<?xml version="1.0" encoding="utf-8" standalone="no"?>

01 区块链数字货币基础

笔者第一次听到“比特币”这个词的时候，想当然地把它当作“数字货币”的通称，以为就是泛指Q币、游戏金币之类的虚拟代币。后来听到这个词多了，认真了解后才知道原来这项发明把“数字货币”带入了一个新的时代。那么，比特币之前的数字货币时代是怎样的呢？

数字货币的早期雏形

通常我们说的“数字货币”是指非政府发行的、有一定市场的通货，并且没有物理实体，依赖于计算机和互联网，一般会用“电子货币”或“数字货币”来称呼。国人最熟悉的“数字货币”应该是Q币了，“80后”有不少人都拥有过它。2002年前后，腾讯公司为了摆脱传统支付系统的羁绊，决定开辟自己的支付渠道，最终将这一产品命名为“Q币”，Q币需用人民币1:1换购，可用于购买腾讯公司销售的虚拟产品，如QQ秀等会员服务。不过，Q币只能由人民币到Q币单向兑换。因此，严格地说，Q币并非我们要说的“币”。

下面介绍的这些数字货币，大多引起了各国政府的关注。

EG币

现在知道EG币（E-Gold）的人不多，因为它已经被多国政府联合取缔了，但EG币曾经风光无限。

1996年，圣·科特斯（St.Kitts）和纳维斯（Nevis）创建了网络机构E-Gold，截至2003年，在E-Gold上使用EG币的客户就已达到100万。EG币不锚定任何一种法币，正如开发该币的机构的英文名字E-Gold所显示的，EG币锚定的是黄金。但由于注册和使用者无需提供真实身份，EG币马上就被网络犯罪群体盯上。2005年，美国特勤局和联邦调查局开始调查E-Gold，但使用EG币的人数仍在增长。2006年，E-Gold用户达到了300万。2007年，E-Gold因涉嫌欺诈、帮助罪犯转移资产和传销被起诉，最终淡出主流。但是，受E-Gold启发的产品仍在不断诞生，其中包括后来知名的LR币。

LR币

2006年，Liberty Reserve公司在哥斯达黎加注册成立。也如它的前辈一样，Liberty Reserve公司同样经历了注册用户的快速增长，迅速突破了100万，但最终也因涉及多项罪名而被取缔。当Liberty Reserve公司在2013年5月被美国联邦检察官根据《爱国者法案》关闭的时候，其在美国地区的用户已达到了20万。美国当局以洗钱、协助罪犯转移资金和无金融交易相关执照经营等罪名指控Liberty Reserve公司创始人亚瑟·布多威斯基（Arthur Budovsky）和联合创始人威拉弟米尔·卡斯（Vladimir Kats）等。LR币之前也是众多外汇交易平台所支持的出入金方式。

WM币

WM币由成立于1998年的WebMoney Transfer Techology公司开发，和EG币一样，WM币也经历了用户快速增长和被犯罪分子利用的阶段。但和E-Gold机构所不同的是，WebMoney Transfer Techology公司主动且有效地遏制了WM币沦为犯罪分子从事非法活动的工具，并成功转型向在线电子商务支付系统发展，至今依然正常运营。它支持俄罗斯卢布、美元、欧元、乌克兰格里夫纳、白俄罗斯卢布、越南盾和黄金，可以通过PC端软件、浏览器插件和手机端App使用。目前很多外汇交易网站和投资类站点都接受WM币的存取业务。

PM币

PM币是由Perfect Money公司开发的。Perfect Money公司创建于2007年，持有巴拿马经营许可执照，具有网络银行的性质。在Perfect Money平台，客户可以用PM币进行美元、欧元等国际货币的交易。和WebMoney Transfer Techology公司一样，Perfect Money公司今天仍在经营，并且还在继续增添支持的币种，其中包括黄金、越南盾和本书后面要提到的比特币。虽然这家公司是合法的，但是其创始人的身份依然是一个谜，并且不支持美国地区，这些措施有可能是Perfect Money公司看到了美国政府对E-gold机构的取缔行为而做的预防。

那些著名的支付组织

下面要探讨的支付公司或组织在法律上并不像前面列举的数字货币那么敏感，它们本身就是由银行或者电商衍生发展而来的。而且，它们并没有发行自己的代币，而是作为支付网络存在。

