codingapi

区块链的来龙去脉

lorne

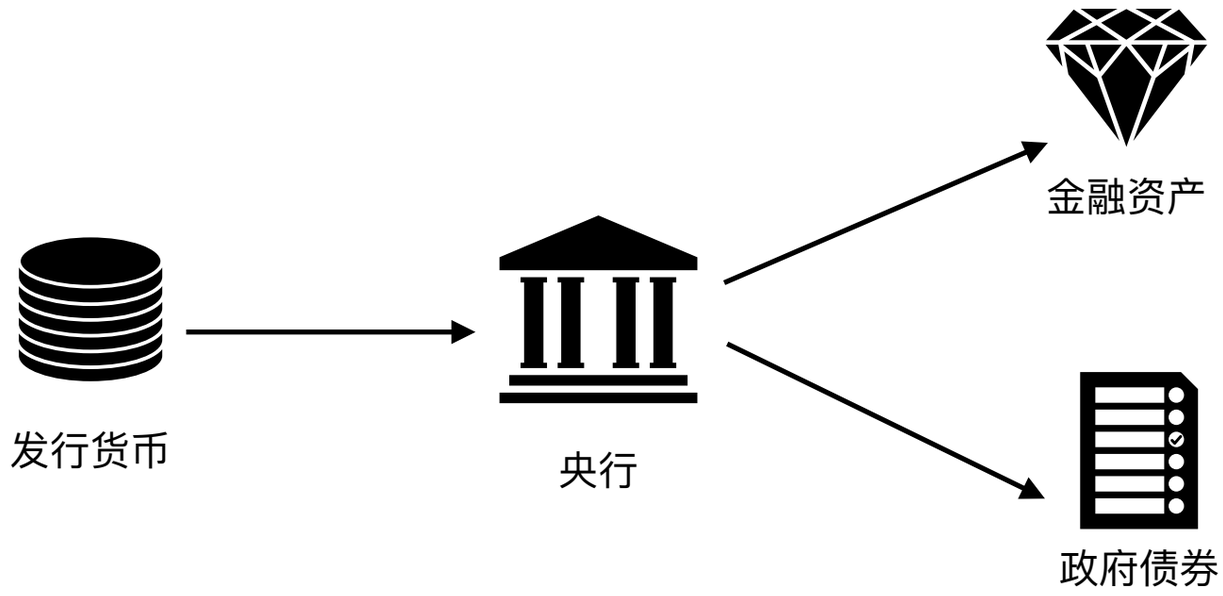
视频讲解地址: https://www.bilibili.com/video/av80262984/

