




# 区块链中暗网情报对抗反洗钱模型

北京众享比特科技有限公司

2016年12月

# 内容提要

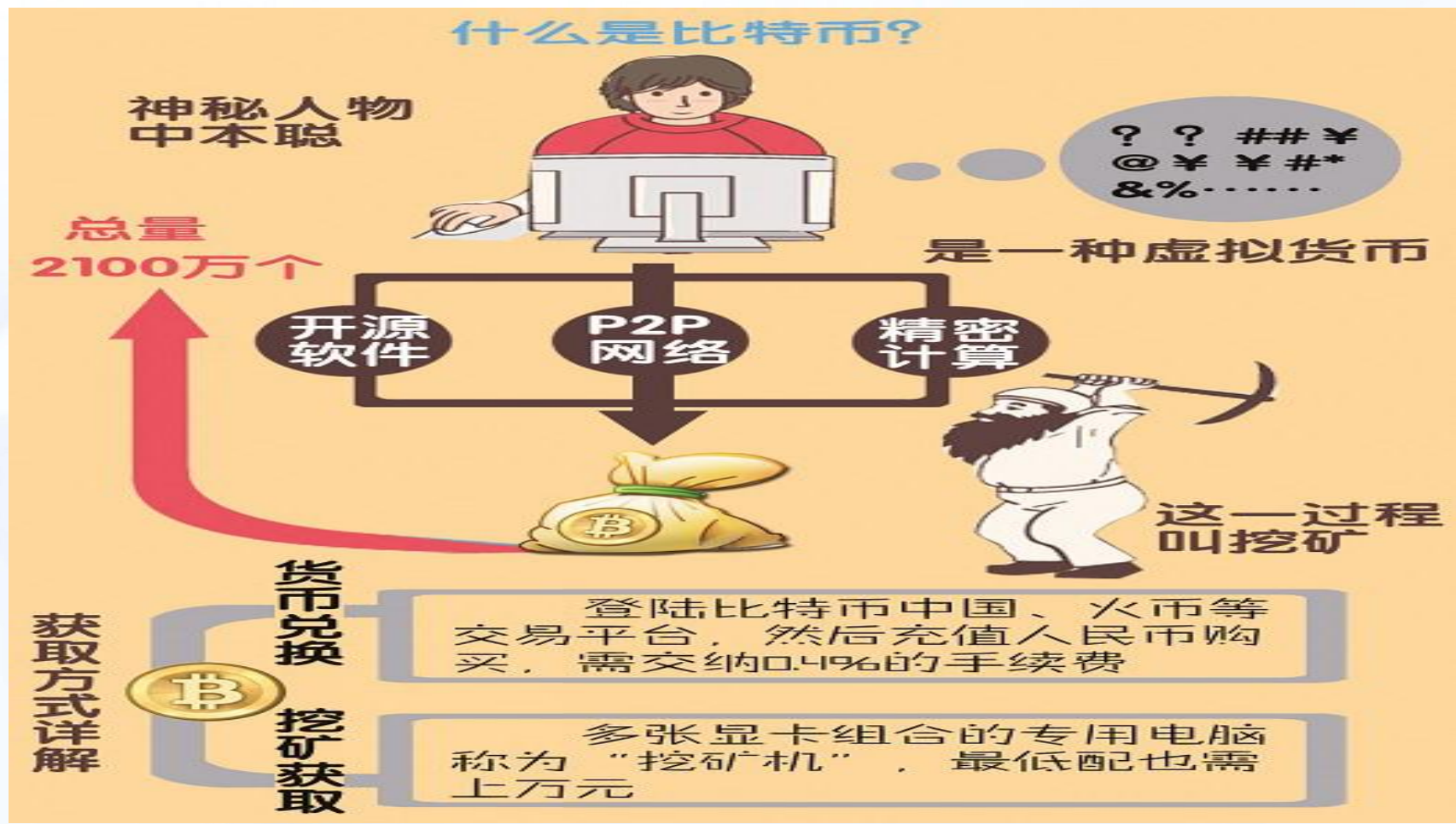
- 
- 区块链暗网现状
  - 反洗钱模型探讨
  - 众享比特公司介绍

# 数字货币交易发展现状

- 全世界645种数字货币总市值达到125亿美元。比特币大概占了100亿美元市值。
- 数字加密货币交易大部分通过传统金融机构来完成。
- 全世界犯罪份子通过大量数字加密货币交易活动用于洗钱。



