# 区块链网络安全态势分析

分享人：张冬冬　　中国刑事警察学院公安信息技术与情报学院

# 目录

# 目录

# （一）区块链起源

区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在2008年发表的奠基性论文《比特币：一种点对点电子现金系统》。

分布式账本

链式数据结构

非对称加密

# （二）区块链概念

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

广义来讲，区块链是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

区链式数据结构

节点共识机制

非对称密码学加密


自动化智能合约

# （三）区块链的关键技术

## P2P节点网络

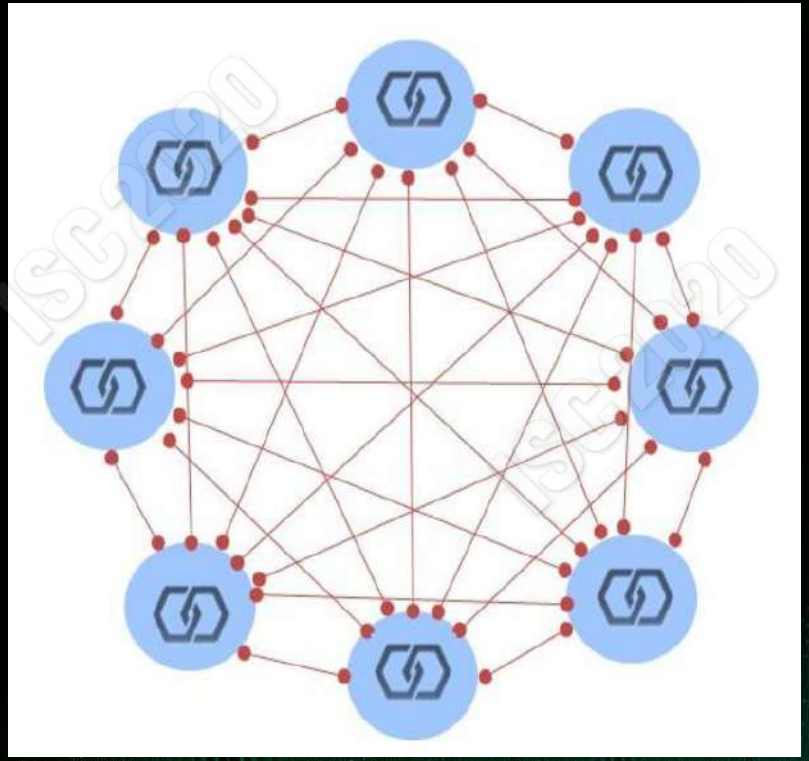
任何机器都可以运行一个完整的比特币节点，一个完整的比特币节点包括如下功能：

1、**钱包**，允许用户在区块链网络上进行交易；

2、**完整区块链**，记录了所有交易历史，通过特殊的结构保证历史交易的安全性，并且用来验证新交易的合法性；

3、**矿工**，通过记录交易及解密数学题来生成新区块，如果成功可以赚取奖励；

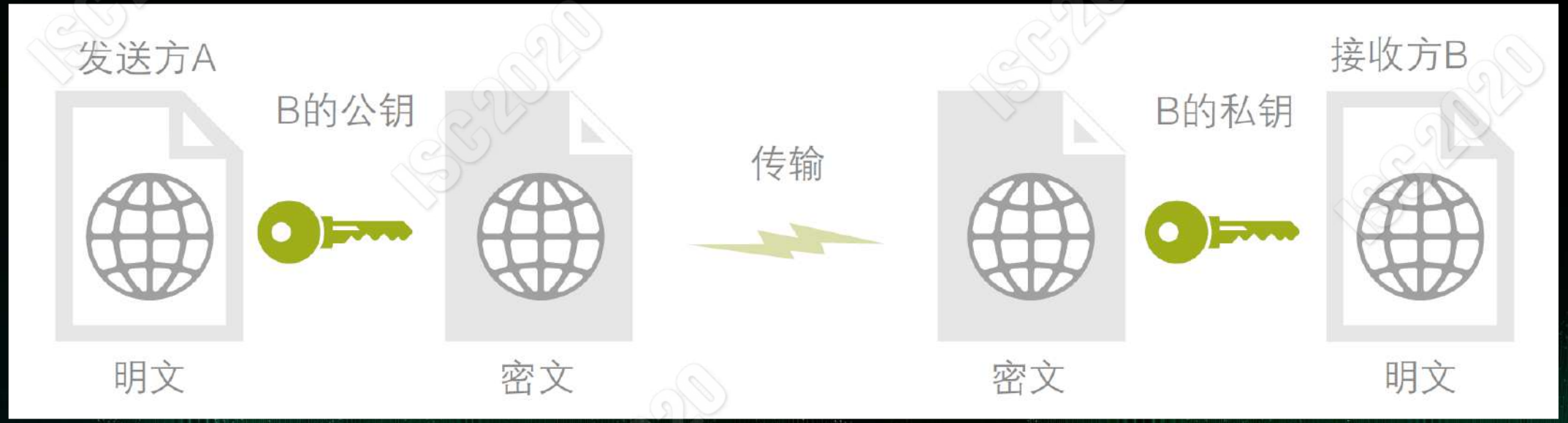
4、**路由功能**，把其它节点传送过来的交易数据等信息再传送给更多的节点；



# （三）区块链的关键技术

## 非对称加密通信

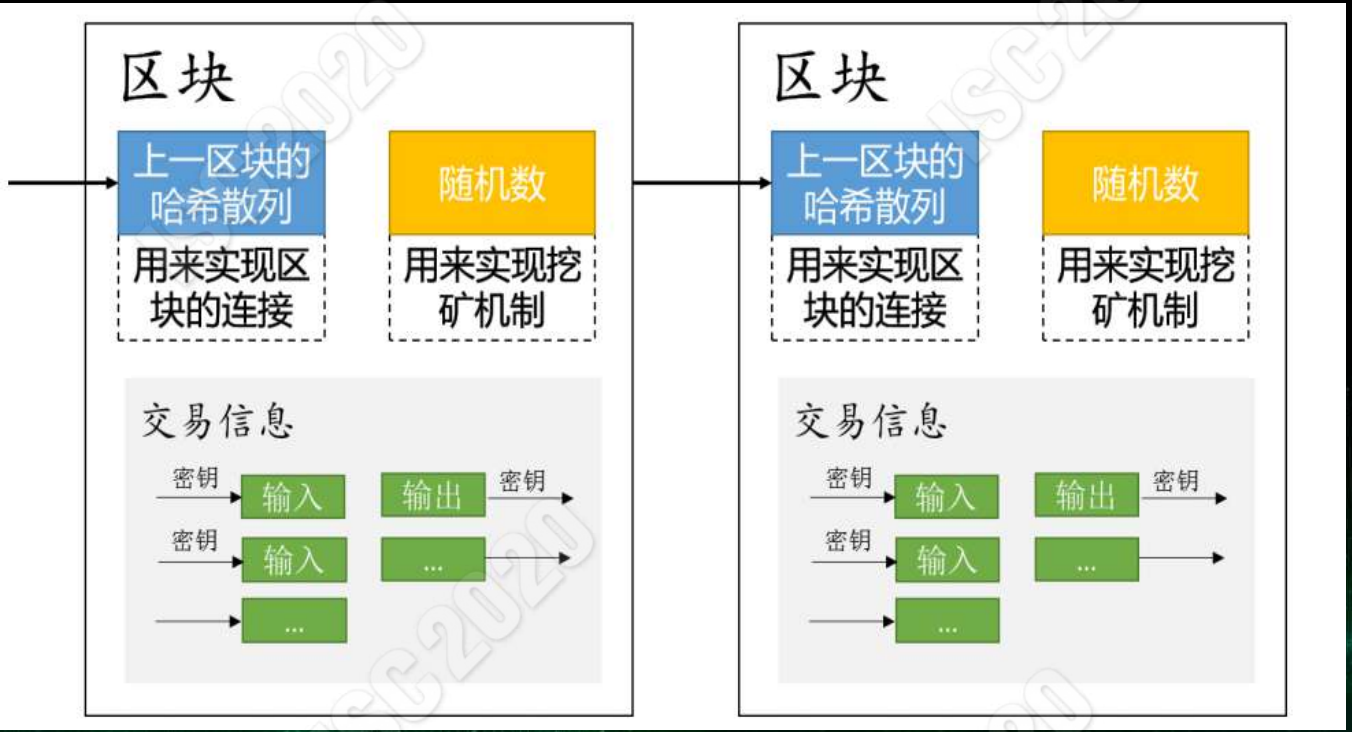
非对称加密算法是指使用公私钥对数据存储和传输进行加密和解密。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方解密接收到的加密内容。



