区块链技术分享

工作原理、数据结构、算法

什么是区块链?

- 为什么会出现区块链技术?
- 区块链的原理、数据结构是什么?
- 区块链可以应用在哪些地方?

原始金融体系

原始金融体系

传统金融体系

- 现金体系
- 信用体系

传统金融体系-现金体系

现代传统金融体系-现金体系

- 现金支付
- 支票支付
- 本票支付
- 汇票支付

现代传统金融体系-信用体系

- 信用卡支付

信用卡支付如何保障支付安全?

- 本质
- 信用
- 一般
- 基于

能证明持卡人身份

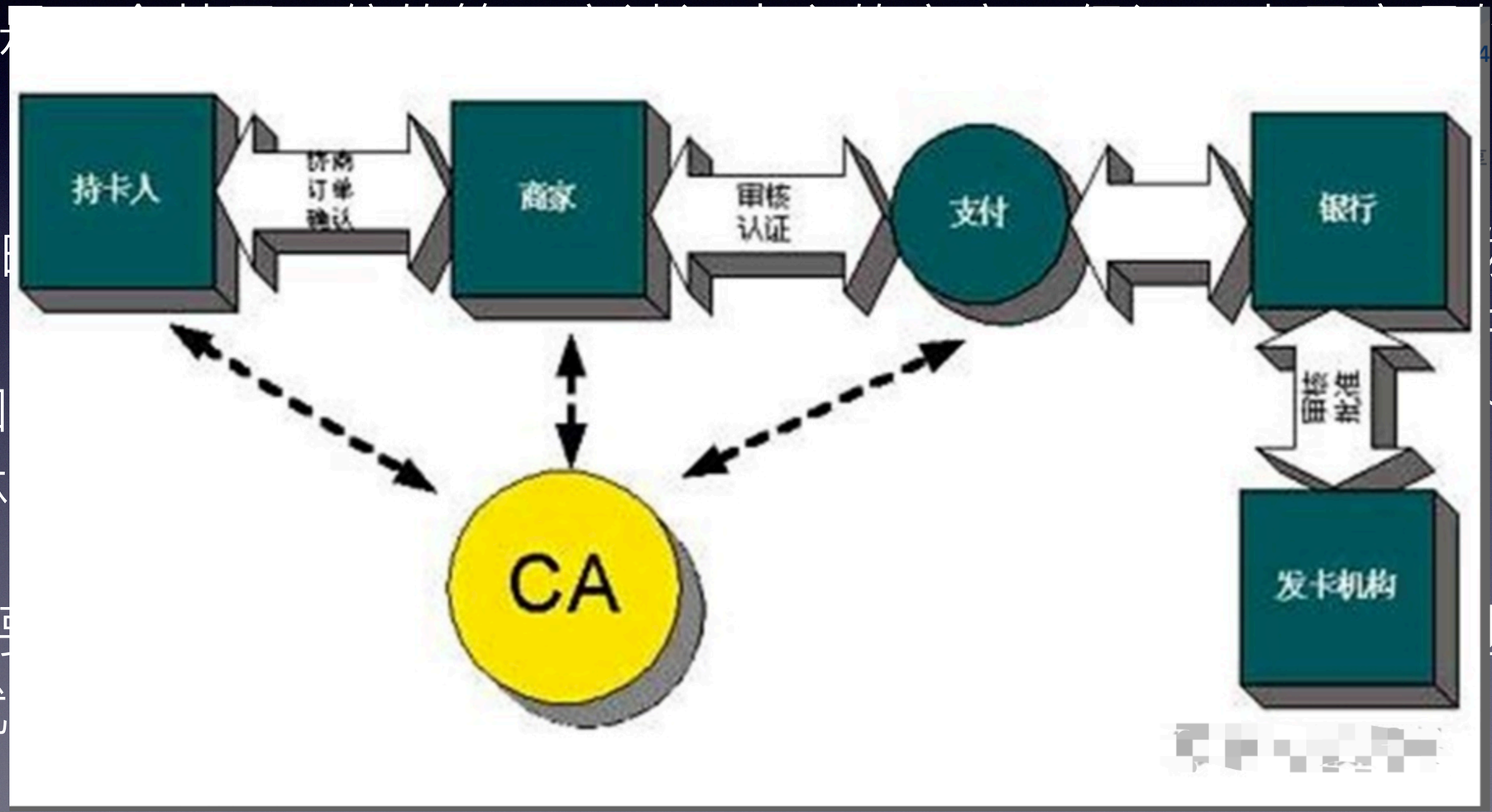
、收单机构、清算机构

网络信用卡

- SET体系(Secure Electronic Transaction,电子安全交易协议)
- HTTPS

SET体系

- SET
- SET
- SET



HTTPS

Protocol	Length	Info
TCP	108	63043 → 440 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256
TCP	108	440 → 63043 [SYN, ACK] Seq=0 Win=65535 Len=0 MSS=654
TCP	84	63043 → 440 [ACK] Seq=1 Ack=1 Win=525568 Len=0
