从区块技术的发展历史看区块链是什么？

原创

哲学的终极三问：“我是谁？我从哪里来？我要到哪里去？”耗费古今中外多少人的心血。

作为区块链的从业者，也面临有三个根本性问题：区块链是什么？区块链怎么产生的？区块链有什么用？

追根溯源，本文尝试从区块链技术的产生背景和技术演进过程来回答:

> 区块链是什么呢？

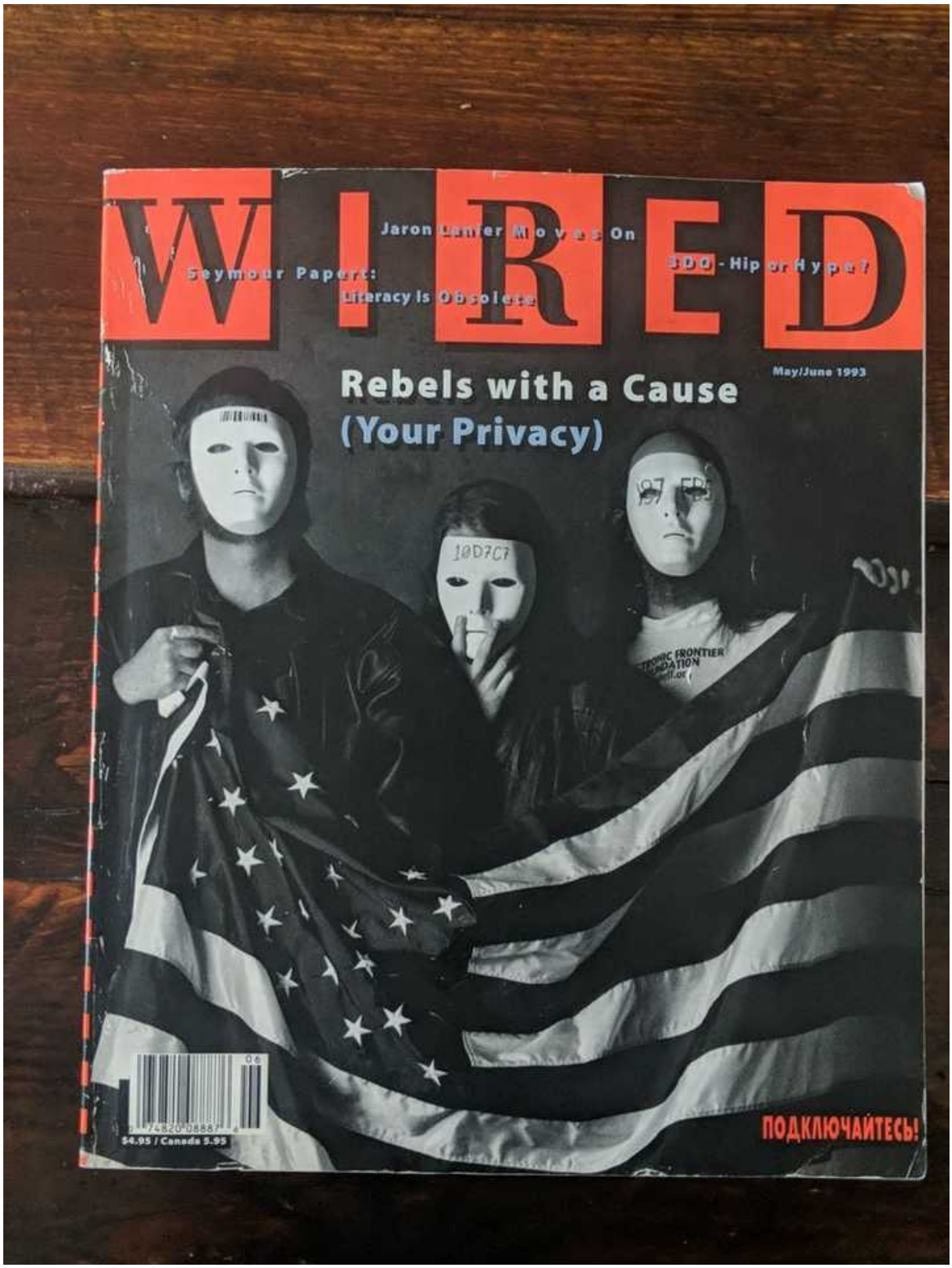
希望对大家理解区块链有所帮助。

区块链前传之密码朋克

任何事情的兴起都有量变到质变的过程，看似横空出世，其实背后都有发展的轨迹和逻辑。区块链的发展也不例外，他的发展源自密码朋克社区。

“密码朋克”一词的首次出现，是在1993年埃里克·休斯出版发《密码朋克宣言》上。具体的英文版本可以见：《A Cyberpunk Manifesto》。

在20世纪80年代以来，人们在处理和保存信息，相互之间通信上越来越以来网络和计算机。加密技术迅猛发展，以保护信息的隐私和通信的安全。但当时这些算法都属于高度机密，完全掌控在国家和大型机构手中。