Visa卡

20世纪40年代末期，一些美国银行开始发行购物券，这种购物券可以在当地商店里

被当作货币一样使用。1951年，纽约的富兰克林国家银行将这种应用规范化，推出了第一种现代信用卡。以加利福尼亚州为营业基础的美洲银行将这一做法在全美范围内予以推广，并在1960年推出了美洲银行卡（Bank Americard），这就是今天Visa卡的前身。同时，美洲银行在每一个主要城市建立一家分支机构。这些分支机构与商户签订合同，让商户接受以卡支付的方式，并且在业务覆盖范围内发展持卡人。

万事达卡

美洲银行卡推广几年后，一批没有被委托经营卡的美国银行家开创了他们自己的网络，接受另一种本地信用卡。1966年8月16日，这一批银行组成了“跨行卡协会（ICA）”，以实现跨行授权、清算和结算的交换功能。ICA后来成为万事达卡（MasterCard）国际组织。与美洲银行卡不同的是，ICA并不是由单一的银行所统辖，而是由ICA成员组成了会员委员会，去管理和运营ICA协会，除了建立授权、清算和结算规则外，ICA还负责市场推广、安全和保护品牌的法律事务。

万事达卡全球总部设在美国纽约。2014年4月4日，世界最大零售商沃尔玛选中万事达卡集团为其处理店面品牌信用卡交易。

贝宝

贝宝（Paypal）是美国易趣（eBay）公司的支付工具，1998年12月由彼得·泰尔（Peter Thiel）及麦克斯·拉夫琴（Max Levchin）创建，其公司总部设在美国加利福尼亚州圣荷西市，允许在使用电子邮件来标识身份的用户之间转移资金，避免了传统的邮寄支票或者汇款的麻烦。贝宝也和一些电子商务网站合作，成为它们的货款支付方式之一，在用户使用这种支付方式转账时，贝宝会收取一定数额的手续费。

贝宝账户分为个人账户、高级账户和企业账户三种类型，分别适用于在线购物的买家用户、在线购物或在线销售的个人商户，以及以企业或团体名义经营的商家，特别是使用公司银行账户提现的商家用户。

支付宝钱包

支付宝钱包运行于用户的智能手机上，也可以通过网页登录，是从阿里巴巴的淘宝网衍生出来的支付平台。它内置活期理财产品余额宝，同时具有信用卡还款、转账、充话费、缴费等功能，在很多地方它还能够打车、去便利店购物和通过售货机买饮料等。

微信支付

微信支付是集成在微信客户端的支付功能，用户可以通过手机快速完成支付流程。微信支付以绑定银行卡的快捷支付为基础，向用户提供支付服务。

用户只需在微信中关联一张银行卡，并完成身份认证，就可将装有微信App的智能手机当成电子钱包使用，之后可购买合作商户的商品及服务，用户在支付时只需在自己的智能手机上输入密码，无需任何刷卡步骤即可完成支付。目前微信支付已实现刷卡支付、扫码支付、公众号支付、App支付，并提供企业红包、代金券、立减优惠等营销新工具。

虚拟货币

除了非政府货币、支付网络，还有一种电子货币，一般被称为广义的电子货币——“虚拟货币”。

随着互联网浪潮的到来，越来越多的网站、平台都有了自己的“货币”，这些货币有别于传统意义上的法定货币，但确实属于资产，它们多数被称作“虚拟货币”。虚拟货币在一定条件下具有一定的价值和使用价值，并且具备交易功能，可以转化为现实财物。在司法实务中，就有因盗窃虚拟货币而入刑的案例。

笔者认为，虚拟货币还可再分为以下两大类。

第一类是通过充值而获得的虚拟货币，比如腾讯公司的Q币、Q点、CF点，或者盛大公司的点券及欢聚时代公司的Y币、红钻等。该类货币只能用于消费，无法直接提现为传统货币（我国的法律明文禁止这么做）。

从性质上来讲，该类虚拟货币有债权的成分，但只能兑付成发行方提供的服务业务，比如说购买虚拟游戏道具，购买腾讯公司的增值服务，购买赠与主播的虚拟礼物等。其最重要的特点是，它和传统货币的兑换比率是固定的。例如，Q币和人民币之间的兑换比率是1:1左右，Q点和人民币之间的兑换比率是10:1；欢聚时代Y币和人民币之间的汇率也为1:1，红钻和人民币之间的兑换比率为100:1。有时，商家为了促销会给予兑换上的一定优惠（如充多少送多少），或者参加活动就送虚拟货币。