TLSv1.2	1118	Client Hello
TCP	84	440 → 63043 [ACK] Seq=1 Ack=518 Win=525568 Len=0
TLSv1.2	1862	Server Hello, Certificate, Server Hello Done
TCP	84	63043 → 440 [ACK] Seq=518 Ack=890 Win=524544 Len=0
TLSv1.2	720	Client Key Exchange, Change Cipher Spec, Encry
TCP	84	440 → 63043 [ACK] Seq=890 Ack=836 Win=525056 Len=0
TLSv1.2	186	Change Cipher Spec, Encrypted Handshake Message

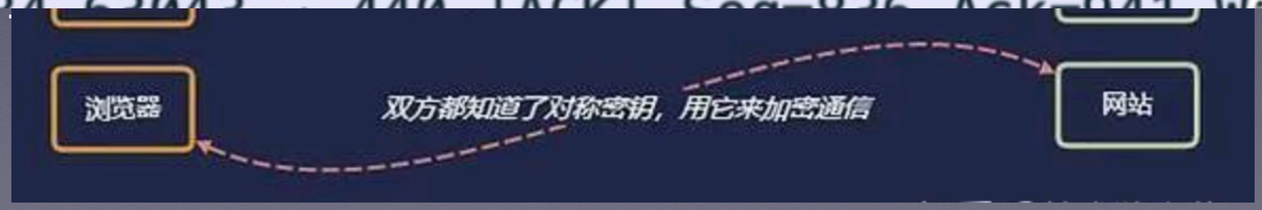
TCP 三次握手

TLS 第一次握手

TLS 第二次握手

TLS 第三次握手

TLS 第四次握手



密码学

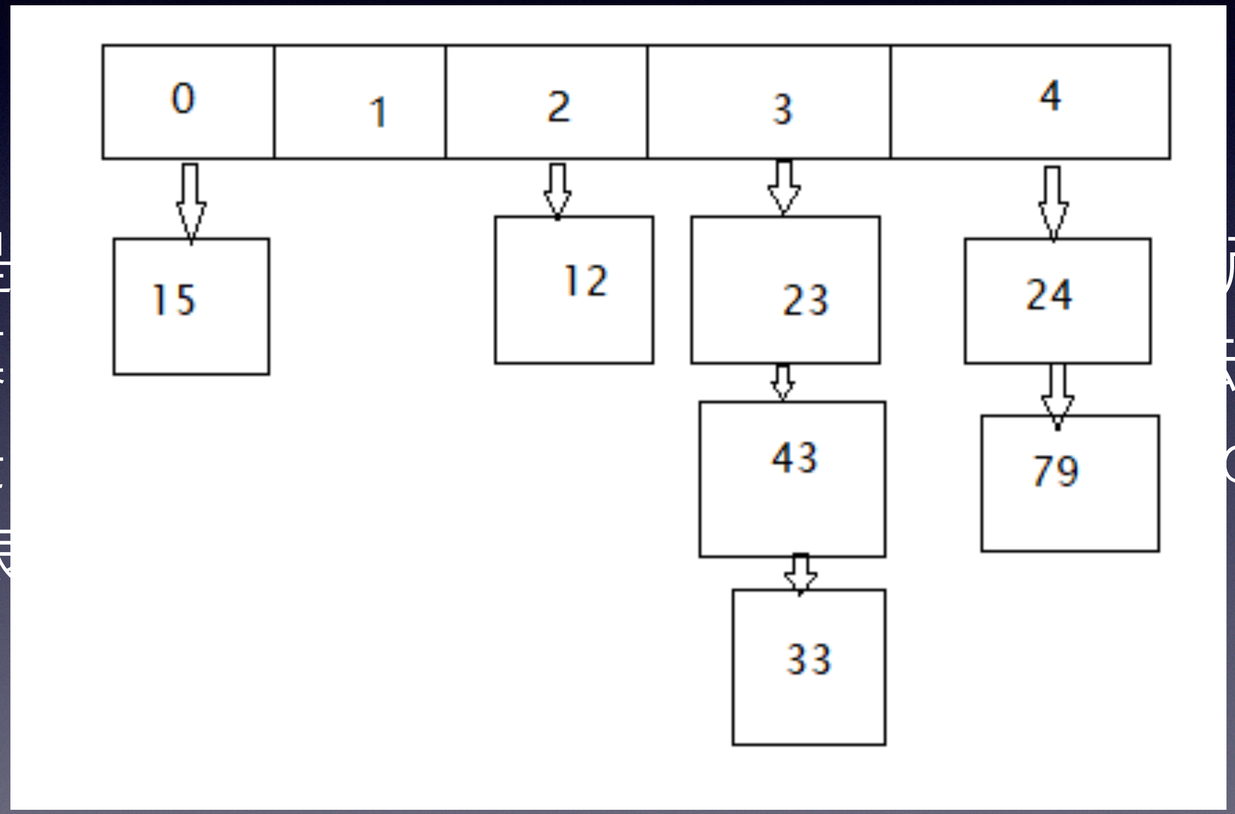
- 密码学是研究编制密码和破译密码的技术科学
- 具有机密性、完整性、身份验证、不可抵赖性特点
- 由明文、密文、密钥组成