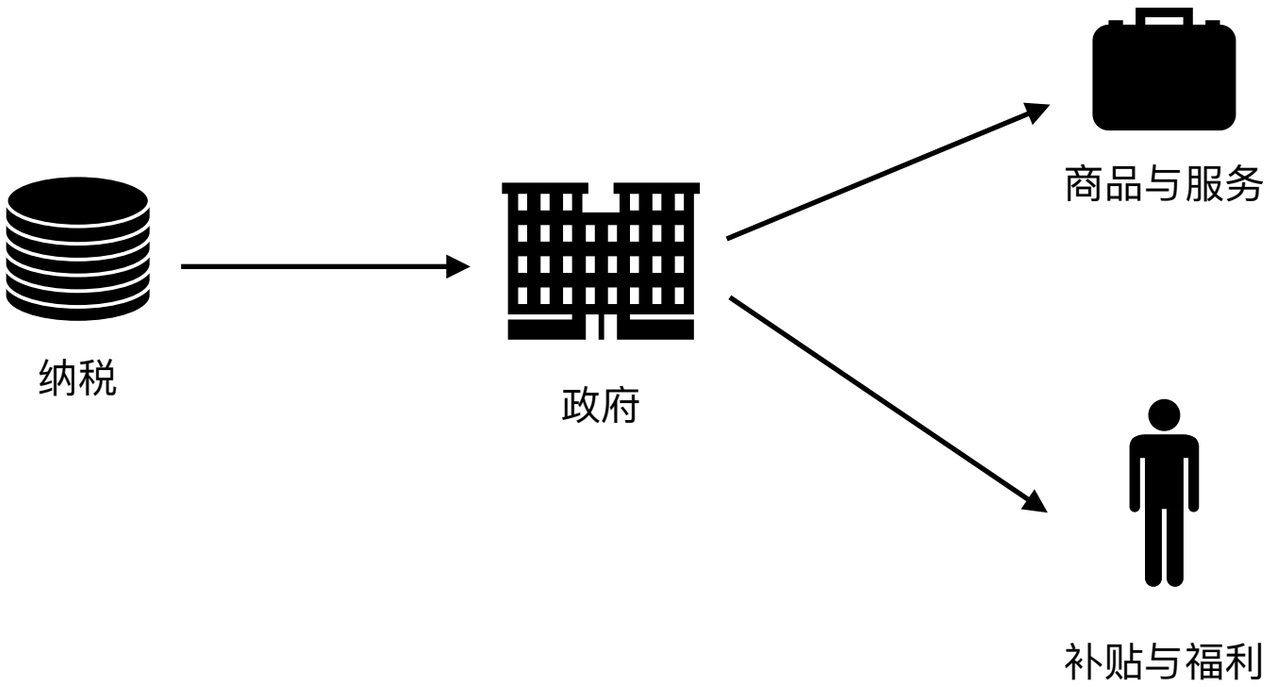
钱是什么

钱其本质是用于物品交易的票据。

一般钱的发行是由国家管理控制的，也是国家为了规范、掌控市场的一种手段。

生活中的钱是怎么来的?





https://www.youtube.com/watch?v=rFV7wdEX-Mo

历史上的通货膨胀事件

codingapi

一战后德国

德国。作为战败国，根据《凡尔赛合约》，德国要支付巨额的战争赔款，约1300亿金马克，面对如此高额的战争赔款，德国十分的不情愿，于是采取相对极端的方式来偿还赔款，那就是发纸币。1919年，德国全年的货币发行量约为500亿，到了1923年，德国货币发行量达到无以复加的天文数字5万亿亿，物价上涨200亿，一美元可以兑换42000亿，货币连纸都不如。

国民党统治时期

国民党统治时期，不顾人民祈求和平的愿望，肆意进行内战，为应对庞大的战争开支，填补政府赤字，国民党只能更多发行法币，使得法币成为一张废纸。后来，国民党开始发行金圆券，要求市民用美元、黄金和法币兑换新币金圆券，在榨干市民最后的血汗钱之后，金圆券最终也和法币一样，成为废纸一张。

苏联解体后的俄罗斯

苏联解体后，俄罗斯为这种不合理的经济结构的苦果背锅。1991年–1992年，短短一年时间，俄罗斯产生严重通货膨胀，物价水平上涨26倍，人民生活苦不堪言。

近年来的委内瑞拉

委内瑞拉和大多数产油国一样，只要开采石油就可以赚取大量外汇，以至于经济结构单一，石油工业占据有据对的支配地位。结果，近年来，随着国际油价的持续下跌，油价高企时的免费医疗、廉价的食品等局面一去不复返，并且委内瑞拉财政也开始紧张，物价开始上涨，2015年，委内瑞拉通货膨胀为120%多，2016年达到惊人的800%，而同期GDP缺萎缩近20%。

https://www.sohu.com/a/204219728_100048764

为什么发行比特币?

1、2009年1月3日，《泰晤士报》头条以“Chancellor onbrink of second bailout for banks”作为标题，说英国财政大臣正处于实施第二轮银行救助的边缘，英国央行将对国内的银行进行财政救助，也就是政府要印钞票来借钱给银行。这句话被写到了比特币的创世块中，作为抗议政府滥发钞票导致通货膨胀的宣誓。

2、也体现了西方世界对自由民主的追求。

比特币是什么

比特币是基于区块链技术发行的虚拟货币。区块链是一个去中心化的分布式账本数据库，每个区块基于密码算法，公开的以时间顺序进行交易。而去中心化分布的区块，即使单独受到攻击也不会使整个链网受到影响。这就是为什么，与互联网相比区块链不仅可以传递信息，还可以传递价值与信任。

https://bitcoin.org/files/bitcoin-paper/bitcoin_zh_cn.pdf

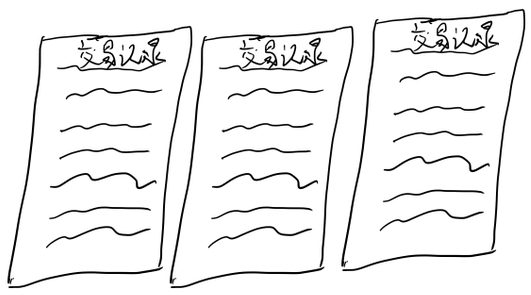
比特币为什么不能作为货币

http://www.bitcoin86.com/price.html

比特币本质是什么

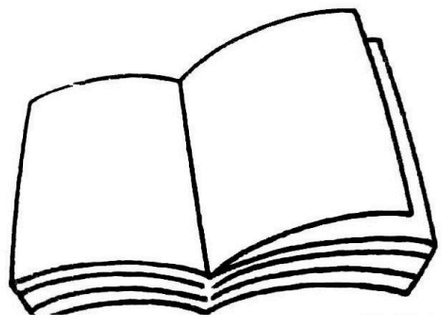
比特币实际上是一个超级账本，账本的数据在区块中，保存在链上。数据由认可比特币的网络节点来维护。