第二类是网络游戏中的货币，以大型多人在线角色扮演类游戏（MMORPG）为主（但不限于此），比如暴雪公司《魔兽世界》中的铜币、银币、金币或腾讯公司运营的《地下城与勇士》中的金币等。这类货币一般由打怪掉落生成，或者向非玩家控制角色（NPC）出售虚拟物品换得，媒体上一般称之为游戏币。

该类货币最重要的特点是：无限发行，往往是打怪越多，掉落越多。一般的规则是

打的怪等级越高，掉落的游戏币也就越多。不过游戏开发商会通过出售虚拟道具、升级角色或装备等方式回收流通中的游戏币，一般规则也是购买、升级的装备等级越高，花费的游戏币就越多。由于获得游戏币需要花费大量的时间和精力，有时玩家为了节省时间会直接向其他拥有富余游戏币的玩家购买，因此游戏币也会产生市场兑换比率，这个比率是市场化的，官方不直接干预，交易游戏币和虚拟资产一般使用官方提供的拍卖行或者第三方运营的交易平台。

不过从长期来看，几乎所有网络游戏中的游戏币都是通胀的，有人甚至写过《魔兽经济学：艾泽拉斯的通货膨胀是如何造成的？》这样的文章，因此网络游戏中的游戏币通常不会被用于储值，毕竟游戏世界设计出来的目的是娱乐消费。不过现实中倒有不少依靠打怪卖游戏币赚法币做生活费的案例。随着法律的健全，盗窃游戏中的虚拟道具和虚拟货币也要负民事甚至刑事责任了。可以说，社会在一定程度上认可了虚拟货币的资产属性。

基于区块链技术的数字货币

2008年，美国次贷危机爆发，伴随全球经济衰退和欧洲国家债权危机，有一个人看到政府货币的信心开始动摇了，便开始着手设计一个新的支付系统，于2008年8月注册域名bitcoin.org。当年10月发表了比特币设计白皮书《比特币：一种点对点的电子现金系统》（Bitcoin:A Peer-to-Peer Electronic Cash System），这个人就是中本聪（Satoshi）。在白皮书中，中本聪描述了一种基于点对点的、可以克服“重复消费”问题的新技术，名叫区块链（Block Chain），其本质是一个公共交易总账，每笔交易都由大量分散的计算机网络认证。

“Satoshi”这个名字来自日文，翻译成中文是“认真思考”的意思。很显然，中本聪精通密码学，也知道如何隐匿自己的真实身份。他最后一次出现是在2010年年末，贡献了最后一段程序后，他便把其余工作交给了开发领导者加文·安德森（Gavin Andersen）。

比特币开源客户端发布于2009年1月，从那时起，比特币网络就正式运行了。第一个比特币区块自然是由中本聪创建的，他在交易备注中留下了这样一句话：“2009年1月3日，英国财政大臣被迫考虑第二次出手纾解银行危机。”这句话正是《泰晤士报》当天的头版文章标题，意思是“2009年1月3日，财政大臣正站在第二轮救助银行业的边缘”，一方面证明了比特币诞生于2009年1月3日之后，另一方面也充满了讽刺意味。

2010年，比特币首次有公开的交易。美国佛罗里达州的程序员拉兹洛·汉耶克花费10000枚比特币兑换了两张披萨，相当于每枚比特币兑换0.003美元。

2010年7月，Mt.gox公司成立，它最初交易的是聚会游戏牌Magic，后来才专注比特币的交易业务。三四年后，其成为知名的比特币交易平台之一。

2010年8月，比特币协议暴露了一个重大缺陷，用户可以利用漏洞绕过比特币的经济限制，创造无限量的比特币。8月15日，有一笔交易竟然产生了1840亿枚比特币。几小时内这一问题被发现，并从比特币的账簿中擦除。这也是比特币历史上少有的一次被发现的重大漏洞。