数据加密算法

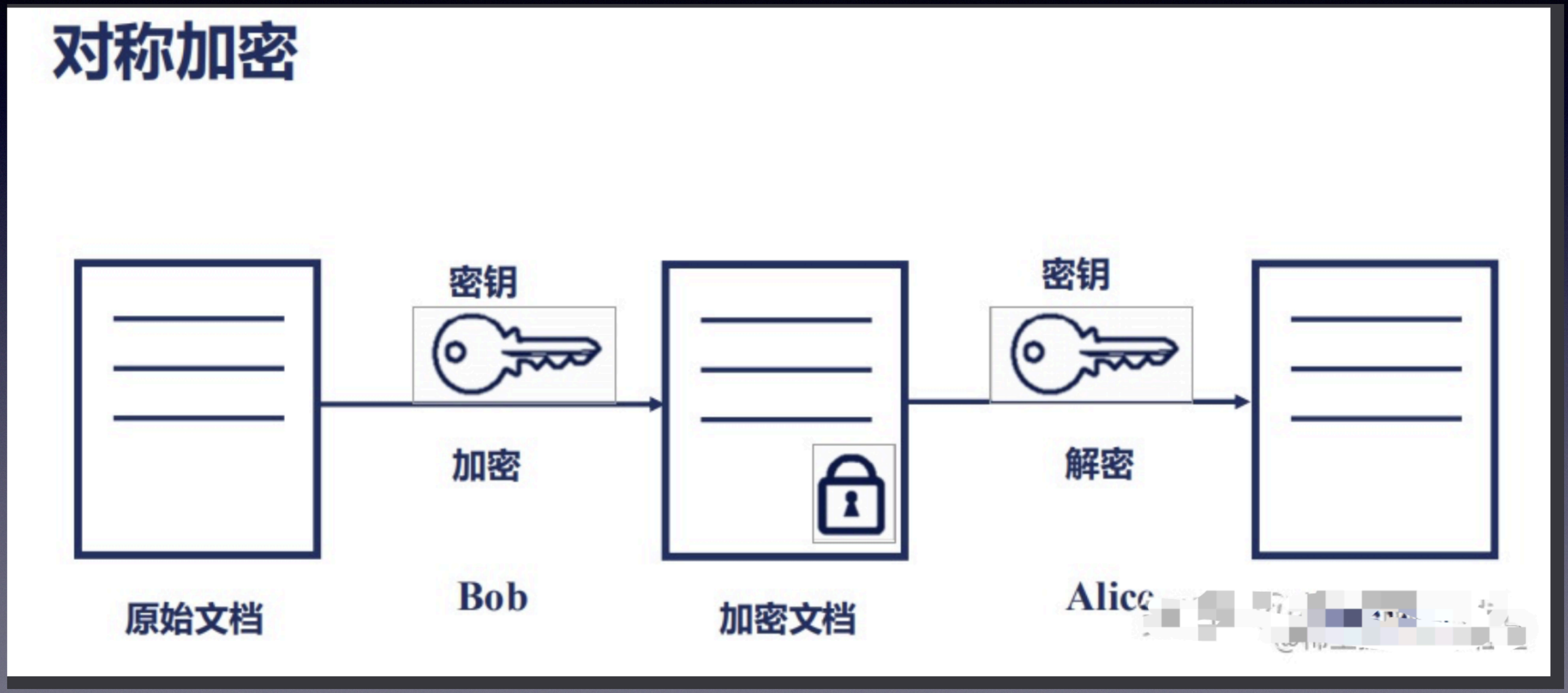
- 杂凑算法(哈希散列算法、摘要算法)
- 对称加密
- 非对称加密

消息摘要算法