交易记录



一页纸一条记录

区块



一个月的记录合成一个账本

区块链

账本与账本之间存在先后顺序

比特币的演变过程

小明储值100元
小红储值100元
小强储值100元

100 ¥

小红

小红支付小明一月打水费用30元

30 ¥

小明

小明买1本《精通Python》

10¥/本

《精通Python》

小明1本《Python项目实战》

15¥/本

《Python项目实战》

小强

加密的格式

codingapi

姓名	私钥	公钥	公钥Hash	地址
小明	2b6dc1b4bf2668c72b7cfe72b1f258de11b03d35bc4f05e70c411e54794065f5	021acfd2b13884279cb061b5b2cc1e51a93133b1c3c169f8ffe0557f868a5cd054	a122117bd37d8ddcae5fa5fa2b935bf425ffe091	1FgzbzW19QDTXVtkP8RWBjQZ5MwGG8N3YX
小红	20872764638709bb33c6b82caf4783e941346c99dbd878ec58830d51a9699d50	0294a0ea995a5ae3a2044b229940707093bec799610077d9f04f1295844ccdcb56	354c0608be7d05a8e962c52c218b575f7f8a88b8	15rotNtKL56Y3A9tq2RgSfpakkb4wNWxXx
小强	613f49362dd1c92fc6fc84657d8e9eafae4f9c0e532a14024350b7534b78904c	03ece833afdd78b51a1deed6abfdb34dd0bd4f5f51ed2c2be0673a405758de341e	85cbe051a3353c48acd344b40708e8d8af98c1a3	1DCT75qLkToASnc69qZLoNHP2VNZDLtaCH

姓名	私钥	公钥	公钥hash	地址
小明	小明私钥	小明公钥	小明公钥Hash	小明地址
小红	小红私钥	小红公钥	小红公钥Hash	小红地址
小强	小强私钥	小强公钥	小强公钥Hash	小强地址

