
您的一些重要文件被我加密保存了。
照片、图片、文档、压缩包、音频、视频文件、exe文件等，几乎所有类型的文件都被加密了，因此不能正常打开。
这和一般文件损坏有本质上的区别。您大可在网上找找恢复文件的方法，我敢保证，没有我们的解密服务，就算老天爷来了也不能恢复这些文档。
有没有恢复这些文档的方法？
当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以人格担保，能够提供安全有效的恢复服务。
但这是收费的，也不能无限期的推迟。
请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，我是绝不会骗你的。
但想要恢复全部文档，需要付款点费用。
是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟付款时间越长对你不利。
最好3天之内付款费用，过了三天费用就会翻倍。
还有，一个礼拜之内未付款，将会永远恢复不了。
对了，忘了告诉你，对半年以上没钱付款的穷人，会有活动免费恢复，能否轮
Payment will be raised on
5/17/2017 21:39:19
Time Left
02:23:59:39
Your files will be lost on
5/21/2017 21:39:19
Time Left
06:23:59:39
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

数字货币项目本身存在漏洞

案例：EOS编译器asset模板漏洞


```
01. asset& operator*=( int64_t a ) {
02.
03.         eosio_assert( a == 0 || (amount * a) / a == amount, "multiplication overflow or underflow" );
04.
05.         eosio_assert( -max_amount <= amount, "multiplication underflow" );  <= (2)
06.
07.         eosio_assert( amount <= max_amount,  "multiplication overflow" );   <= (3)
08.
09.         amount *= a;
10.
11.         return *this;
```

P.O.D · New Block Trend
新区势 2018 WISE

360区块链安全研究

http://blogs.360.cn/

区块链安全，机会与挑战

安全事件频发
监管严重缺乏
项目安全问题严重

P.O.D · New Block Trend
新区势 2018 WISE

THANKS