1.2 区块链的起源和现状

01 区块链的起源

1. 密码朋克的成立

1992年，英特尔高级科学家蒂姆·梅在自己的家中和朋友聚会。聚会上他和朋友讨论着互联网应该如何更好的保护人们的隐私。 “**怎样保护全世界民众的隐私在互联网上不被别有用心的人利用呢?**”这个问题困扰着蒂姆·梅，和朋友们的讨论一直进行到深夜。但他还是应该高兴，以前一个人的困扰至少变成了大家的困扰。他们还成立了一个小组：**密码朋克**。

在聚会结束一周后，小组中的埃里克·休斯就写了个程序，可以接收加密邮件，擦除所有身份标记，并将它们发送回用户列表，当你签名后，你会得到休斯的回信。

02 区块链的起源

1. 密码朋克的成立

1993年，埃里克·休斯和其他几个人，升级迭代了加密电子邮件系统，直接把系统改名叫“密码朋克”。密码朋克也不再是一个小组，使用密码朋克邮件系统的用户约1400人。这些人逐渐形成一个非常私密的圈子。

同时，埃里克·休斯发布了《密码朋克宣言》向权力机构发起了挑战：“在电子信息时代，个人隐私在一个开放的社会中是必需品。我们不指望政府、公司或者其他什么不要脸的组织来承诺我们的隐私权。我们必需保护我们的隐私。**必需有人站出来做一个软件，用来保护个人隐私**……我们计划做这样一个软件。”

03 区块链的起源

1. 密码朋克的成立

Tim May

最先提出密码朋克概念的英特尔高级科学家

04 区块链的起源

2. Ecash

大卫·乔姆是密码朋克的领袖级人物，他在1990年发明了**密码学匿名现金支付系统**，即Ecash。乔姆认为分布式的、真正的数字现金系统应该为人们的隐私加密。因此他的电子支付系统里的加密使用了数学编码。还有一个小特点就是支付时**付款方匿名的，收款方非匿名的。**

1990年的Ecash当时风头正劲，微软和visa等巨头纷纷宣布支持，有趣的是大卫乔姆和中国的河南政府也签订了合同，从德意志银行、澳大利亚高级银行、瑞士信贷和日本三井住友银行获得了牌照，只可惜理念太超前了，而当时的人类社会并没有大范围实施的基础，于1998年Ecash宣布倒闭。