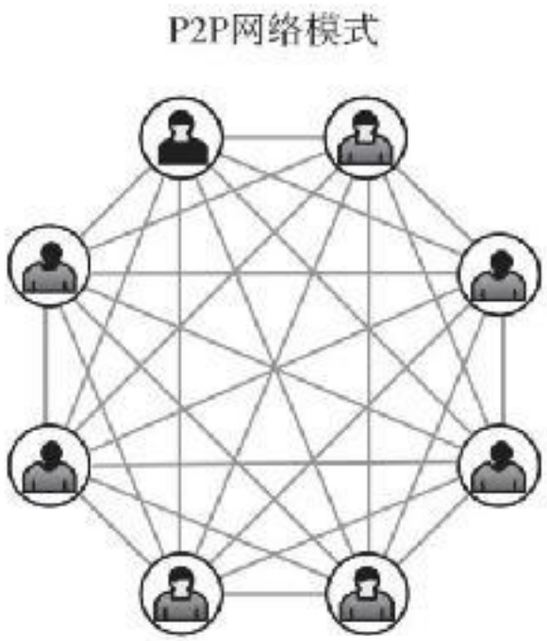
如何记账的

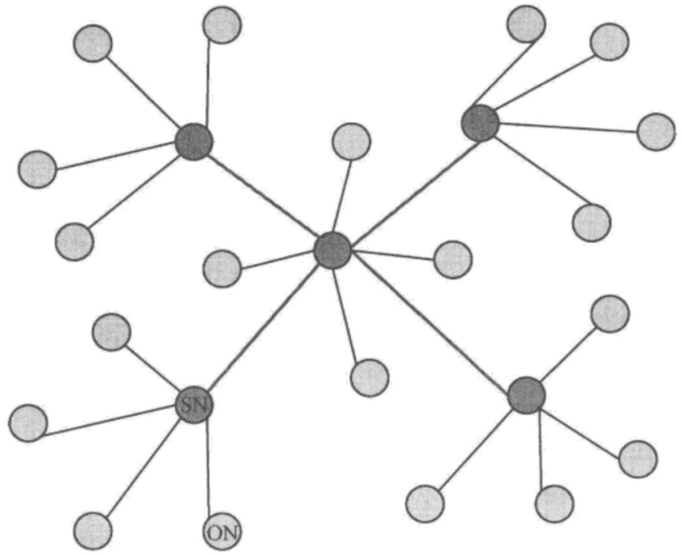
编号	交易记录	发起方签名	发起方公钥	接受方	金额	接受方公钥Hash
1	-	-	-	小明地址	100	小明公钥Hash
2	-	-	-	小强地址	100	小强公钥Hash
3	-	-	-	小红地址	100	小红公钥Hash
4	3	小红对记录3签名	小红公钥	小明地址	30	小明公钥Hash
5	3	小红对记录3签名	小红公钥	小红地址	70	小红公钥Hash
6	4	小明对记录4签名	小明公钥	小强地址	10	小强公钥Hash
7	4	小明对记录4签名	小明公钥	小明地址	20	小明公钥Hash
8	7	小明对记录7签名	小明公钥	小强地址	20	小强公钥Hash
9	1	小明对记录1签名	小明公钥	小强地址	5	小强公钥Hash
10	1	小明对记录1签名	小明公钥	小强地址	95	小明公钥Hash

拜占庭将军问题?

区块链里的大家互相信任的前提是大家一致认可数据相同且校验过的数据。俗话说，不能把鸡蛋放在一个篮子里，为了数据的安全，区块链将数据在各个节点上都保存了一份，那么分开发就存在一个麻烦的问题，就是数据如何同步的问题，共识机制就是解决这个问题的规则。

比特币如何解决的这个问题?





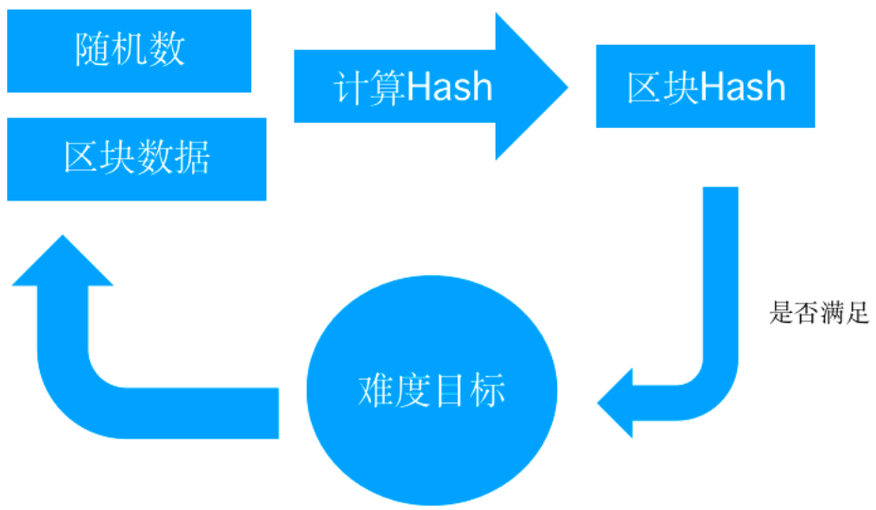
1、时间控制 （难度）
2、排队控制 （区块）

假如同步数据的难度为N，若区块中存在M条记录，那么加入区块以后将难度降低了M倍，即难度为N/M。假如每1秒中同步一次的数据难度为N，若每M秒中同步一次数据，那么区块的难度就降低了M倍，即难度为N/M。