# （三）区块链的关键技术

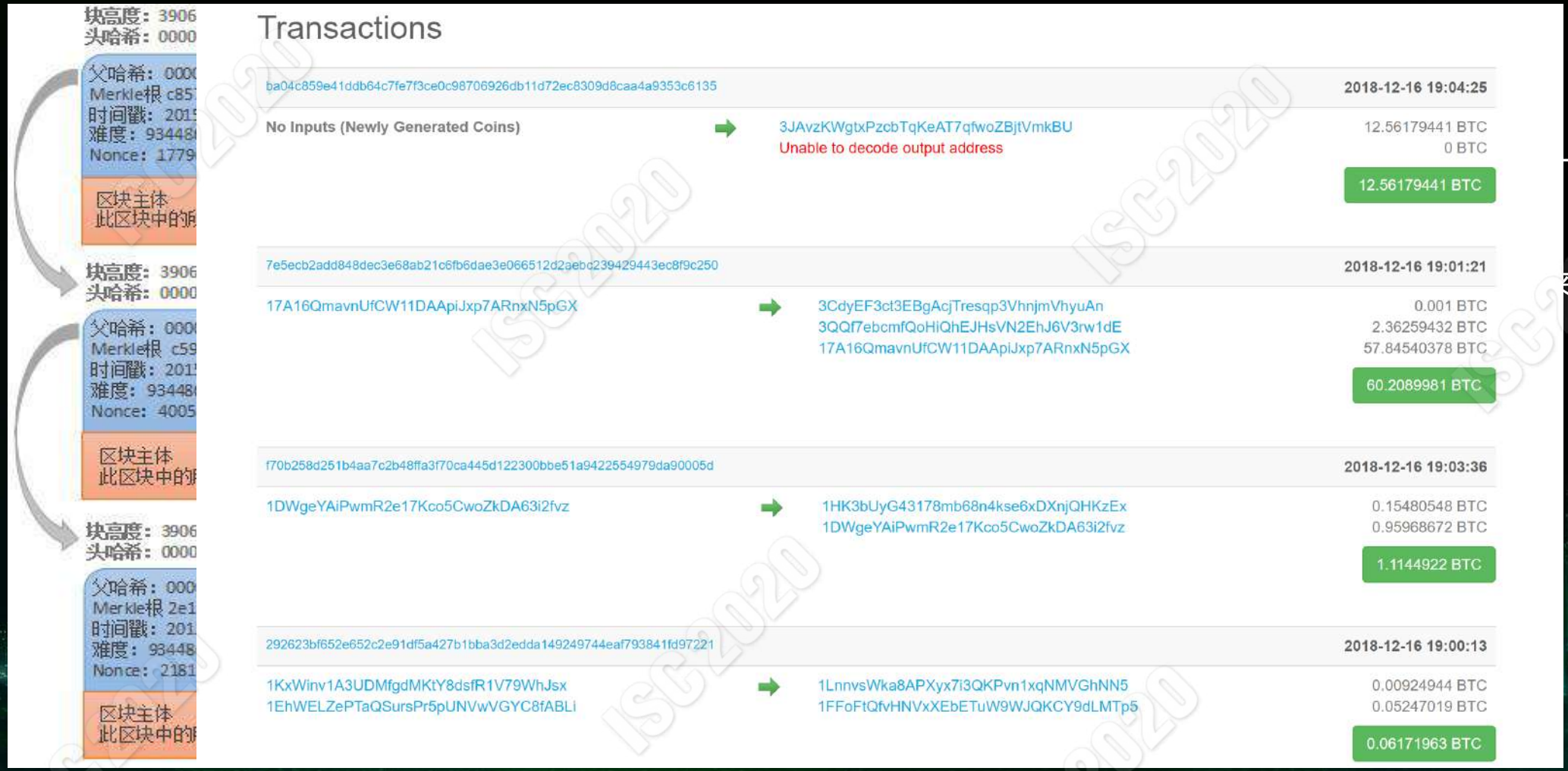
## 链式数据结构

区块是一种记录交易的数据结构。每个区块由区块头和区块主体组成，区块主体只负责记录前一段时间内的所有交易信息，区块链的大部分功能都由区块头实现。



# （三）区块链的关键技术

## 区块头




首尾相连

的一个数

# （三）区块链的关键技术

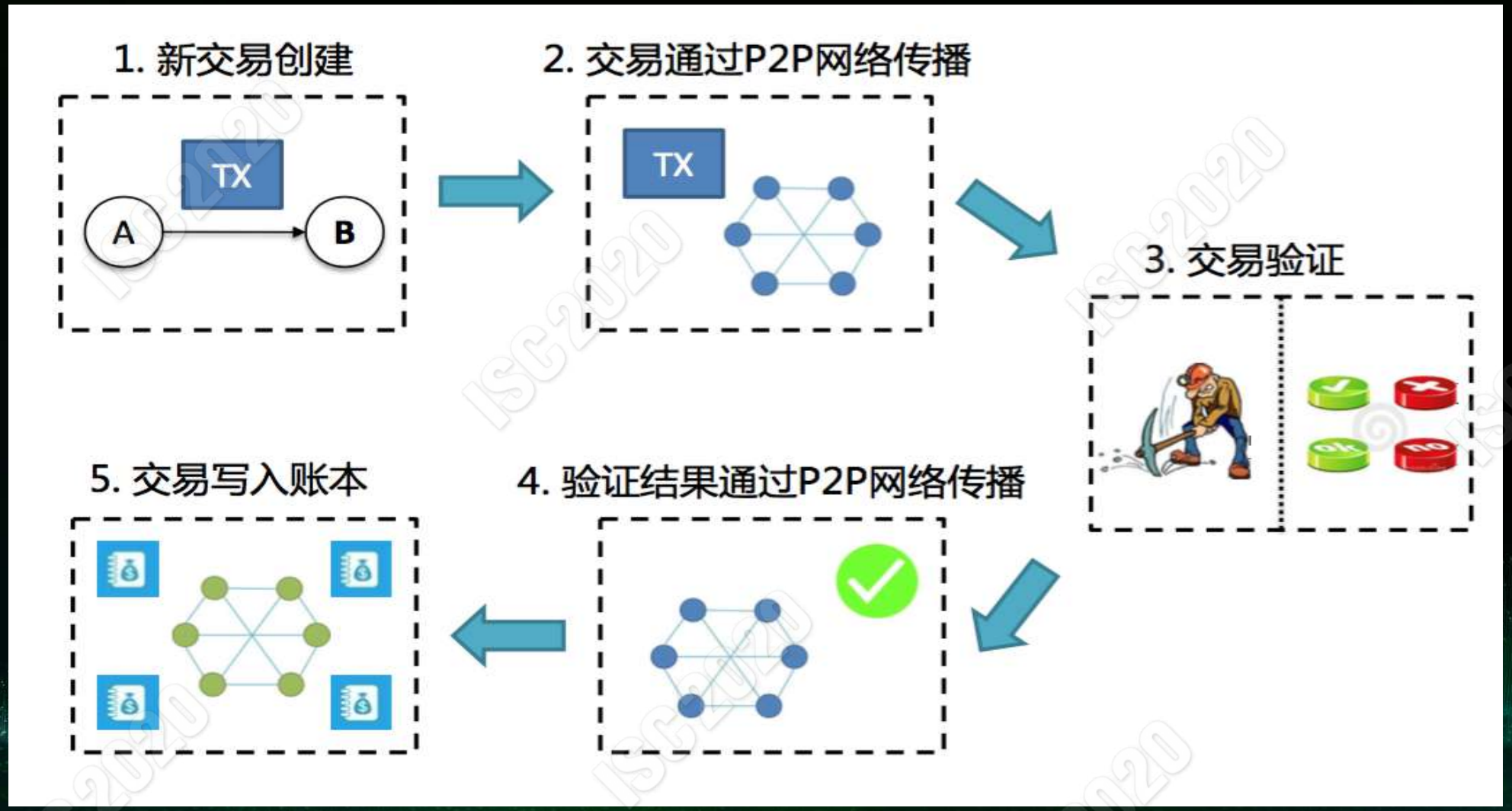
## 共识机制

比特币在Block的生成过程中使用了POW机制，一个符合要求的Block Hash由N个前导零构成，零的个数取决于网络的难度值。要得到合理的Block Hash需要矿机对区块头的随机数进行大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的Block Hash值，说明该节点确实经过了大量的尝试计算，这样就构建了一个工作量证明机制。

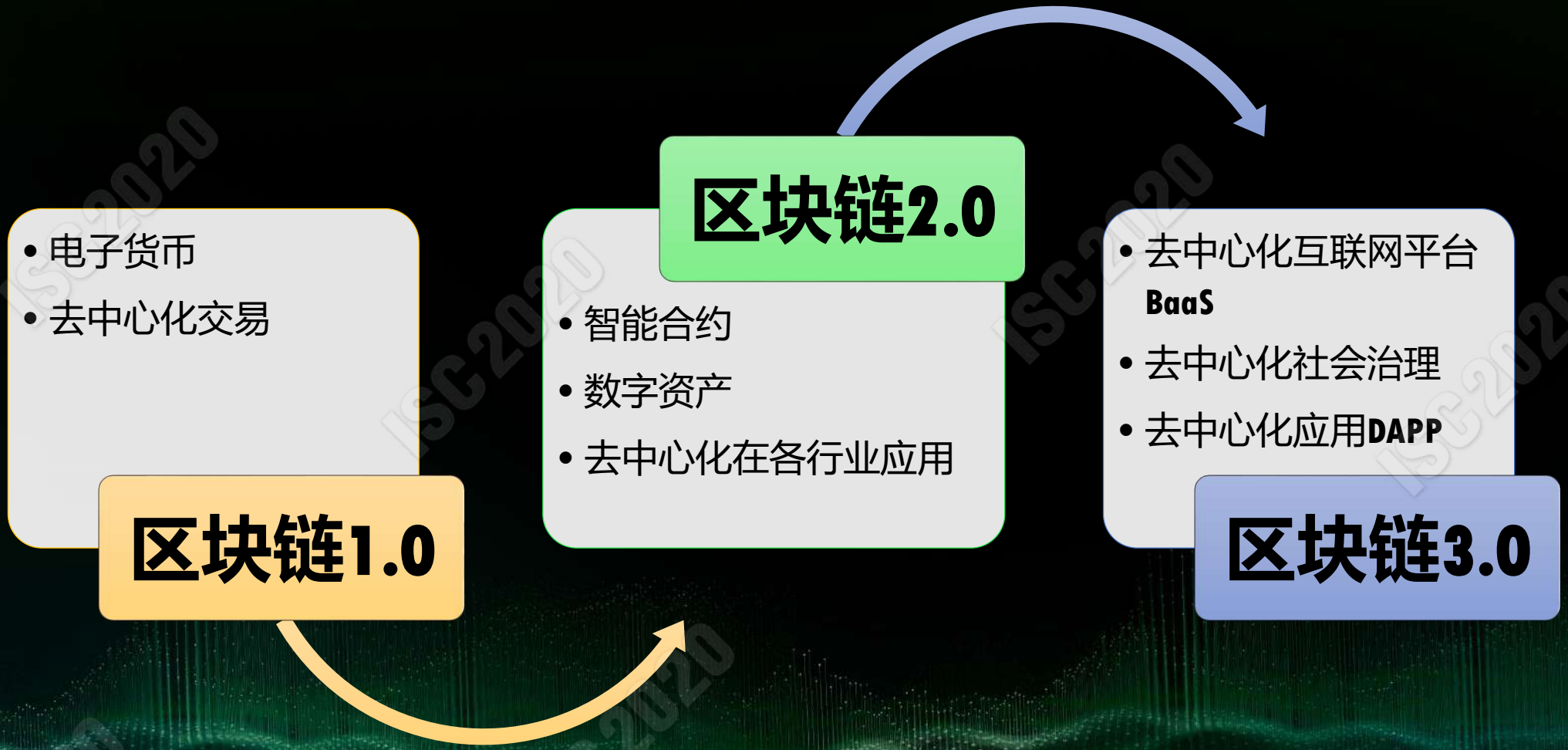
```php
$header_hex = "01000000" . // version
// previous block hash
"81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a308000000000000" .
// merkle root hash of transactions in this block
"e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b" .
// Time
"c7f5d74d" .
// Bits (Difficulty)
"f2b9441a" .
// Nonce
"42a14695";
$header_bin = pack("H*", $header_hex); // hex to bin
$h = hash('SHA256', hash('sha256', $header_bin, true), true); // double sha256

echo bin2hex($h), "\n";
// output: 1dbd981fe6985776b644b173a4d0385ddc1aa2a829688d1e0000000000000000
echo bin2hex(strrev($h)), "\n";
// output: 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
```