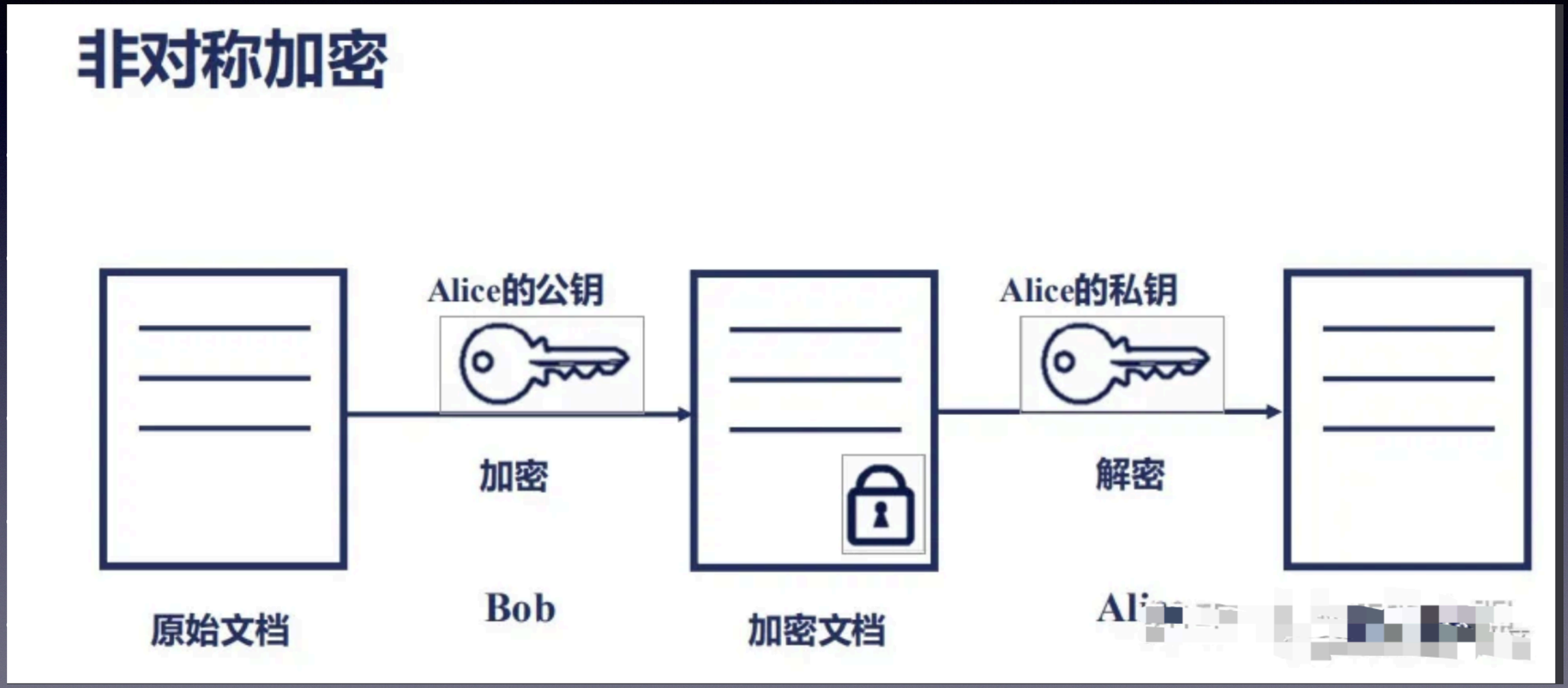
- MD5 用的是 产生 信息摘要，以 防止被篡 而是 摘要算法。 无论是 bits 的一个散列值串 (通常表