# 什么是比特币

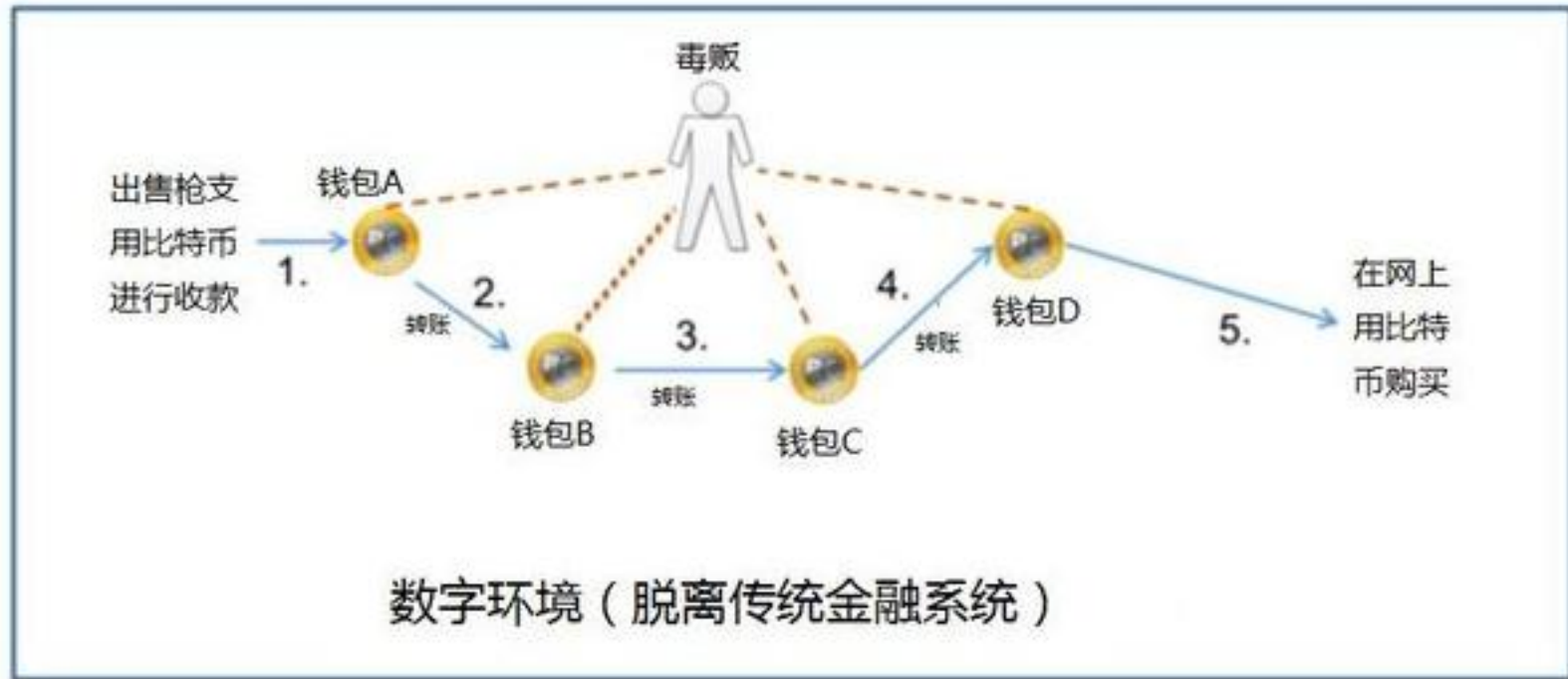


# 比特币洗钱犯罪案例

- 2015年10月香港富商黄煜坤遭绑架，绑匪要求以“比特币”支付赎金7000万元港币
- 比特币在台湾并不被视为有效货币，且具有高度私密性
- 赎金只要付出，根本无法追踪，“比特币比人头户还难追”。