# （四）区块链交易过程

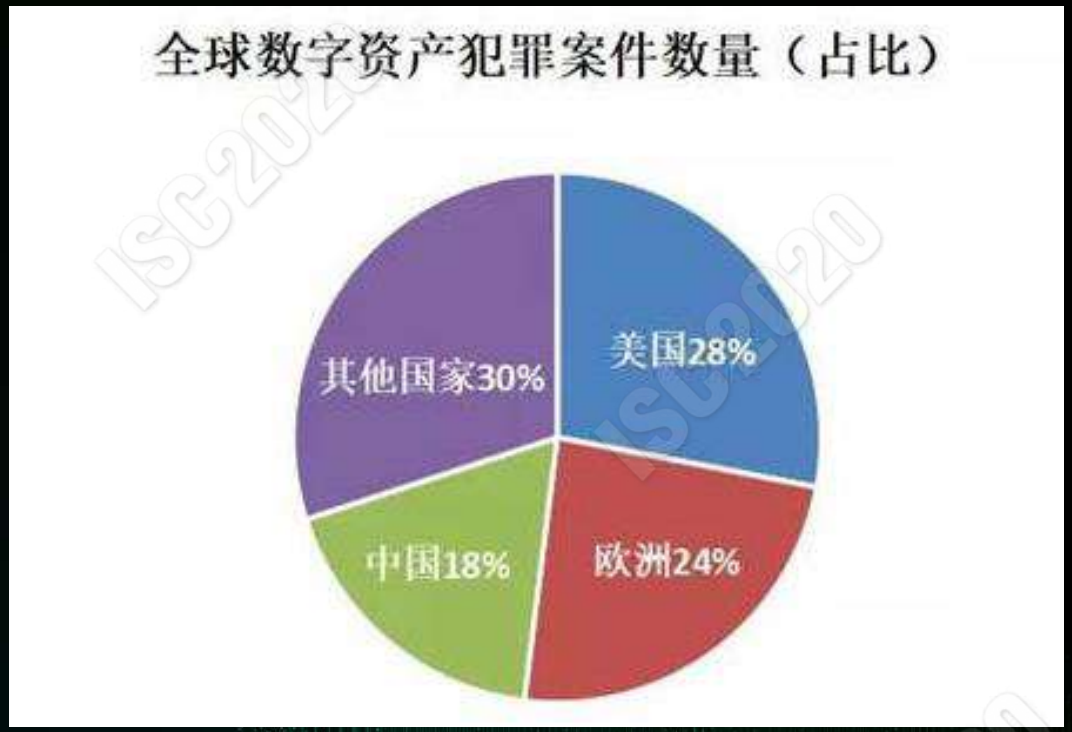


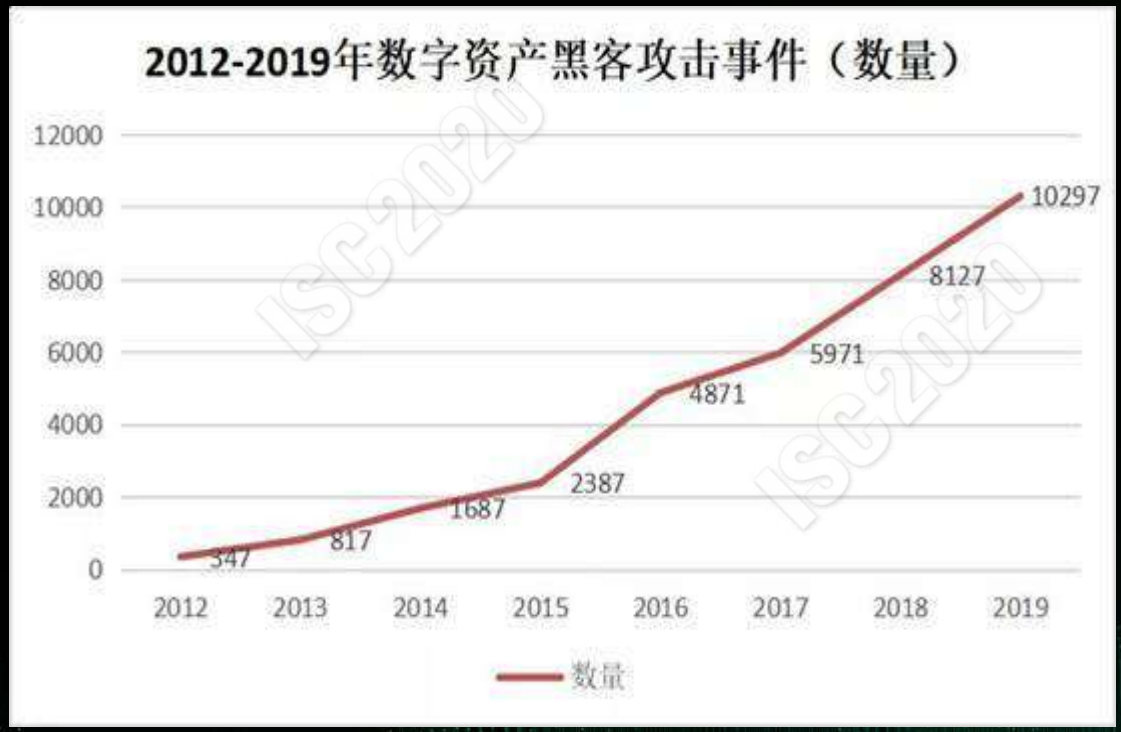
# （五）区块链发展



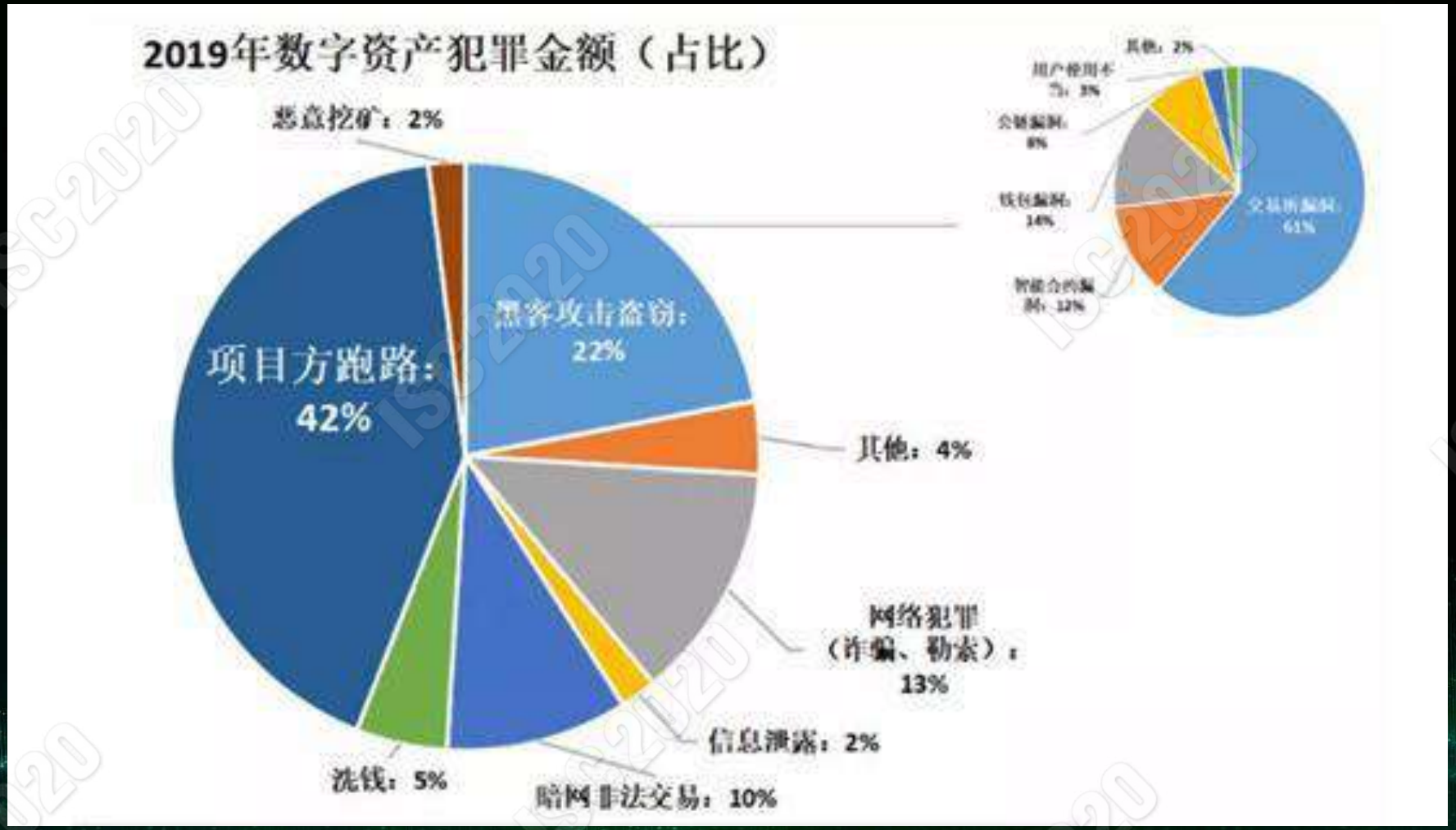
# 目录

# 2019年全球区块链安全事件统计

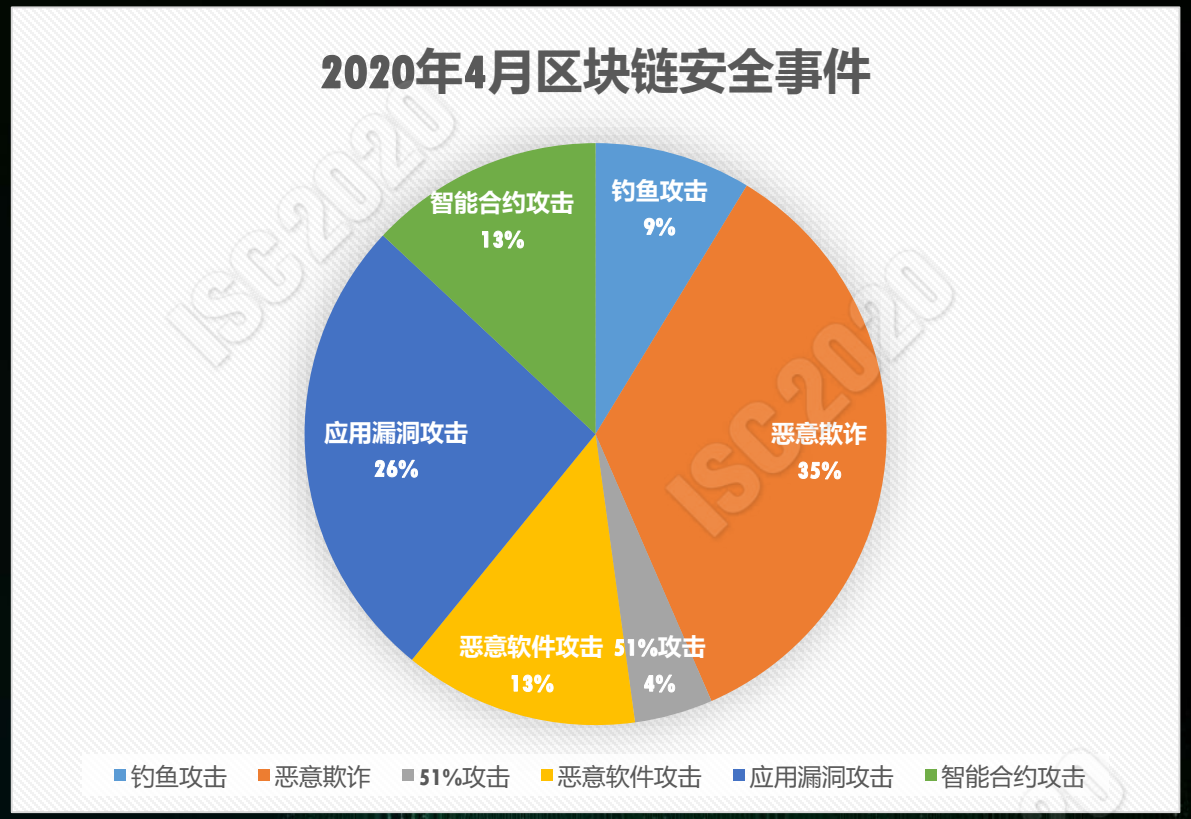


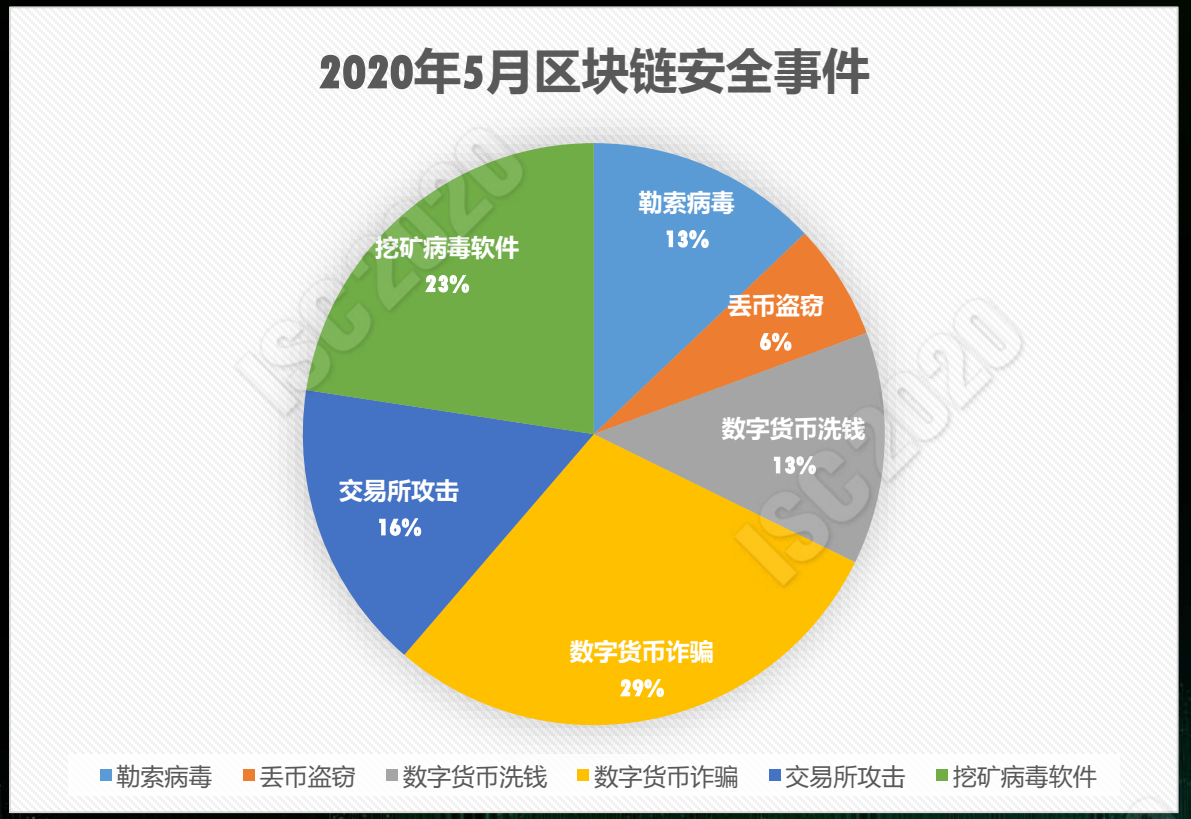



# 2019年全球区块链安全事件统计



# 2020年4、5月区块链安全事件



# 目录

# （一）利用虚拟货币开展非法集资


**马克币** 传销
- 信息来源 公安部
- 相关报道 全国公安机关采取强力措施持续严打传销犯罪
- 运作模式 虚拟货币 点击查看详情 >

**亚欧币** 传销
- 信息来源 公安部
- 相关报道 全国公安机关采取强力措施持续严打传销犯罪
- 运作模式 虚拟货币 点击查看详情 >

**皇尊币** 传销
- 信息来源 山东省青州市公安局
- 相关报道 青州警方破获特大网络传销案 会员近7000人
- 运作模式 虚拟货币 点击查看详情 >

**恒星币** 传销
- 信息来源 公安部
- 相关报道 全国公安机关采取强力措施持续严打传销犯罪
- 运作模式 虚拟货币 点击查看详情 >

**麦加币** 传销
- 信息来源 常州金坛公安
- 相关报道 常州警方破获特大网络传销案 涉案金额达1.3亿元
