



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

ISC 2020 第八届互联网安全大会

> 数字孪生时代下的新安全 New Security in the Digital Twin Era





区块链概述 01

区块链安全事件态势 02

区块链犯罪案件类型 03





01

区块链概述

区块链安全事件态势

区块链犯罪案件类型





(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



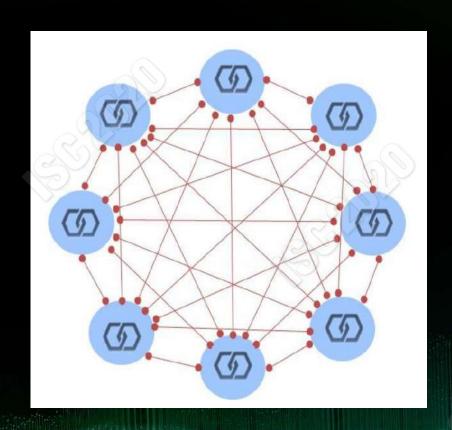


(三) 区块链的关键技术

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。



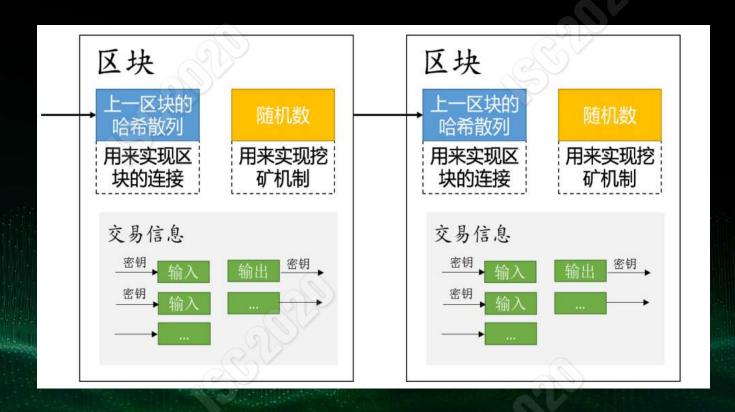




区块链的关键技术

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

Transactions

区块头

块高度: 3906 头哈希: 0000

父哈希: 0000 Merkle根 c85 时间戳: 2015 难度: 934486 Nonce: 1779

区块主体 此区块中的原

块高度: 3906 头哈希: 0000

父哈希: 0000 Merkle根 c59 时间戳: 2011 难度: 934486 Nonce: 4005

> 区块主体 此区块中的肥

块高度: 3906 头哈希: 0000

父哈希: 000 Merkle根 2e1 时间戳: 201 难度: 93448 Nonce: 2181

区块主体 此区块中的

No Inputs (Newly Generated Coins) ⇒ 3JAvzKWgtxPzcbTqKeAT7qfwoZBjtVmkBU Unable to decode output address 7e5ecb2add848dec3e68ab21c6fb6dae3e066512d2aebd239429443ec8f9c250 17A16QmavnUfCW11DAApiJxp7ARnxN5pGX ⇒ 3CdyEF3ct3EBgAcjTresqp3VhnjmVhyuAn 3QQf7ebcmfQoHiQhEJHsVN2EhJ6V3rw1c 17A16QmavnUfCW11DAApiJxp7ARnxN5p f70b258d251b4aa7c2b48ffa3f70ca445d122300bbe51a9422554979da90005d → 1HK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2 292623bf652e652c2e91df5a427b1bba3d2edda149249744eaf793841fd97221 ⇒ 1HK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2		2018-12-16 19:04:2
17A16QmavnUfCW11DAApiJxp7ARnxN5pGX 3CdyEF3ct3EBgAcjTresqp3VhnjmVhyuAn 3QQf7ebcmfQoHiQhEJHsVN2EhJ6V3rw16 17A16QmavnUfCW11DAApiJxp7ARnxN5p 470b258d251b4aa7c2b48ffa3f70ca445d122300bbe51a9422554979da90005d 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2fvz 4NK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2fvz		12.56179441 BT 0 BT
17A16QmavnUfCW11DAApiJxp7ARnxN5pGX 3CdyEF3ct3EBgAcjTresqp3VhnjmVhyuAn 3QQf7ebcmfQoHiQhEJHsVN2EhJ6V3rw16 17A16QmavnUfCW11DAApiJxp7ARnxN5p 470b258d251b4aa7c2b48ffa3f70ca445d122300bbe51a9422554979da90005d 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2fvz 1HK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2		12.56179441 BT0
3QQf7ebcmfQoHiQhEJHsVN2EhJ6V3rw10 17A16QmavnUfCW11DAApiJxp7ARnxN5p 170b258d251b4aa7c2b48ffa3f70ca445d122300bbe51a9422554979da90005d 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2fvz → 1HK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2		2018-12-16 19:01:2
1DWgeYAiPwmR2e17Kco5CwoZkDA63i2fvz 1HK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2	Brw1dE	0.001 BT 2.36259432 BT 57.84540378 BT
1DWgeYAiPwmR2e17Kco5CwoZkDA63i2fvz 1HK3bUyG43178mb68n4kse6xDXnjQHKz 1DWgeYAiPwmR2e17Kco5CwoZkDA63i2		60.2089981 BT
1DWgeYAiPwmR2e17Kco5CwoZkDA63i2		2018-12-16 19:03:3
292623bf652e652c2e91df5a427b1bba3d2edda149249744eaf793841fd97221		0.15480548 BT 0.95968672 BT
292623bf652e652c2e91df5a427b1bba3d2edda149249744eaf793841fd97221		1.1144922 BT0
		2018-12-16 19:00:1
1KxWinv1A3UDMfgdMKtY8dsfR1V79WhJsx 1LnnvsWka8APXyx7i3QKPvn1xqNMVGhN 1EhWELZePTaQSursPr5pUNVwVGYC8fABLi 1FFoFtQfvHNVxXEbETuW9WJQKCY9dLN		0.00924944 BT 0.05247019 BT