2010年11月，比特币的总市值超过100万美元。

2011年2月，比特币因单价达到1美元而在资讯科技网站Slashdot上广受赞誉。

2011年4月，《福布斯》刊文“加密货币”介绍了比特币。

2011年6月，维基百科开始接受比特币捐助，那时比特币的市值已达2.06亿美元。

同月，高科传媒发表了一篇介绍黑市购物网站“丝路”（Silk Road）的文章，该网站是一家出售违禁品以换取比特币的网站。

同月，Mt.gox作为承担了90%比特币交易的平台，承认用户信息遭泄露，其中包括6万份用户名、电子邮件和密码，部分信息遭泄露的用户还在其他比特币钱包网站MyBitcoin上使用相同的用户名及密码，导致二次被黑，有600人的比特币被黑客盗走。有些人甚至盗取了Mt.gox管理员的登录权限，出售成千上万的假比特币，瞬间令比特币的价格从17.51美元跌至0.01美元。Mt.gox随后宣布这些交易取消，并停止交易7天。从那时起，比特币开始了漫漫下跌路。

2011年的恶性事件发生后，比特币用了一年时间重新获得买家和卖家的信任。2012年出现了首期比特币杂志；首次有知名网站博客平台（WordPress）接受比特币付款；首次有出租车服务和汽车供应商接受比特币付款；首次有私人医疗服务接受比特币支付；比特币教学首次进入公共课堂；首次可以用比特币购买音乐专辑，并且出现了首个比特币诉讼案和只针对比特币的信用违约交换交易。

2012年10月，欧洲央行对比特币的评价是：“如果适用范围扩大化，比特币将对央行的声誉产生负面影响。这种风险在评估央行总体风险时应予以考虑。”

2012年11月，比特币迎来第一次产量减半，也就是每四年左右挖矿获得的比特币数量会减半。

2013年2月，单个比特币的价格首次超过一盎司白银。

同月，新闻网站Reddit接受比特币付费订阅。

2013年3月，比特币总市值超过10亿美元。

同月，比特币的新版本出现“分叉”问题，不同版本的软件对同一个区块的有效性判定不同，这样就使一个比特币支付两次成为可能（分叉之前的比特币在每一条链上只能支付一次）。Mt.gox马上暂停了比特币寄存业务，致比特币价格短期下跌37%，不过很快又恢复到了之前的水平，大部分用户没受影响，且问题最终被修复了。

2013年4月，塞浦路斯宣布没收部分居民存款。比特币在这种新闻背景下脱颖而出，价格先达到100美元，几天后又涨至200美元。

2013年5月，美国政府发现Mt.gox未以资金交易的角色注册公司，随后即冻结了其相关账户。

2013年10月，美国联邦调查局关闭了Silk Road网站，并以毒品交易等罪名抓捕了相关人员，比特币的价格应声大跌，随后又恢复正常。美国联邦调查局声称，在抓捕过程中他们没收了26000枚比特币。

同月，首个比特币ATM机在加拿大温哥华诞生。

2013年11月，时任美联储主席的伯南克表示他们没有权力监督虚拟货币，并认为如果这项创新能够给人类带来一个更安全、快速和高效的支付系统，那么它就具备长期的发展前景。

同月，英国维珍银河公司宣布接受比特币支付预订机票。

2013年12月，中国人民银行宣布所辖银行不接受比特币交易，比特币随即跌至600美元，但很快又反弹至900~1000美元。

2014年2月，Mt.gox倒闭，网站宣称被盗了85万枚比特币，达到当时比特币存量的7%，从那时起比特币再次进入熊市。

2015年，伴随比特币诞生的技术——区块链，再次进入了公众视线。几十家银行加入R3CEV区块链联盟，研发区块链技术用于结算、合约、信托、融资等行为，其中包括富国银行、美国银行、纽约梅隆银行、花旗银行、德意志银行、汇丰银行、摩根士丹利、澳大利亚国民银行等。

同年，以太坊项目正式上线，标志着公有链智能合约技术的发展迈出了重要的一步。同时比特币的基本面也完成了自己的筑底。

2016年6月，比特币价格突破了两年来的新高，从1500元人民币平台涨至5000元；同时，其他区块链货币也走出了波澜壮阔的行情，以太坊几天就涨到了145元。

同月，基于以太坊的应用——去中心化自治组织（decentralized autonomous organization，DAO）曝出了重大漏洞，并导致去中心化自治组织项目上的以太币被黑客窃取，瞬间刺穿了以太坊的泡沫，以太币短短2天就从145元跌至68元，并在该价格段附近震荡。

2016年8月，美元汇率交易所Bitfinex被盗近12万枚比特币，比特币一夜闪崩约26%。

2016年11月，经过三个月的恢复，比特币在大陆的人民币汇率交易所上再创新高。

可以预见的是，这些并不是比特币和竞争币种的终点，在未来几年里，区块链数字货币还会继续书写它们的传奇。