- 运作模式 虚拟货币 点击查看详情 >

**克拉币** 传销
- 信息来源 公安部
- 相关报道 全国公安机关采取强力措施持续严打传销犯罪
- 运作模式 虚拟货币 点击查看详情 >

**云数贸-五行币** 传销
- 信息来源 公安部
- 相关报道 公安部：“五行币”系列传销组织头目宋密秋从印尼被缉捕归案
- 运作模式 虚拟货币 点击查看详情 >

**霹克币** 传销
- 信息来源 公安部
- 相关报道 全国公安机关采取强力措施持续严打传销犯罪
- 运作模式 虚拟货币 点击查看详情 >

**万福币** 传销
- 信息来源 湖南省常德市公安局
- 相关报道 常德破获美国未来城“万福币”特大网络传销案
- 运作模式 虚拟货币 点击查看详情 >

**莱汇币** 传销
- 信息来源 齐齐哈尔市铁锋公安分局
- 相关报道 男子创建“莱汇币”手机APP 非法集资3000多万被抓获
- 运作模式 虚拟货币 点击查看详情 >

**维卡币** 传销
- 信息来源 公安部
- 相关报道 全国公安机关采取强力措施持续严打传销犯罪
- 运作模式 虚拟货币 点击查看详情 >

# （二）利用虚拟货币开展网络传销

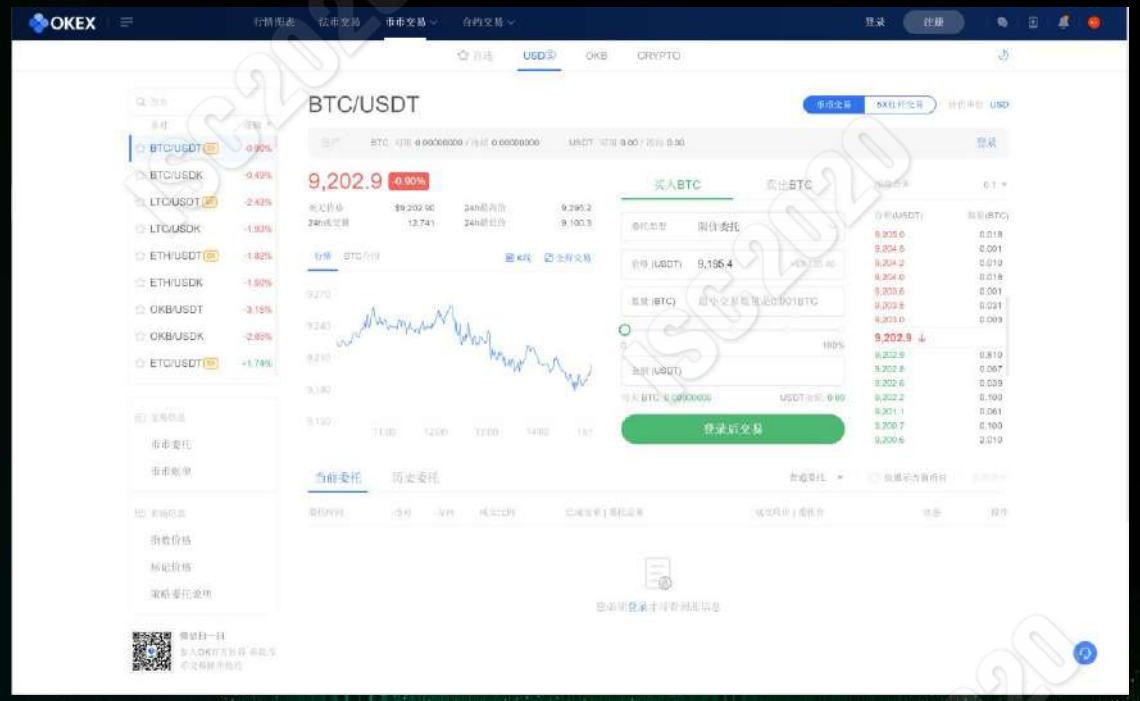


| 2019年立案、破获的项目 | | | | | | |
|---|---|---|---|---|---|---|
| | 项目主体 | 主体所在地 | 形式 | 创立时间 | 目前项目状态 | 涉案金额 |