首尾相连

的一个数





(三) 区块链的关键技术

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。

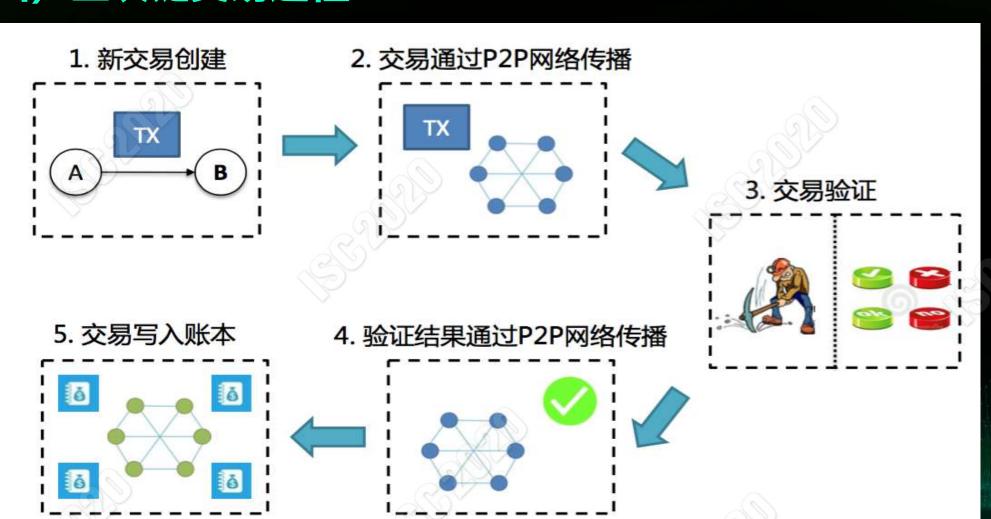
共识机制

```
php
$header_hex
                   "01000000"
                                . // version
              // previous block hash
              "81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a30800000000000"
              // merkle root hash of transactions in this block
              "e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b"
              // Time
              "c7f5d74d"
             // Bits (Difficulty)
              "f2b9441a"
              // Nonce
              "42a14695";
              = pack("H*", $header_hex); // hex to bin
Sheader bin
         hash('SHA256', hash('sha256', $header_bin, true), true); // double sha256
echo bin2hex($h), "\n";
// output: 1dbd981fe6985776b644b173a4d0385ddc1aa2a829688d1e0000000000000000
echo bin2hex(strrev($h)), "\n";
// output: 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
```