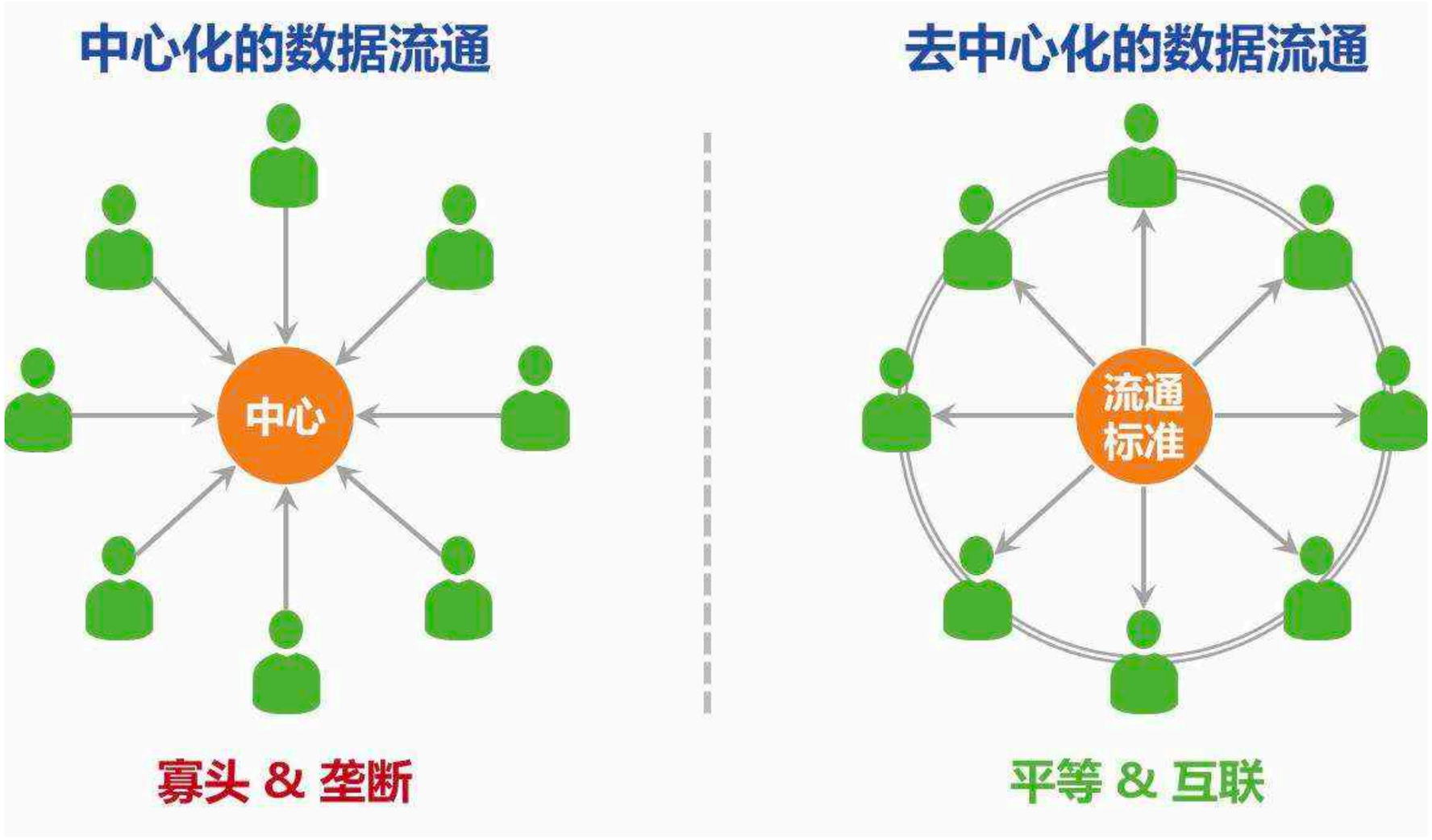
什么是挖矿？

你妈妈喊你回家吃饭哦，回家罗回家罗
你妈妈叫你回家吃饭啦，回家罗回家罗

1000010010101101**1**1111110000010101101000100111110000**0**0101**1**001011
1000010010101101**0**1111110000010101101000100111110000**1**0101**0**001011



什么是去中心化?



1、时间戳服务器
2、SPV简单支付验证

区块链的发展史

区块链的三个阶段：

区块链1.0 比特币

区块链2.0 以太坊(智能合约)

区块链3.0 价值与信任

区块链是一个去中心化的分布式账本数据库，每个区块基于密码算法，公开的以时间顺序进行交易。而去中心化分布的区块，即使单独受到共计也不会使整个链网受到影响。这就是为什么，与互联网相比区块链不仅可以传递信息，还可以传递价值与信任。

中本聪在倡导什么?

比特币的技术出现以后，促使区块链技术的迅猛发展，但是区块链的背后依旧还存在去中心化与中心化的博弈，就如今天的交易所与矿池的存在一样。但是随着以太坊、区块链3.0的全面发展，去中心化的理念会慢慢深入人心的。

今天全世界的人民都认同法律的存在，每个人遵纪守法去旅行自己的责任，这里就如同区块链的网络世界，不同之处是在于目前还是由人来掌控，随着去中心化的深入，或许真有一天，世界的规则不再需要人来监管，而是基于区块链技术来监管。

若你对技术感兴趣，想要了解分布式、物联网、区块链、深度学习，请关注我

CodingAPI lorne
wangliang@codingapi.com

https://www.codingapi.com/