| BHB | / | / | 金融安全区块链平台 | 2018年12月 | 2019年8月12日，BHB主要负责人刁某某已被四川省青神县公安局刑事拘留 | 超过20亿 |
| 趣步 | 重庆趣步网络科技有限公司 | 重庆市 | 走路挖矿形式 | 2018年11月 | 2019年8月10日，趣步“营业执照”已经被吊销，目前经营状态成撤销状态 | / |
| SKY云世纪 | 云世纪国际控股集团 | 香港 | 商城形式 | 2016年6月 | 2019年8月，湖南省石门县人民法院依法作出最终判决 | 传销骨干吸收传销资金近2亿元 |
| “一路有喜”商城（喜宝币） | 深圳一路有喜科技有限公司 | 广东省 | 商城形式 | 2017年1月 | 2019年8月，广东省深圳市南山区法院对深圳“一路有喜”特大虚拟货币网络传销案进行宣判 | 8万名会员，共涉及资金8338万余元 |
| MBI虚拟货币（M币） | 恩必爱集团 | 马来西亚 | 金融投资理财 | 2014年 | 2019年8月，广西贺州市中级法院二审宣判该网络传销案 | 500万元以上 |
| 大师币 | / | 黑龙江省 | 虚拟货币投资 | 2018年 | 2019年8月，犯罪嫌疑人已被刑事拘留 | 260余万元 |
| 比特猪 | / | / | 区块链宠物游戏 | / | 2019年8月，已立案调查 | / |
| 乐存币（NBY） | 宁波贵安企业管理有限公司 | 宁波 | 健康保健、投资理财项目 | 2019年1月 | 2019年7月，“乐存基金”项目已被立案调查 | / |