区块链交易过程







区块链发展

- 电子货币
- 去中心化交易

区块链1.0

区块链2.0

- 智能合约
- 数字资产
- 去中心化在各行业应用

- 去中心化互联网平台 BaaS
- 去中心化社会治理
- 去中心化应用DAPP

区块链3.0





区块链概述

02

区块链安全事件态势

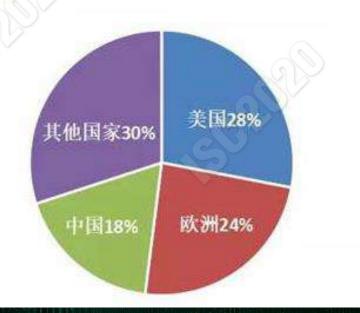
区块链犯罪案件类型

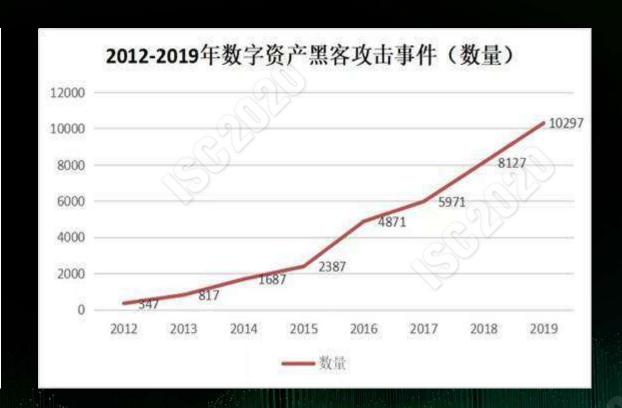




2019年全球区块链安全事件统计

全球数字资产犯罪案件数量(占比)