对称加密



非对称加密



数字签名

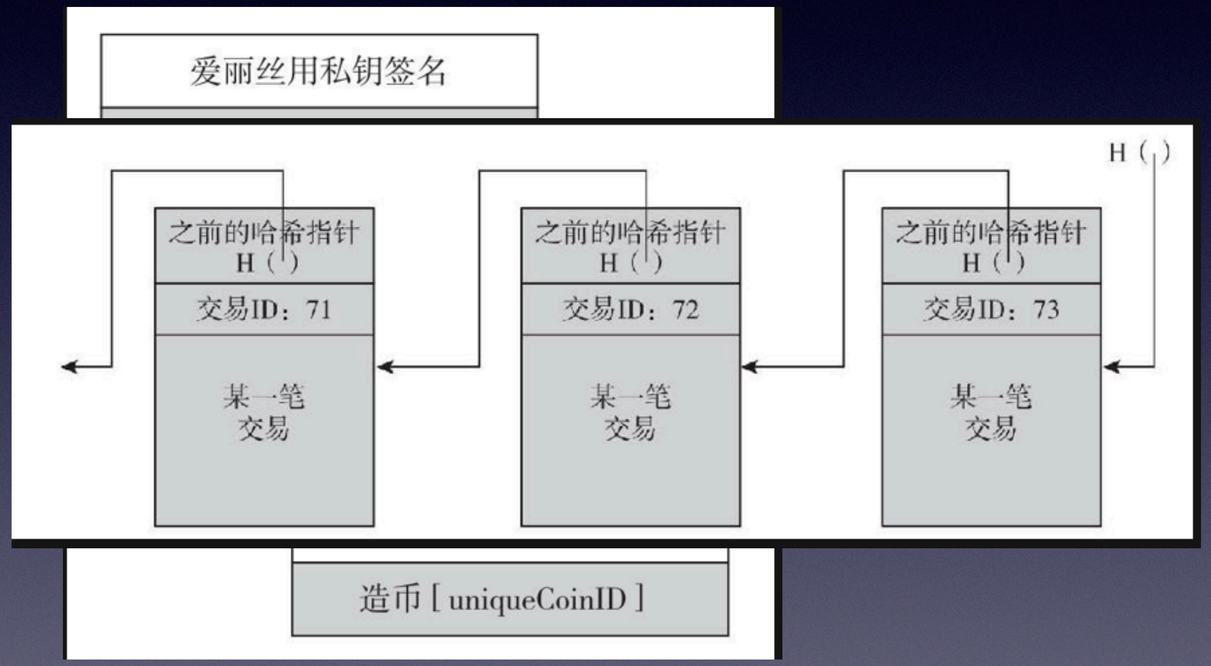
- 数字签名技术是基于非对称加密技术之上的，是非对称加密技术的组成部分
- 签名过程是用私钥加密，验证过程则是用公钥对签名解密，再和消息作对比(对签名解密无法恢复出任何关于消息的信息，解密出来的只是消息的摘要，通过解密后的消息摘要与签名重新计算作对比，此过程只能用于验证消息来源身份)

为什么会出现区块链

- 密码朋克发动了两场运动:
- 1. 自由主义(没有或者极少政府干预会让社会更好)
- 2. 自由主义+强加密，产生公钥密码学
- 密码朋克推动了加密技术的发展，并为接下来去中心化电子现金货币的演进提供理论指导

为什么会出现区块链

- 高飞币
- 财奴币

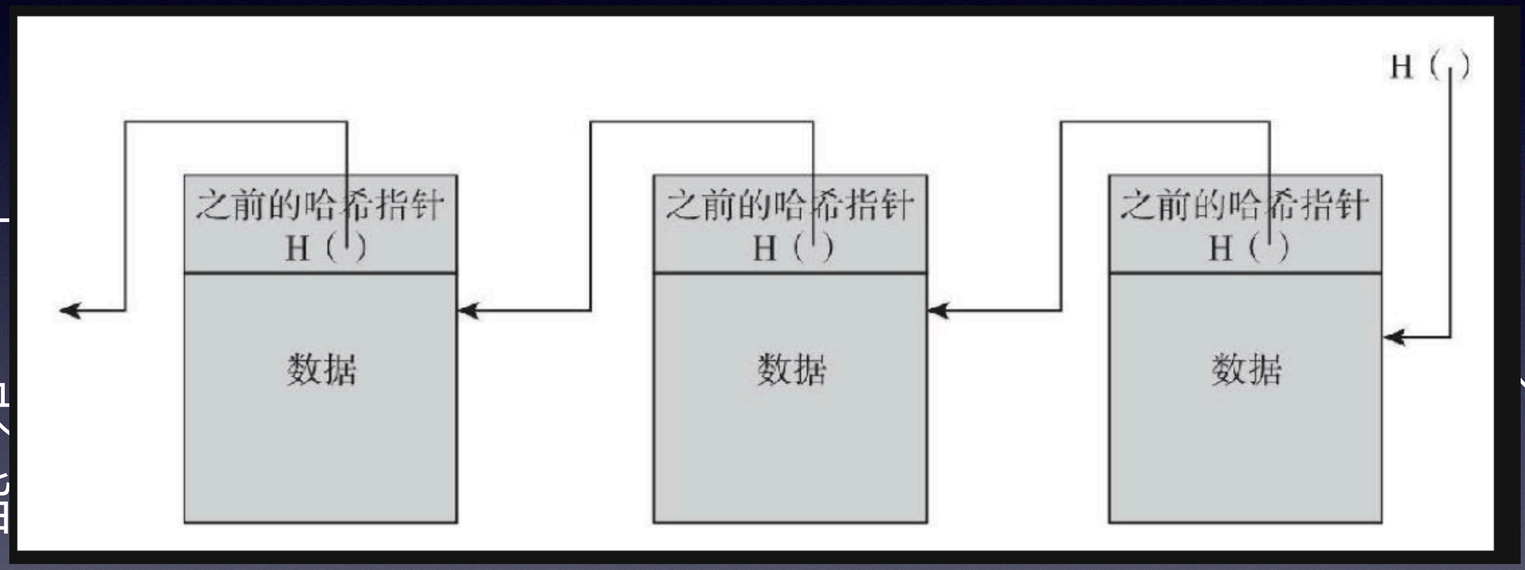


什么是区块链?