| Plustoken | / | 声称韩国 | 智能搬砖钱包 | 2018年2月 | 2019年7月，重要操盘手已归案 | / |
| 光锥币（LCC） | 南非区块链技术团队 | / | 影视数字区块链 | 2018年 | 2019年7月，大同警方破获打着投资“LCC光锥币”旗号的特大集资诈骗案 | 100余万元 |
| DCRC | / | / | 版权溯源平台 | 2019年 | 警方已立案，案件在进一步侦办中 | / |
| 金砖储备资产货币 | / | 北京 | 虚拟资产储备数字货币 | 2017年4月 | 2019年5月，被列为公安部公布的第二批61个民族资产解冻类诈骗虚假项目 | |
| 英雄链（HEC） | / | 北京 | 博彩类 | 2018年1月 | 2019年4月，珠晖公安分局破获 | 3亿余元 |
| fc积分 | 信富公司 | 浙江 | 挖矿形式 | 2015年7月 | 2019年3月，徐州市云龙区人民法院第一法庭开庭审理该案 | / |

# （三）传播勒索病毒索取比特币行为

# （四）利用数字货币跨境逃汇行为

如果有单位在境内利用人民币或外币购买比特币，又将比特币通过网络转移到境外，然后在境外汇兑成外币或人民币的，满足数额要求的情况下，就可能成立逃汇罪。




# （五）以智能合约为犯罪手段的犯罪

在信息网络犯罪阶段，犯罪分子利用网络传播信息，发布违法犯罪的信息，最终寻找被害人并锁定被害人。在价值网络阶段，犯罪分子利用智能合约招募犯罪实施者，也就是招募共同犯罪的行为人。