05 区块链的起源

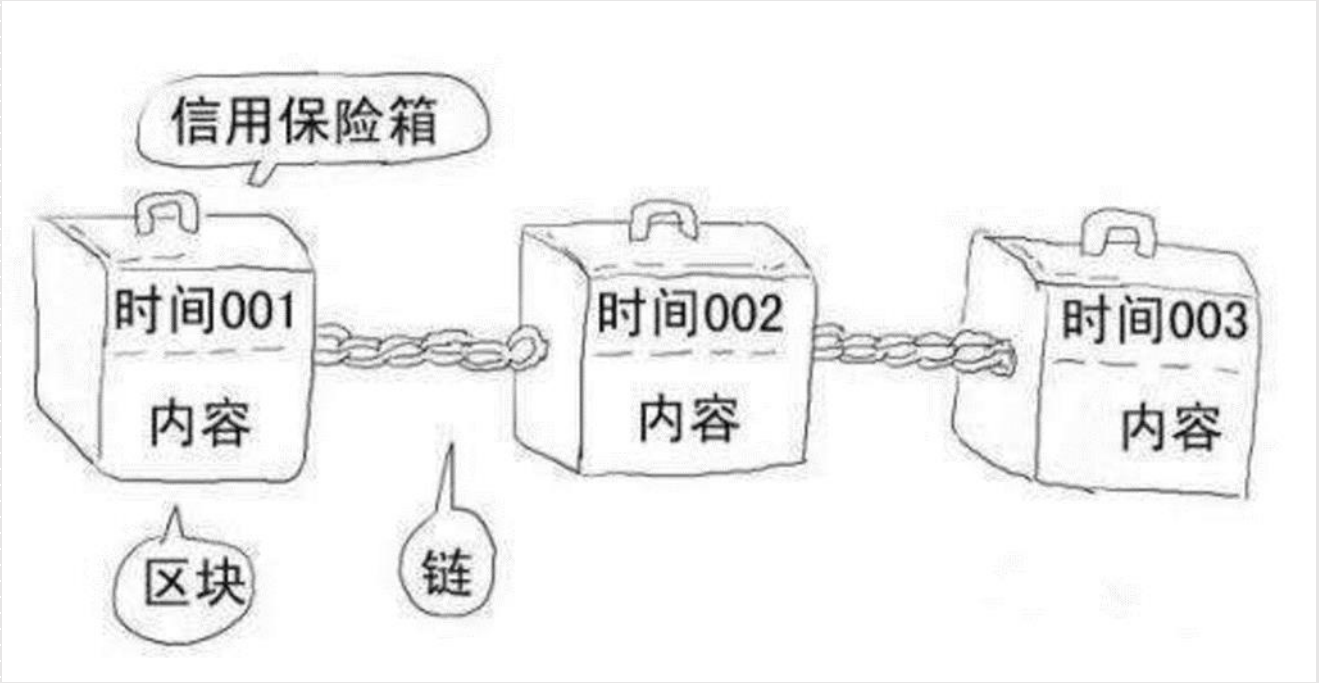
3. 哈希现金

英国密码学家亚当·贝克也是密码朋克的成员。1997年，他发明了哈希现金，用到了**工作量证明系统(proof of work)**。其实亚当贝克最初发明这个系统是想**解决垃圾邮件的问题**，也就是为了避免其他人发送包含有相同信息的邮件。它的工作量证明系统，解决了数字货币的一大难题：如何保证数字货币不被交易过很多次?这就要求计算机在获得信息之前，做一定的工作量计算来避免重复交易。

06 区块链的起源

4.时间戳概念

1997年，密码朋克成员哈伯和斯托尼塔提出了时间戳概念(一种签名协议)。后来这个保证了数字货币安全问题，即用时间戳的方式来保证文件的先后顺序。时间戳协议要求在文件创建后，不能改动。当一个虚拟货币被交易时，被盖上时间戳，它就不能被改动，这个技术协议只被政府小范围应用。



07 区块链的起源

5.比特币诞生

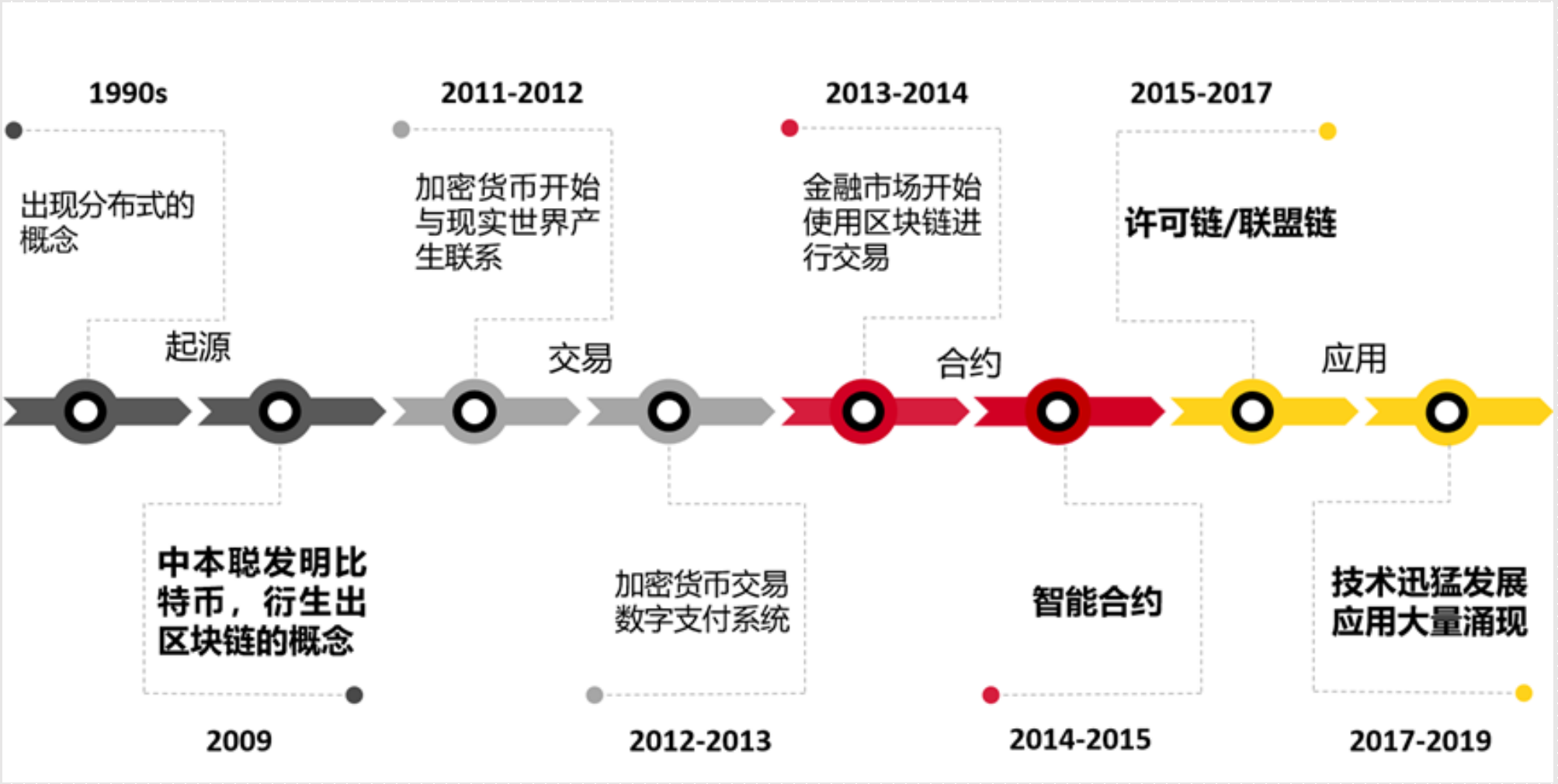
2004年，一位密码朋克成员哈尔芬妮提出了电子货币和加密现金的概念。他理想中的这种货币是可重复使用的，并参照了失败项目的优点。但是他的设想还是不够成为一种世界型的虚拟货币。终于在2008年，**中本聪**对大卫乔姆的Ecash进行了优化，综合了时间戳、工作量证明机制、非对称加密技术、UTSO的结构，最终他发明了比特币。人们就把**比特币的底层技术称为区块链。**