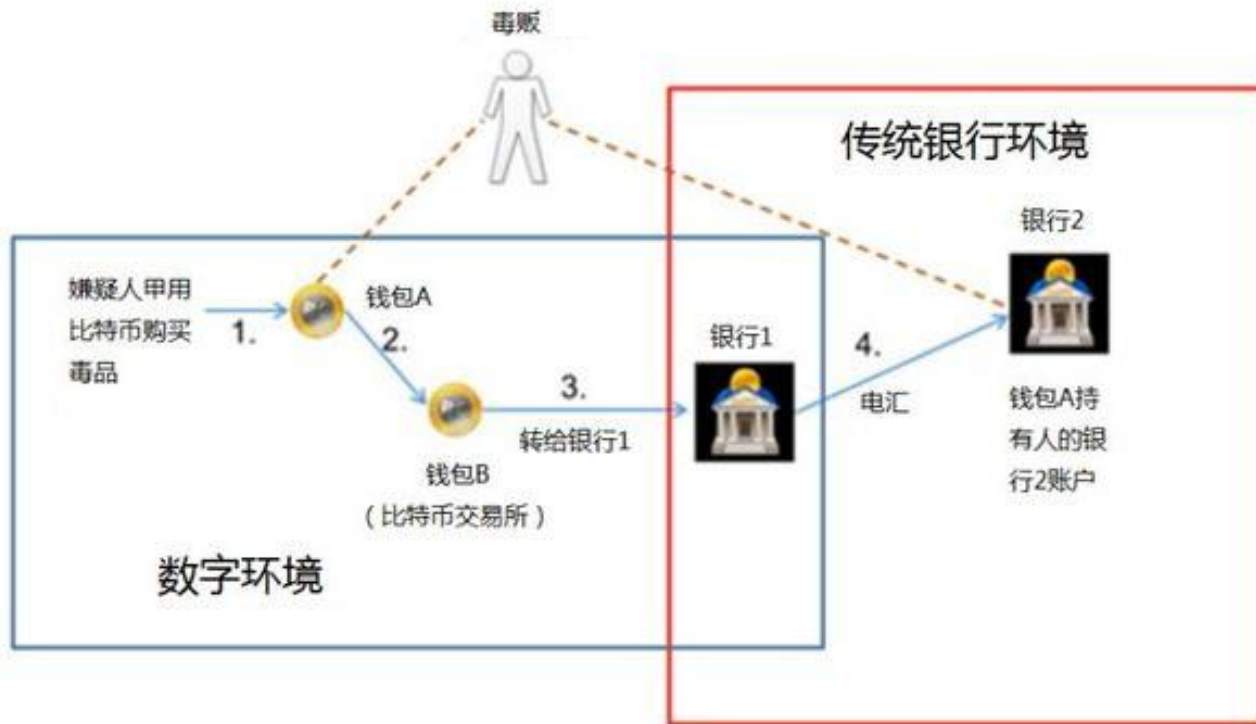
# 加密交易的独立式环境



数字货币通过不同虚拟钱包进行转移，最后用于在线零售平台的购买。这种方式同银行这类传统金融机构没有联系。



# 加密交易的交互式环境



数字货币通过不同虚拟钱包转移，最终转换成法定货币并电汇给传统金融机构。

# 暗黑币

- 与比特币类似，但是它有一个特性就是能够在很大程度上掩盖转账痕迹
- 你可以把暗黑币从一个账户A转移到另一个账户B
- 你使用账户B里的暗黑币兑换现金时，网警不能发现这些钱是从账户A转移过去的





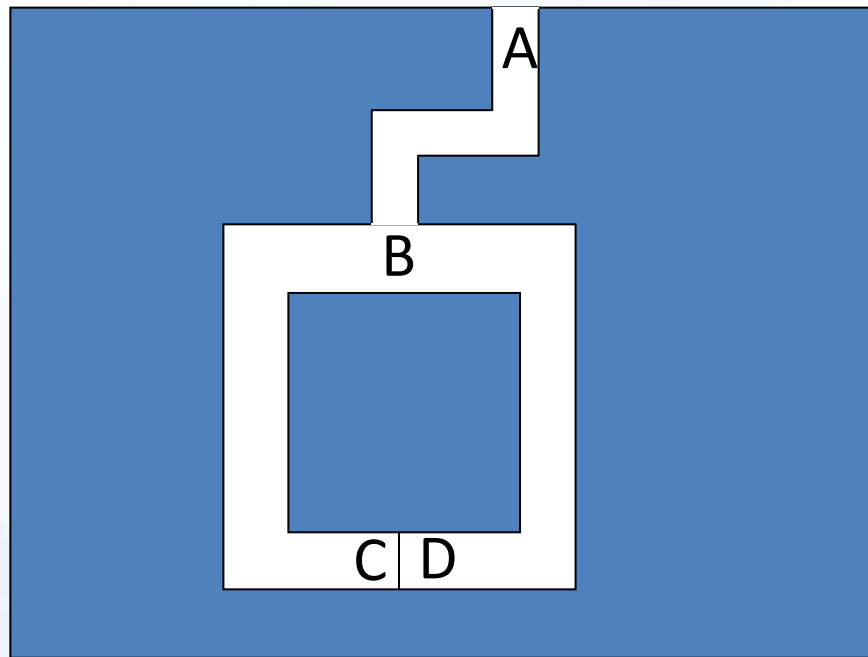
- 2016年10月号称终极匿名的Zcash发布。采用了零知识证明技术。
- “如果说比特币有95%的匿名性，那么Zcash就有100%的匿名性。它可以保证支付的完全机密，同时通过公共区块链维护去中心化网络的运行。
- 和比特币不同，Zcash交易可以隐藏区块链上的发送人、接收人以及交易金额。
- 有正确浏览密钥的人才可以看到交易信息。用户可以完全掌控并选择向谁提供这个浏览密钥。