- 通过哈希指针而不是普通指针构建的一个链表，就是区块链
- 那什么是区块?

哈希指针

- 一个指针
- 每个区块 上一个区块指针指



哈希指针

- 一般哈希
- 必须具备
- 1） 碰撞
希函数H具有碰撞阻力
- 2）隐秘性
概率分布，在给定H（r||x
- 3）谜题友
果无法找到一个可行的方
称哈希函数H为谜题友好。

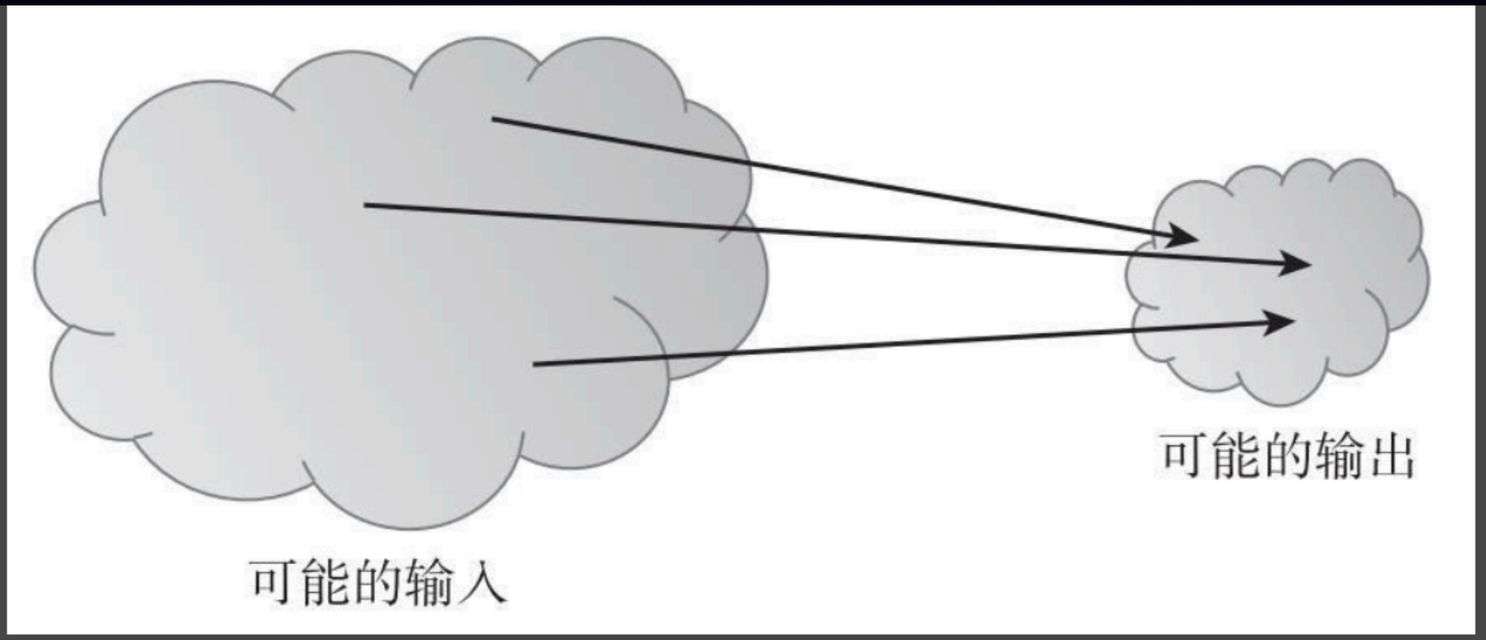


图1.2 必然的碰撞

注：因为输入的数量超过输出的数量，我们可以确定某一个输出肯定对应多个输入。

真实区块头数据


```
{
    "hash": "000000000003ba27aa200b1cecaad478d2b00432346c3f1f39
    86da1afd33e506",
    "ver": 1,
    "prev_block": "000000000002d01c1fccc21636b607dfd930d31d01c3
    a62104612a1719011250",
    "mrkl_root": "f3e94742aca4b5ef85488dc37c06c3282295ffec96099
    4b2c0d5ac2a25a95766",
    "time": 1293623863,
    "bits": 453281356,
    "nonce": 274148111
}
```