密码朋克

一些奉行自由主义和无政府主义的技术极客们敏锐的意识到，在信息时代隐私的重要。他们要用开源的加密算法和工具，来保护个人信息和隐私免受攻击。这些人聚集在一起形成密码朋克社区。社区中的很多人都在后来互联网的发展中，有着举足轻重的影响力：

> Tim May（英特尔公司前首席科学家） John Gilmore（太阳微系统公司的明星员工） David Chaum （大卫乔姆） Phil Zimmerman （PGP技术的开发者） Julian Assange（维基解密创始人） Adam Back （亚当·拜克） Wei-Dai （可能是华裔，地位尊崇） Hal Finney （PGP加密的发明人之一） Tim-Berners Lee 爵士 (万维网发明者) John Perry Barlow (赛博自由主义政治活动家) Nick Szabo（BitGold 发明人，智能合约的发明人）

经过多年努力，密码朋克及其追随者开发出了多种数据和通信加密工具，为捍卫个人隐私做出了巨大的贡献。但是最为密码朋克孜孜以求的，是匿名电子货币系统。

在中本聪和他的比特币出现之前，有三个项目对比特币产生起到关键性影响力。

E-cash项目

由David Chaum提出。就是这个大胡子老头，知名老码农不知道为啥都喜欢留大胡子。

E-cash的目标是建立起一套匿名的互联网支付系统，付款人可以证明交易存在，但任何第三方都无法获取支付的信息。E-cash试图在现存金融体系内，制造出一个黑洞，在黑洞内流转的资金无法追踪。David Chaum在荷兰注册公司运营E-cash，并且为其技术注册了专利。这使得他遭遇了来自左右两侧的攻击，密码朋克认为他的商业运作和专利申请违背了密码朋克运动的宗旨，而现存的金融系统则不能容忍资金无法追踪。

B-money

由Wei Dai提出, 下面这位，你没猜错，是华人GG。

跟后来的比特币非常相似，它们都基于P2P网络、无中心的运行，通过不可伪造的计算铸造货币等等，但只提出概念并无真正实现。Wei Dai是著名的密码朋克，是著名的Crypto C++ library的作者和维护者。为了向他致敬，以太坊最小货币单位Wei，以他的名字命名。

Hashcash

由Adam Back设计。Adam Back在今天的区块链行业仍然具有巨大的影响力。他是Blockstream公司的创始人和CEO，比特币核心开发者大部分都是Blockstream公司的雇员。

Hashcash其实并不是要解决通用的支付问题，它的出发点是如何防止对互联网资源的滥用，例如如何对抗垃圾邮件。Hashcash提出通过不可伪造的hash运算生成某种证明，类似于邮票，发送电子邮件必须贴邮票，从而大幅提高垃圾邮件的发送成本。Hashcash首创了通过Hash运算提供工作量证明的机制。后来被用在比特币的POW算法当中

除了以上提及的三个项目，对区块链做出贡献的项目还有很多。其中包括以“智能合约”概念提出者而著称的Nic Szabo。后面再以太坊项目中会提到智能合约。

区块链1.0之比特币

先有比特币，才有区块链。所以，比特币的重要性不言而喻。至今仍然是区块链领域最重要的项目，目前占据整个数字货币市场的66%。（数据见： CoinMarketCap）

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ Exchanges ▾ Watchlist USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$178,077,121,534	$9,782.73	$40,097,993,990	18,203,212 BTC	3.25%	
2	Ethereum	$23,270,541,760	$212.34	$17,031,381,832	109,588,744 ETH	7.19%	
3	XRP	$12,210,005,220	$0.279417	$2,989,829,894	43,698,224,662 XRP *	1.38%	
4	Bitcoin Cash	$8,112,702,261	$444.19	$5,235,782,001	18,263,975 BCH	3.21%	
5	Bitcoin SV	$5,455,061,934	$298.72	$2,814,871,084	18,261,190 BSV	1.46%	
6	Litecoin	$4,732,038,194	$73.91	$5,818,749,920	64,023,535 LTC	2.78%	
7	Tether	$4,648,554,582	$1.00	$50,399,592,804	4,642,367,414 USDT *	0.08%	
8	EOS	$4,350,995,172	$4.57	$4,098,867,332	951,883,324 EOS *	2.29%	
9	Binance Coin	$3,188,303,574	$20.50	$376,584,529	155,536,713 BNB *	7.06%	
10	Cardano	$1,548,545,342	$0.059727	$145,612,751	25,927,070,538 ADA	0.61%	