座右铭：“万币的产生皆平等”。

# 零知识证明

- (1) V 站在 A 点。
  - (2) P 一直走到迷宫深处，随即选择 C 点或者 D 点。
  - (3) 在 P 消失后，V 走到 B 点。
  - (4) V 向 P 喊叫，要她：从左通道出来，或者从右通道出来。
  - (5) P 答应了，如果有必要她就用秘密口令打开密门。
- P 和 V 重复第(1)至第(5)步  $n$  次。



# 内容提要

- 
- 区块链暗网现状
  - 反洗钱模型探讨
  - 众享比特公司介绍

- 比特币是完全匿名的吗？

用户可以开多个比特币地址，并且地址跟他现实生活中的真实身份没有任何联系，因而具有一定匿名性，被广泛运用于洗钱和违禁物品交易，不过这一特性实为“伪匿名”，比特币的交易仍可以追本溯源到交易者本身。

- 如何进行比特币交易追踪？

比特币的交易历史是完全公开的，所有人都可以通过你的钱包地址在区块链中查询你的钱包现金流入与流出，并可向上追溯至这些比特币的终极起源，即从区块生成后发送到的那个地址。

# 比特币交易追踪原理

- 比特币整个支付网络中所发生的每一笔交易都会被记录在“区块链”（blockchain）中——这是比特币货币体系用以追踪谁何时拥有哪些比特币，以及防止欺诈和伪造的分散化交易记录机制。



<b>Block Chain</b>		<b>区块链</b>	
Magic Number	4	魔数	0xD9B4BEF9
Block Size	4	区块大小	
Block Head	80	区块头	
Block Body	-	区块体	
<b>Block Head</b>		<b>区块头</b>	
Version	4	区块头版本	
Prev Block Hash	32	前一区块头hash256	hash256(x)=sha256 sha256(x))
Merkle Root Hash	32	交易内容hash256	
Time	4	UNIX时间戳	从1970年1月1日起的秒数
Bits	4	目标值	用以标注挖矿难度
Nonce	4	随机数	用以调整当前区块头hash
<b>Block Body</b>		<b>区块体</b>	
Transactions Counter	1-9	交易单数量	Variable Integer类型
Merkle Root	-	交易单内容	
<b>Merkle Root</b>		<b>交易单内容</b>	
Transactions 1	-	交易单1	挖矿奖励（Coinbase）
Transactions 2	-	交易单2	
<b>Transactions</b>		<b>交易单</b>	
Version	4	交易单版本	
Inputs Counter	1-9	收入单数量	Variable Integer类型
Inputs Detail	-	收入单内容	
Outputs Counter	1-9	支出单数量	Variable Integer类型
Outputs Detail	-	支出单内容	
Lock Time	4	锁定时间	从当前时间起无法用于支出的秒数
<b>Inputs Detail</b>		<b>收入单内容</b>	
Inputs 1	-	收入单1	
Inputs 2	-	收入单2	
...	...	...	
<b>Outputs Detail</b>		<b>支出单内容</b>	
Outputs 1	-	支出单1	
Outputs 2	-	支出单2	
...	...	...	
<b>Inputs</b>		<b>收入单</b>	
Previous tx Hash	32	引用交易单hash	
Previous Output Index	4	引用交易单支出单索引号	
Inputs Script Length	1-9	收入脚本长度	Variable Integer类型
Inputs Script	-	收入脚本	
Sequence Number	4	序列号	0xFFFFFFFF
<b>Outputs</b>		<b>支出单</b>	
Amount	8	比特币数量	单位：1聪=0.00000001比特币
Script Length	1-9	支出脚本长度	Variable Integer类型
Script	-	支出脚本	