杀人内容

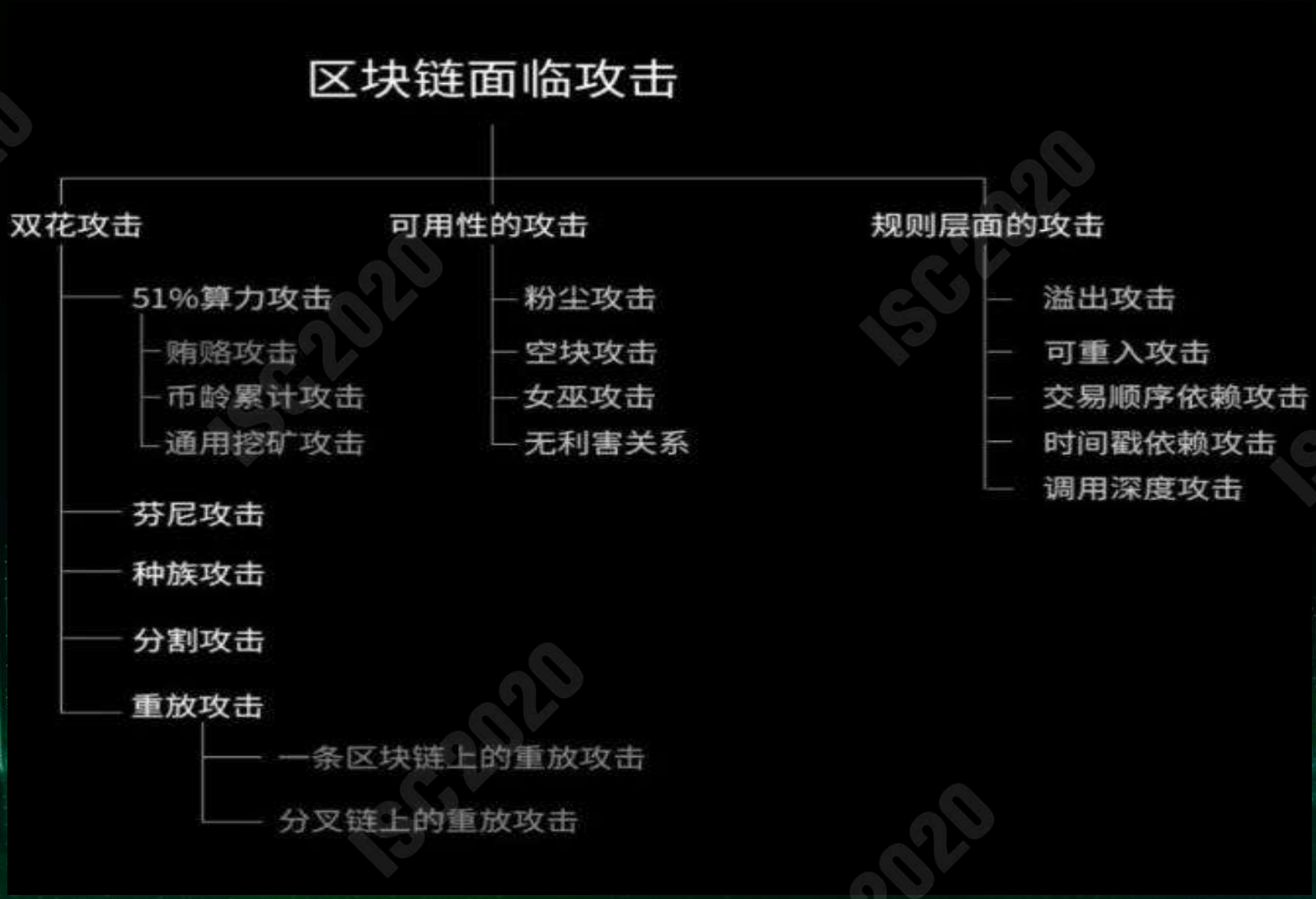
支付条件


IF( ), THEN( );

杀人属实

支付执行

# （六）以智能合约为犯罪对象的犯罪



# （七）以智能合约为犯罪空间的犯罪

## 网络舆情

Overview | Comments | Loan

Transaction Information | Tools & Utilities

| | |
|---|---|
| TxHash: | 0x2d6a7b0f6adeff38423d4c62cd8b6ccb708ddad85da5d3d06756ad4d8a04a6a2 |
| TxReceipt Status: | Success |
| Block Height: | 5490403 (1409060 Block Confirmations) |
| TimeStamp: | 237 days 14 hrs ago (Apr-23-2018 07:02:20 AM +UTC) |
| From: | 0x44938b01da1feb3f6fa1cf38870ee564e25d9bf3 |
| To: | 0x44938b01da1feb3f6fa1cf38870ee564e25d9bf3 |
| Value: | 0 Ether ($0.00) |
| Gas Limit: | 800000 |
| Gas Used By Transaction: | 599000 (74.88%) |
| Gas Price: | 0.0000000013 Ether (1.3 Gwei) |
| Actual Tx Cost/Fee: | 0.0007787 Ether ($0.07) |
| Nonce & {Position}: | 0 \| {107} |
| Input Data: | Peking University teachers and classmates:<br>How are you!<br>I am Yueluo from the 2014 Foreign Languages Institute. I was one of the eight students who submitted<br>the “Information Disclosure Application Form” to Peking University on the morning of April 9. I dragged my<br>tired body and wrote this text to illustrate some of the things that have happened to me recently |

View Input As

# （七）以智能合约为犯罪空间的犯罪

## 网络舆情

Transaction Information

Tools & Utilities

| | |
|---|---|
| TxHash: | 0xb1ed364e4333aae1da4a901d5231244ba6a35f9421d4607f7cb90d60bf45578a |
| TxReceipt Status: | Success |
| Block Height: | 6007493 (891958 Block Confirmations) |
| TimeStamp: | 147 days 18 hrs ago (Jul-22-2018 02:49:54 AM +UTC) |
| From: | 0x2aabb1f4c9e8148b8863147c81725053294f59ae |
| To: | 0xc72bd346a00f48a62cccdf4793cff8dd2c096ac8 |
| Value: | 0.001 Ether ($0.09) |
| Gas Limit: | 1000000 |
| Gas Used By Transaction: | 777432 (77.74%) |
| Gas Price: | 0.00000001 Ether (10 Gwei) |
| Actual Tx Cost/Fee: | 0.00777432 Ether ($0.67) |
| Nonce & {Position}: | 14 \| {17} |
| Input Data: | 0x2001 年，东北一家国有疫苗公司悄无声息进行改制。多年后再回首，人们才明白其中意义。<br>那年的 9 月 18 日，上市公司长春高新旗下的长生生物迎来了两位新的股东——韩刚君和杜伟民。<br><br>韩刚君用 1932 万元买下了长生生物 30% 的股权，成为第二大股东；他和杜伟民的合资公司则成为了长生的小股东。 |

View Input As

Private Note: <To access the Private Note Feature, you must be Logged In>


# THANKS

ISC 2020
第八届互联网安全大会
INTERNET SECURITY CONFERENCE 2020
数字孪生时代下的新安全
New Security in the Digital Twin Era