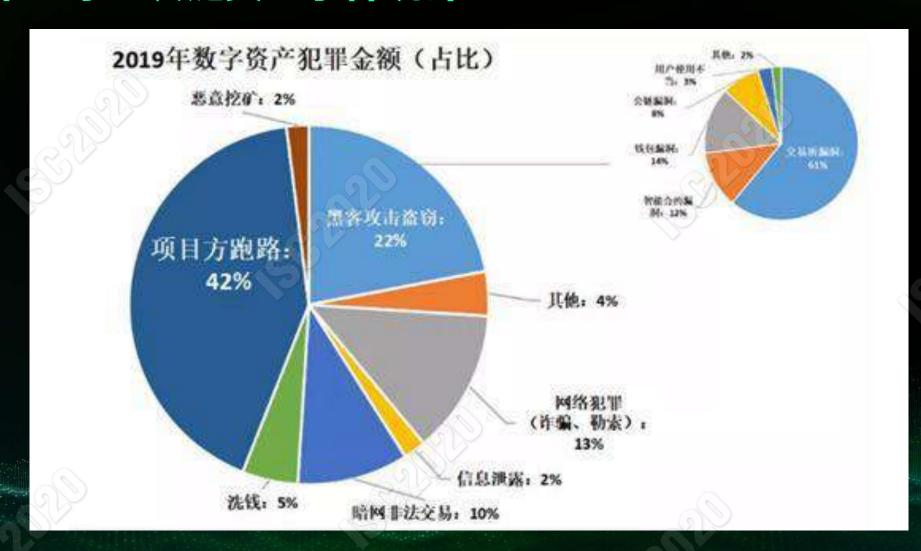








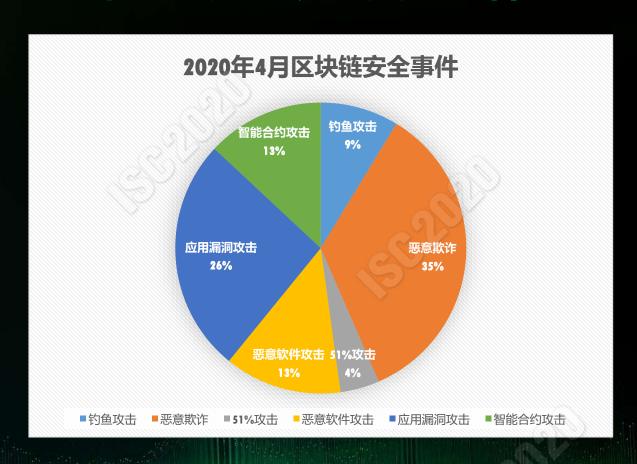
2019年全球区块链安全事件统计

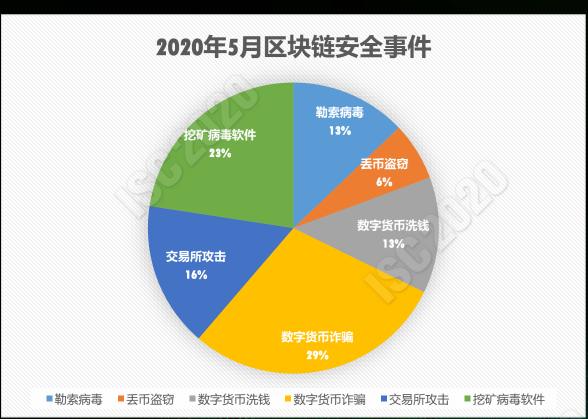






2020年4、5月区块链安全事件









区块链概述

区块链安全事件态势

区块链犯罪案件类型 03





(一)利用虚拟货币开展非法集资

• 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

运作模式 虚拟货币

点击旅看评情〉

恒星币

马克币

• 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

云数贸-五行币

信息来源 公安部

相关报道 公安部: "五行币" 系列传销组织头 目宋密秋从印尼被琅捕归案

运作模式 虚拟货币

点击查看详情》

齐齐哈尔市铁锋公安分局

相关报道 男子创建"菜汇币" 手机APP 非法集 资3000多万被抓获

运作模式 虚拟货币

点击直看详情〉

亚欧市

• 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

• 运作模式 虚拟货币

点击查看详惯〉

麦加币

• 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

露克市

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

• 运作模式 虚拟货币

点击资蜀详情〉

维卡币

相关报道 全国公安机关采取强力措施持续严打

• 运作模式 虚拟货币

点击宣看详情〉

皇尊市

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

· 信息来源 公安部

运作模式 虚拟货币

点击查看洋债〉

点击查看详情〉

克拉币

· 信息来源 湖南省常徳市公安局

常德破获美国未来城"万福币"特大

运作模式 虚拟货币

点击查看详情。







• 信息来源 公安部

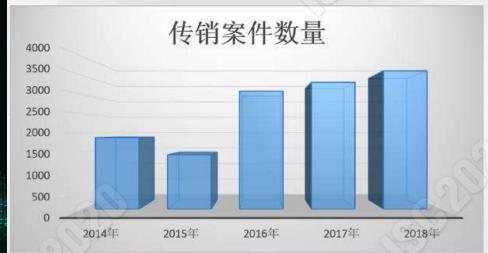






(二) 利用虚拟货币开展网络传销





	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
внв	一些集局外	1	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
建步	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 经被用销,目前经营状态成撤销状态	1
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
大师市	10	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	1-35	2019年8月,已立案调查	1
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	1
光锥币 (LCC)	南非区块链技术 团队	1	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	V.	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)	1	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	180





(三) 传播勒索病毒索取比特币行为

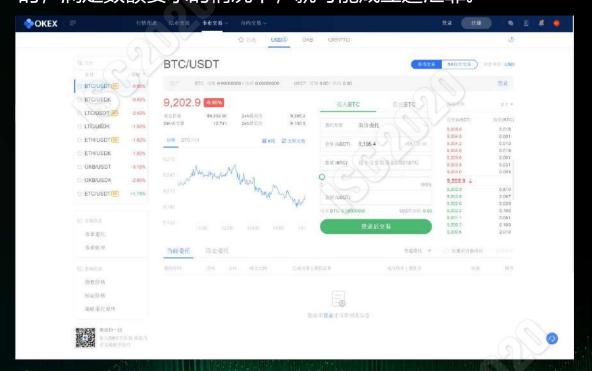






(四) 利用数字货币跨境逃汇行为

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 土/***

支付执行







(六) 以智能合约为犯罪对象的犯罪

区块链面临攻击

分叉链上的重放攻击







(七) 以智能合约为犯罪空间的犯罪

网络舆情

Overview Comments		Loan ▼
Transaction Information 3 9		Tools & Utilities ▼
TxHash: TxReceipt Status: Block Height: TimeStamp: From:	0x2d6a7b0f6adeff38423d4c62cd8b6ccb708ddad85da5d3d06756ad4d8a04a6a2 Success 5490403 (1409060 Block Confirmations) 237 days 14 hrs ago (Apr-23-2018 07:02:20 AM +UTC) 0x44938b01da1feb3f6fa1cf38870ee564e25d9bf3	
To: Value: Gas Limit:	0x44938b01da1feb3f6fa1cf38870ee564e25d9bf3 0 Ether (\$0.00) 800000	
Gas Used By Transaction: Gas Price:	599000 (74.88%) 0.000000013 Ether (1.3 Gwel)	
Actual Tx Cost/Fee: Nonce & {Position}:	0.0007787 Ether (\$0.07) 0 {107}	
Input Data:	Peking University teachers and classmates: How are you! I am Yueluo from the 2014 Foreign Languages Institute. I was one of the eight students who s the "Information Disclosure Application Form" to Peking University on the morning of April 9 tired body and wrote this text to illustrate some of the things that have beenned to me recovery lines.	. I dragged my





(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	
То:	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情无声息进行改制。多年后再回首, 人们才明白其中意义。 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。	Ê
	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: 0	<to access="" be="" feature,="" in="" logged="" must="" note="" private="" the="" you=""></to>	





第八届互联网安全大会 360互联网安全中心

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