比特币产生的历史背景，可以见之于中本聪在比特币创世区块，也是第一个区块链中的写入的内容：

> The Times 03/Jan/2009 Chancellor on brink of second bailout for banks(2019年1月3日，财政大臣正在实施第二轮银行紧急援助的边缘)

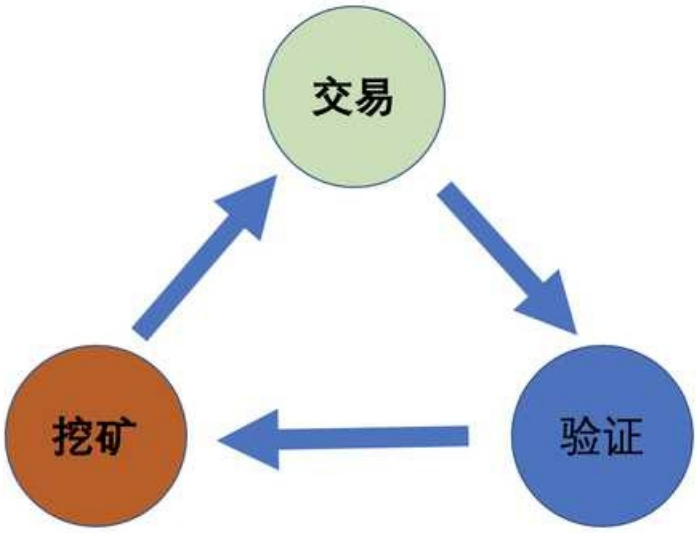
这句话可以在比特币区块链浏览器中看到：

https://btc.com/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

所以，比特币是在2008年金融危机这样一个特定历史环境下的产物，嘲讽政府无节制地发行货币，金融系统的崩溃。它核心要解决：货币发行的去中心化和透明性，建立一套由算法规则来掌控的货币体系。

比特币的设计机制可以仔细阅读他的白皮书：https://github.com/xiaolai/bitcoin-whitepaper-chinese-translation

比特币的基本运行过程见下图：



比特币的基本运行过程

核心分三个阶段：

交易：交易这使用钱包工具，点对点地进行交易，并广播交易信息到比特币的网络当中

验证：矿工接受并加哈交易的合法性，将其打包并进行“挖矿”

铸币：系统奖励成功“挖矿”的矿工一定数额的比特币

比特币网络已稳定运行十年，它实现了：

货币的去中心化。

货币发行的透明化

货币流通全球化

货币交易的匿名化

个人掌控货币的所有权

这个时期的比特币，在技术是称之为分布式不可篡改的电子账本系统。提供了一个可信数据库的环境，属于区块链1.0特有的技术。围绕比特币，后续诸多项目作出不同的改进，但本质上都是属于一种特殊的数据库系统。

区块链2.0之以太坊

比特币的独特魅力吸引全球很多人的参与，随着越来越多人的加入，技术在不断的迭代和升级。

2014年，年仅19岁的Vitalik, 发布了以太坊白皮书，并与合作者一起，在一年之后实现了以太坊上线。以太坊把图灵完备的虚拟机引入区块链，把整个网络变成一台全世界共用的通用虚拟计算机。

Vitalik

2017年，基于以太坊的各种1co,带动整个行业的发展，随之而来的各种DApp应用的兴起又大大拓展区块链的应用广度和深度。以太坊也因其特殊的贡献和社区认可度，牢牢占据数字货币市场的第二名（数据见：CoinMarketCap）。

Vitalik也因此一战封神，江湖人称V神，这是属于他的高光时刻，不仅拥有巨大的影响力，还拥有巨额的财富，巅峰时期，他拥有的以太坊价值高达近十亿美金。区块链行业以其高度的自由和财富光环，吸引各种人蜂拥而至。

至此区块链进化到2.0时代，从可信账本，到可信计算机。从以太坊开始，区块链不再只是一个数据库，它已经变成一个计算的平台。依托于平台，可以开发出各种DApp(Decentralized App)，关于DApp是什么，后面可以见我曾经写过的一篇万次长文：《万字长文讲述DApp发展：迎接DApp大时代的到来》。

区块链3.0?