# 区块中输入输出信息

## Transactions

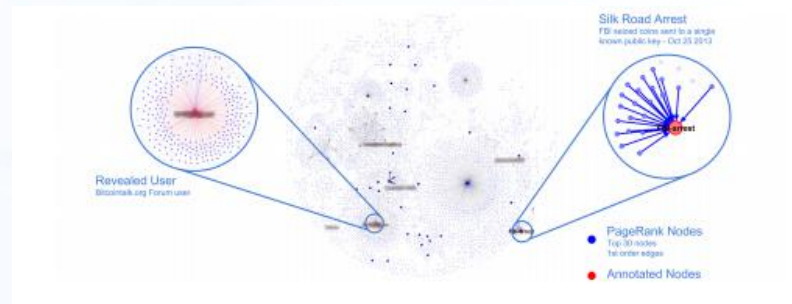
Transaction	Fee	Size (kB)	From (amount)	To (amount)
<a href="#">51d37bdd87...</a>	0	0.135	Generation: 50 + 0.01 total fees	<a href="#">15nNvBTUdMaiZ6d3GWCeXFu2MagXL3XM1q</a> : 50.01
<a href="#">60c25dda8d...</a>	0	0.259	<a href="#">1HuppjXz7dPrt2a67LqacDW5T4VanFrpqC</a> : 29.5	<a href="#">1B8vkT58i8KUPVJvvyQfrbc8Wjwu3vEarQ</a> : 0.5 <a href="#">1BQbxzgRSLEsmv1JNc8MG76wdUgMwbsaww</a> : 29
<a href="#">01f314cdd8...</a>	0.01	0.617	<a href="#">1NdzSE6sHubscXJrv7jJn2gd4fL9L3ai6E</a> : 0.03 <a href="#">1Jjv9m5VrRUE7VoktCsj18KUSqkqchhbum</a> : 0.02 <a href="#">1HsYJJPqTn34DEjMnTb3VfKckX7ZcWPibm</a> : 4.82	<a href="#">175FNxcLc1YrTwwG6TcsywcsHYdVqyhbwc</a> : 0.01 <a href="#">1MueNMRJmcqVQeqE7v4dqogpNbhyxqq8R6</a> : 4.85
<a href="#">b519286a10...</a>	0	0.404	<a href="#">12DCoCVvDCkQShZ5RTh9bysgCkmkRMNQbT</a> : 0.14 <a href="#">13CJwnnXJPwkzY4Xnaoqf8dnyNBwrHG9fe</a> : 0.01	<a href="#">1Mos7p8fqJKBcYNRG1TdT5hBRxdMP6YHPy</a> : 0.15

# Tor网络攻击

1. 伪装成特定用户并通过比特币P2P网络进行发送“畸形”消息。
1. 这些错误消息会增加Tor网络对某个IP的错误计数，当错误消息足够多时，会导致该IP被Tor网络封禁24小时。
1. 目标用户也会被Tor服务器群封禁。最终该用户只能通过正常方式连接比特币服务器。
2. 当用户连接比特币服务器时，其IP地址就会暴露出来。



- 通过网页爬虫技术获取比特币交易网站的交易商品信息（商品类别、数量、时间、图片等）和用户信息。
- 现有爬虫对抓取目标的描述可分为：基于目标网页特征、基于目标数据模式和基于领域概念。
- 网页分析算法：基于网络拓扑结构、基于网页内容、基于用户访问行为。
- 通过网页爬虫技术可以抓取和提取违法交易。



# 交易网络监控分析

- 通过对网络的监控交易用户的TCP/IP信息，获取用户的IP地址。
- 通过对比特币交易网站、比特币论坛等社区的监控，例如电子邮件地址、发货地址、信用卡和银行账户细节,IP地址、公钥地址等信息。
- 把IP地址信息、用户账号信息和公钥地址关联。



比特币虽说有一定的匿名性，但其所有交易都是公开的，加上中国政府几乎能监控到所有的现实社会。所以，中国政府要对比特币进行监管，其实不难，甚至比传统的交易方式更加容易监管。