08 区块链现状

区块链技术从诞生到现在经历了三个阶段。

- 区块链1.0-----**数字货币**，以比特币为代表的去中心化的数字支付。
- 区块链2.0-----**智能合约**，以以太坊为代表的支持用户自己编写智能合约，构建去中心化的应用DAPP。
- 区块链3.0-----**延伸到各个领域**，也就是将区块链运用到各行业具体的场景中去。

09 区块链现状


1990s
出现分布式的概念
起源
中本聪发明比特币，衍生出区块链的概念
2009
2011-2012
加密货币开始与现实世界产生联系
交易
加密货币交易数字支付系统
2012-2013
2013-2014
金融市场开始使用区块链进行交易
合约
智能合约
2014-2015
2015-2017
许可链/联盟链
应用
技术迅猛发展应用大量涌现
2017-2019

10 区块链的未来发展

- **广泛被应用：**未来区块链将渗透到各行各业，企业政府等部门，比如：银行业、支付和现金交易、股票交易、供应链金融、可编程金融、跨境银行间清算、学术研究、选举、汽车业、物联网、研究预测行业、在线音乐、共享乘车、房地产、保险、医疗、政务信息等都有很大的应用。

- **加强治理：**现如今区块链正处在发展的关键节点，区块链行业处于由乱到治的关键阶段。2017年9月，中央七部委联合发布《关于防范代币发行融资风险的公告》，明确指出首次代币发行（ICO）进行融资的活动涉嫌从事非法金融活动。此后，区块链行业的负面效应逐步得到遏制，出现了一些积极变化。“专注技术落地，服务实体经济”正越来越成为业内人士的共识。

11 国家和地方政府的相关政策

国家知识产权局

《知识产权重点支持产业目录(2018年本)》	2018.01

工信部

《2018年信息化和软件服务业标准化工作要点》	2018.03
《2018年中国区块链产业发展白皮书》	2018.05
《工业互联网发展行动计划（2018-2020年）》	2018.06

卫生健康委员会

《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》

财政部

《财政部前三批PPP示范项目整改情况通报》	2018.09

商务部等12部委

《关于推进商品交易市场发展平台经济的指导意见》	2019.02

最高人民法院

《人民法院第五个五年改革纲要（2019—2023）》	2019.02

北京市

《北京市推进政府服务“一网通办”工作实施方案》	2018.07
《北京市促进金融科技发展规划（2018年-2022年）》	2018.11

上海市

《促进区块链发展的若干政策规定（试行）》	2018.09

天津市

《关于深化“互联网+先进制造业”发展工业互联网的实施意见》	
《天津市促进大数据发展应用及条例》	2018.12

重庆市

《关于贯彻落实推进供应链创新与应用指导意见任务分工的通知》	
《我市五大举措积极推动区块链产业发展》	2018.06

河北省

《关于加快推进工业转型升级建设现代化工业体系的指导意见》	
《河北雄安新区规划纲要》	2018.04

辽宁省

《关于积极推进供应链创新与应用的实施意见》	2018.02

广东省

《深圳市工业互联网发展行动计划（2018-2020年）》	2018.06
《广州市黄埔区广州开发区促进区块链产业发展办法实施细则》	

吉林省

《关于加快引进和培育我省区块链产业的建议》	2018.05

四川省

《关于积极探索区块链技术发展应用的决定》	2018.07
《成都市网络信息安全产业发展规划（2018-2022年）》	

福建省

《关于加快全省工业数字经济创新发展的意见》	2018.01
《关于深化“互联网+先进制造业”发展工业互联网实施意见》	

云南省

《关于积极推进供应链创新与应用的实施意见》	2018.08
《云南省科学数据管理实施细则》	2018.09