以太坊之后，区块链技术又有什么样的发展趋势呢？抛开那些瞎喊区块链3.0甚至4.0之外的项目，真正的区块链3.0技术在哪里呢？

从真正技术发展的跨度来看，并没有太脱离可信计算的范畴，从这点意义上看不能算作真正意义上的3.0。 但随着应用的不断深入，在一些关键技术和应用广度上取得新的突破

性能

区块链的“不可能三角”，也称为“三元悖论”，就是指区块链网络无论采用哪种共识机制来决定新区块的生成方式，皆无法同时兼顾扩展性（Scability）、安全性（Security）、去中心（Decentralization）这三项要求，至多只能三者取其二。

比特币和以太坊(1.0)，采取POW算法， 全网节点参与共识，兼顾安全和去中心，导致扩展性差，TPS低。比特币10分钟一个区块，在受限于区块大小，最终每秒7币交易。以太坊的tps是10-20之间。为此，很多其他项目采取一些新的共识算法来解决这个问题。

性能问题，业内核心有两类解决方案：

一类是采取新的共识算法，在不可能三角中牺牲其中一部分。

EOS采取DPOS共识，27个节点在亚秒(0.5s)间隔出块，而且对节点的性能和网络提交要求极高。实际跑出的TPS高达5000+，满足绝大部分应用要求。但有限节点数，就导致去中心化的成都降低，受到很多人的诟病。

EOS

iota采取DAG做共识，底层区块不在一个个一次排列好的一个线性结构，变成一张有向无环图。这种结构的扩展能力很强，能够多个节点同时参与共识，理论上性能可以无限大。

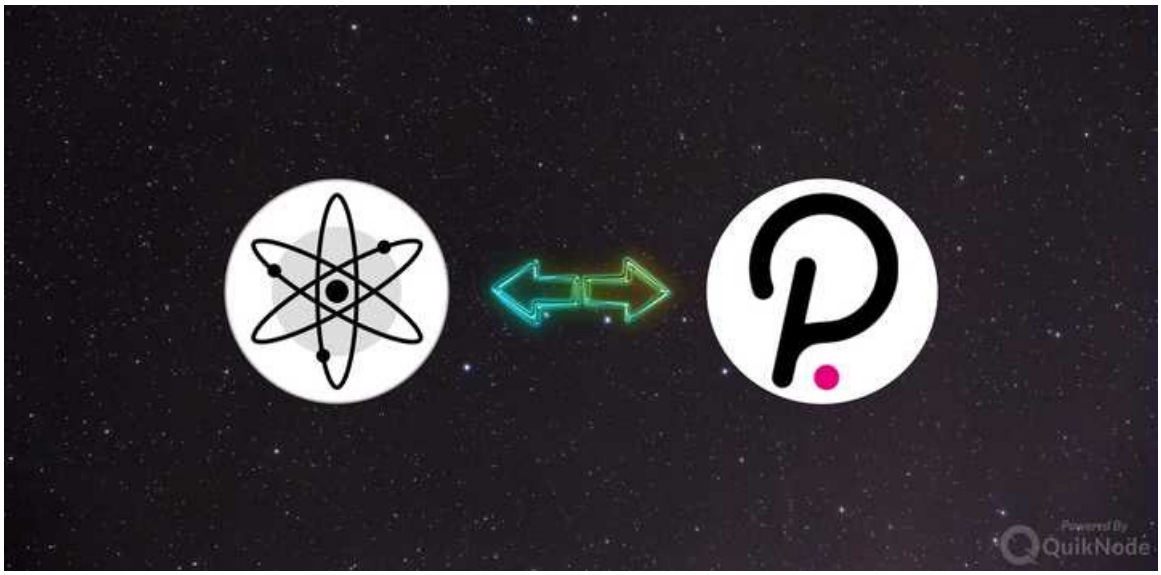
另外还有像Algorand项目，号称已经解决不可能三角问题，都很值得关注。

还有一类是称之为Layer2 的扩展方案，主要是围绕以太坊展开。一种是分片方案，另外一种是链下方案，在此就不做详细探讨。

跨链

区块链行业繁荣的背后，伴随着一个个项目的发展和崛起，这样就出现一条条独立的链，彼此隔离，形成一个个独立的信息孤岛，不形成网络效应，是无法发展壮大和涌现出新的事物。如何突破信息孤岛的问题，让不同的链之间能够相互通信就是跨链需要解决的问题。

围绕跨绕问题，在2019年，Cosmos和Polkadot，备受关注。二者都形成独立的解决方案，先解决本身同质链的通信问题，在通过适配的方式解决跟其他链的跨链问题。都有一个基本的核心组件，Cosmos的Tendermint，Polkadot的Substrate，能够做到一键发链。也就是开发者不需要独立开发区块链系统，简单的一些命令就能创建一条链，非常便捷。



当然，还有一些其他技术要点比如：Oracle, 隐私保护，去中心存储这些也在不断发展。

总结

> 罗马不是一天建成的。

区块链经过10+年的发展，从技术的角度看：区块链从一个可信的账本，变成一个可信的计算机平台。核心都是可信，也就是区块链一直在通过算法来解决价值问题。所以，我们也经常说，区块链是信任的机器。

解决信任问题，是区块链提供的最核心价值。后面有机会再讲。