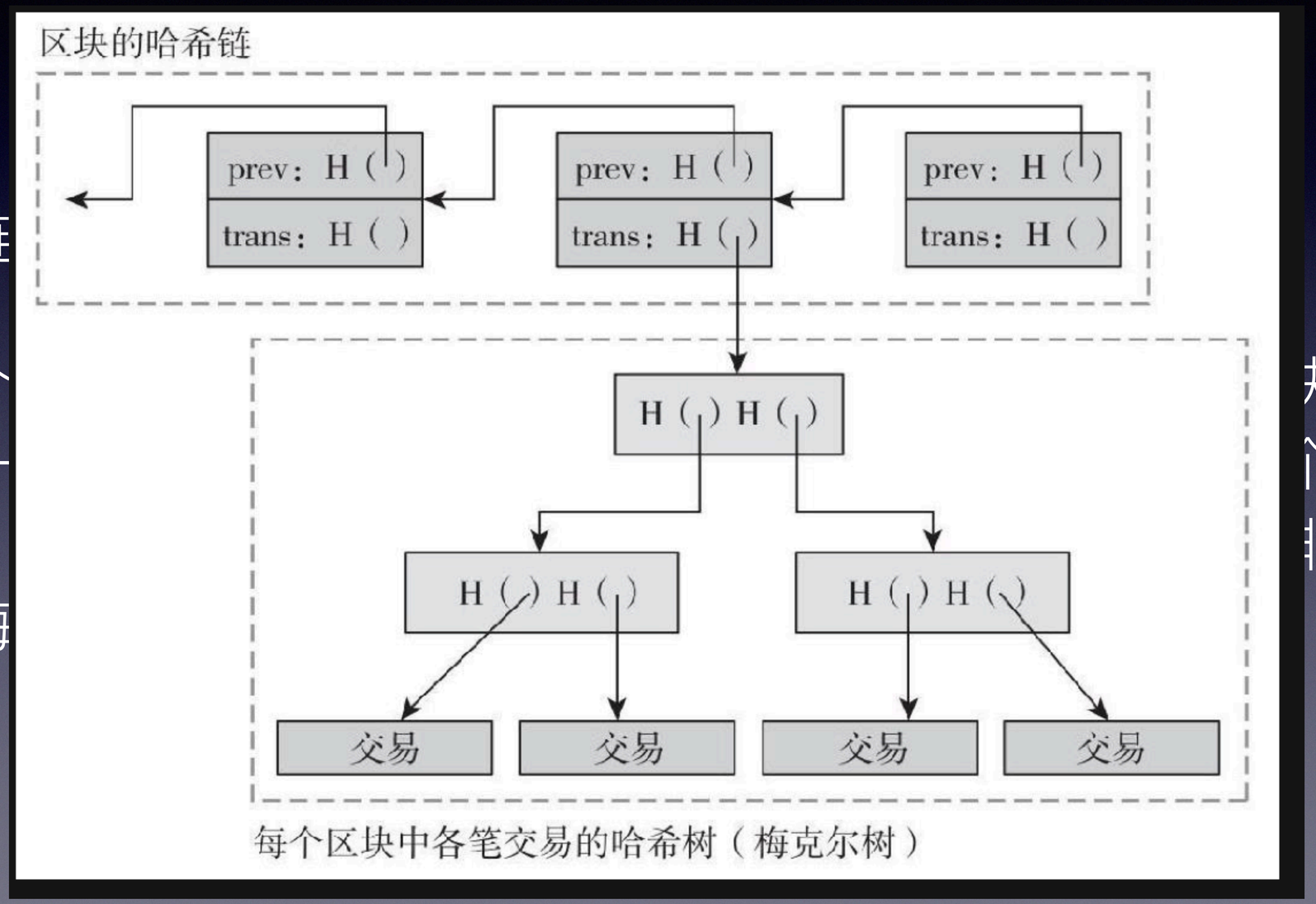
真实区块链交易数据


```
{
    "hash": "8c14f0db3df150123e6f3dbbf30f8b955a8249b62ac1d1ff16284aefa3d06d87",
    "ver": 1,
    "vin_sz": 1,
    "vout_sz": 1,
    "lock_time": 0,
    "size": 135,
    "in": [{
        "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
        },
        "coinbase": "044c86041b020602"
    }],
    "out": [{
        "value": "50.00000000",
        "scriptPubKey": "041b0e8c2567c12536aa13357b79a073dc4444acb83c4ec7a0e2f99dd7457516c5817242da796924ca4e999
        47d087fedf9ce467cb9f7c6287078f801df276fdf84 OP_CHECKSIG",
        "next_in": {
            "hash": "f3e6066078e815bb24db0dfbff814f738943bddaaa76f8beba360cfe2882480a",
            "n": 12
        }
    }],
    "nid": "70ab531a68f973f7d20b8260cb5e7fecba3699c48715b8b44539ff9776d0b88e"
}
```

区块链数据结构

- 区块链

- 第一个 块头部，里面有一 个树状数据结构， 排列存储。也叫梅



什么是区块链

Bitcoin Block 784,059

Mined on April 05, 2023 10:31:10 • All Blocks

F2Pool

Coinbase Message • ,z>mmd) % t&xwJKO:Eu <]2y (; ;oN`; p /F2Pool/g oA

A total of 17,572.68 BTC ($494,971,309) were sent in the block with the average transaction being 5.7976 BTC ($163,301). F2Pool earned a total reward
$176,044. The reward consisted of a base reward of 6.25 BTC $176,044 with an additional 0.3704 BTC ($10,433.09) reward paid as fees of the 3,031 tr
were included in the block.