- 1、比特币交易网站实名化
- 2、大数据
- 3、监管数据节点
- 4、全民监管

# 国际反洗钱联盟

- 2016年八月加拿大多伦多举办的区块链、数字加密货币以及反洗钱大会。与会人员超过100个，均来自大型金融机构、执法部门以及监管机构，还有区块链社区。
- 一套统一的方案可以帮助建立较强的知识基础以及标准的术语。促成关键的伙伴关系，从而用于检测反洗钱可能性。
- 区块链联盟是美国的一个公私论坛，由广大公司及组合联合组成，联盟的目的是加强区块链及加密货币方面的知识，提高执法部门的调查效率。





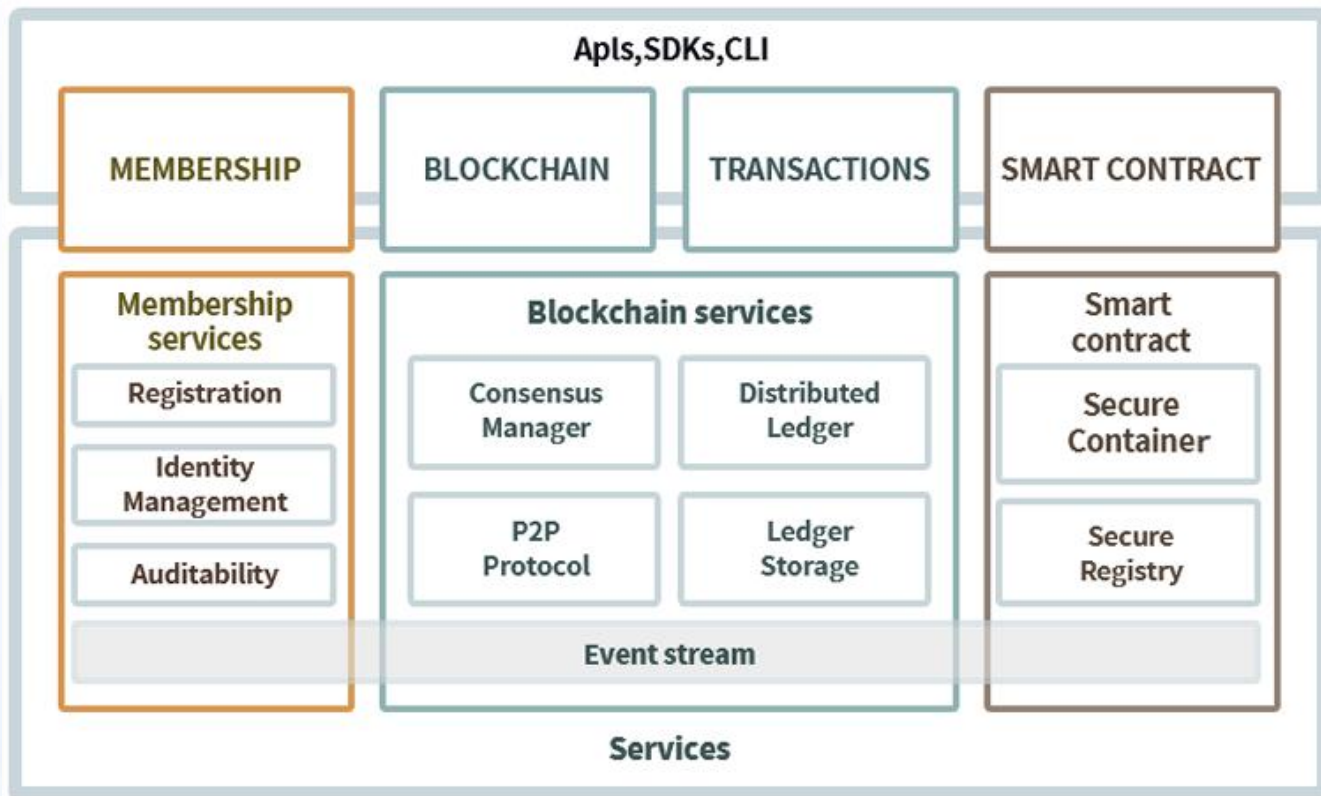
# 内容提要

- 区块链暗网现状
- 反洗钱模型探讨
- 众享比特公司介绍

# PeerSafe对区块链的视角（1）



# PeerSafe对区块链的视角（2）





# THANK YOU!



[www.peersafe.cn](http://www.peersafe.cn)