Blockchain →

#784060 #784060 #784059 #784058 #784057 #784056 #784055 #784054 #784053 #784052 #784051 #784050

Output Value	17,579.30 BTC
Transactions	3,031
Witness Tx's	2,649
Inputs	6,409
Outputs	10,455
Fees	0.37039684 BTC
Fees Kb	0.0002601 BTC
Fees kWU	

Reward	6.62039684 BTC
Mined on	2023年4月05日 22:31:10
Height	784,059
Confirmations	1
Fee Range	0-589 sat/vByte
Average Fee	0.00012220
Median Fee	0.00005595

Pool

Place your

区块链数据结构

比特币

- 2008年，“中本聪发表题为“比特币：一种点对点的电子现金系统”的白皮书”
- 拒绝服务攻击
- 双重支付攻击
- 分布式共性

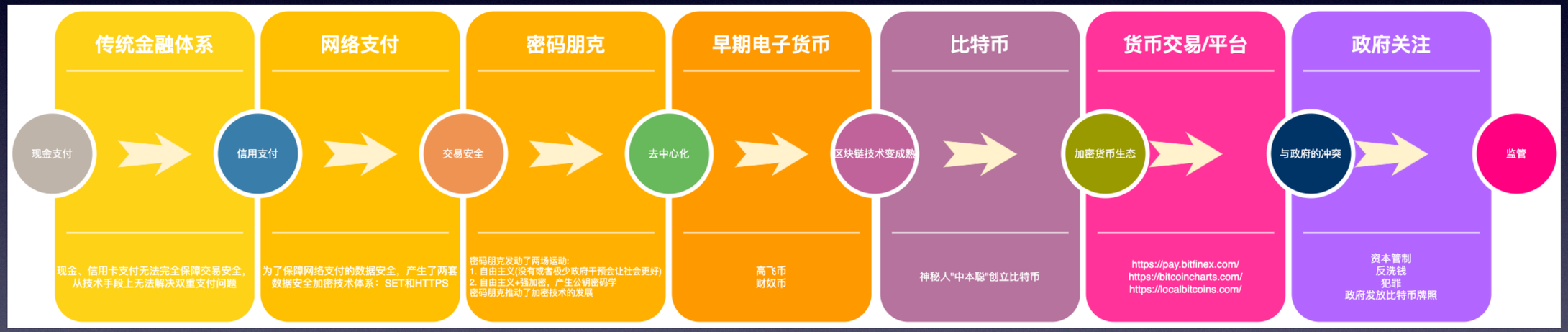
以太坊的智能合约

- 在以太访[illegible]程序。任何人支付后，就可[illegible]个以太坊合约。其它用户可[illegible]

```
contract NameRegistry {
      mapping(bytes32 => address) public registryTable;
      function claimName(bytes32 name) {
            if (msg.value < 10) {
                  throw;
            }
            if (registryTable[name] == 0) {
                  registryTable[name] = msg.sender;
            }
      }
}
```

图10.9 一个用于实现域名注册功能的简单以太坊智能合约

加密货币未来


传统金融体系
现金支付
信用支付
现金、信用卡支付无法完全保障交易安全，从技术手段上无法解决双重支付问题
网络支付
交易安全
为了保障网络支付的数据安全，产生了两套数据安全加密技术体系：SET和HTTPS
密码朋克
去中心化
密码朋克发动了两场运动:
1. 自由主义(没有或者极少政府干预会让社会更好)
2. 自由主义+强加密，产生公钥密码学
密码朋克推动了加密技术的发展
早期电子货币
区块链技术变成熟
高飞币
财奴币
比特币
神秘人"中本聪"创立比特币
货币交易/平台
加密货币生态
https://pay.bitfinex.com/
https://bitcoincharts.com/
https://localbitcoins.com/
政府关注
与政府的冲突
资本管制
反洗钱
犯罪
政府发放比特币牌照
监管

区块链未来应用

- 医疗领域--使用区块链智能合约帮助患者和医生安全地传输敏感的医疗信息
- 金融领域--加密货币
- 农业领域--利用区块链的特性，对食品供应链安全进行溯源管理
- 农业保险--去中心化数据存储方式，解决买卖双方信任不足问题。通过智能合约，让赔付流程自动化，赔付效率变得更高
- 物联网 (IoT)--物联网有数百万个应用程序和许多安全问题，增加了更高的数据安全性

谢谢！！