目　录

1、 比特币是基于 P2P 技术的电子现金系统 4
1.1、 比特币交易流程就是交易记录编码到区块，区块上链 5
1.1.1、 比特币钱包是一个存储和管理用户密钥的数据结构 5
1.1.2、 比特币上限 2100 万个，记账权奖励由基础和手续费组成 6
1.2、 去中心化便是所有节点参与记账，所有交易对所有节点透明可见 7
1.3、 记账方式是将“转账记录”组合成“区块”，“区块”上“链条” 7
1.4、 比特币采用工作证明（POW）来获酬，激励各方积极将区块“上链” 8
2、 比特币依赖哈希算法、数字签名、共识算法等技术 9
2.1、 哈希运算通俗的理解就是一堆公式用来产出对应比特串 9
2.2、 数字签名主要应用于发送记录和核实发送记录 10
2.2.1、 比特币地址由钱包里储存的公匙产生 11
2.3、 比特币区块采用默克尔树结构 12
2.4、 比特币采取的共识算法是工作证明类，计算 Nonce（挖矿） 13
2.4.1、 带入 SHA-256 算法算出 Nonce 值（挖矿） 14
3、 比特币产业链主要集中在硬件厂商和交易平台 14
3.1、 上游是硬件厂商，是以比特大陆、嘉楠科技为首的算力单元生产商 14
3.2、 下游是加密货币交易平台，以 Coinbase 为首，零售券商为辅 16
4、 各国对比特币接受程度不一，但是都对其技术充满热情 17
5、 受益标的 19
6、 风险提示 19

图表目录

图 1: 比特币 4 年来最高最低点间涨了近 29 倍 4
图 2: 比特币 2021 年 5 月 28 日 8 日均成交量高于沪深 300 5
图 3: “交易记录”组成“区块”，区块组成“链条” 5
图 4: 比特币钱包就是储存密匙的数据结构，核心就是私钥/公钥 6
图 5: 去中心化网络更加透明，所有节点参与 7
图 6: 任何一笔交易包含交易方地址，金额，手续费时间等信息 8
图 7: 第 685116 个区块包含 1143 笔交易，基础奖励是 6.25 个比特币 8
图 8: SHA-256 就是对输入字符补位，取常量和迭代计算 10
图 9: 通过私匙与文件的哈希值运算来加密，只能通过公匙与文件运算来解密 11
图 10: ECDSA 运用椭圆加密算法加密 11
图 11: 钱包对于公匙进行一系列转换，从而生成比特币地址 12
图 12: 区块上的默克尔树结构便是交易哈希码俩俩组合，哈希运算后再组合 13
图 13: 鄂尔多斯市的矿场年产 13 万个比特币（折合近 300 亿），耗电 500 万千瓦时 14
图 14: 蚂蚁矿机 S19Pro 是目前市面上最受欢迎的矿机之一 15
图 15: 阿瓦隆 A1246 在上述条件中的比特币挖矿收益可达每年 4258 美元 15
图 16: 蚂蚁矿机 S19 Pro 在上述条件中的比特币挖矿收益可达每年 6072 美元 16
图 17: Coinbase 一季度营收 18 亿美元，同比增长 844.82%，已超 2020 年收入 16
图 18: 0 手续费和最高 8%返现的币安 Visa 卡有望推动加密货币的普及 17
图 19: 区块链技术架构可以降低交易成本、提升社会效率和保证透明性 18
图 20: 众多韩国民众依靠比特币买房，禁止比特币交易引来群众请愿 19

表 1： 相关受益标的估值表 19

1、 比特币是基于 P2P 技术的电子现金系统

比特币白皮书对于比特币的定义是一种节点对节点的电子现金系统。从通俗的理解角度出发，**比特币更像是一个全球大账本**。这个大账本拥有三个特质：（1）去中心化。（2）“区块+链”的记账方式导致账本不易篡改。（3）使用电子货币（比特币）来激励各节点参与“上链”。

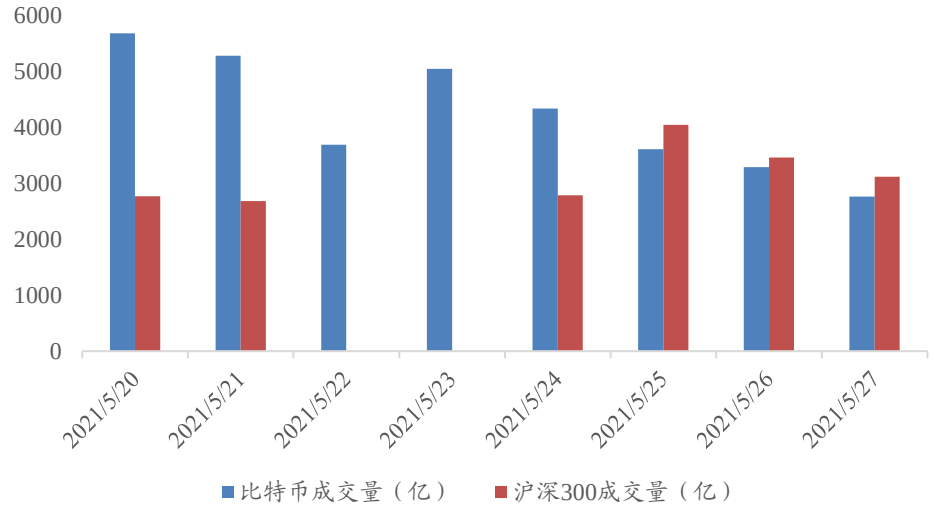
比特币因其价格过山车般波动而备受瞩目。2009 年 1 月 3 日，中本聪发明了比特币系统并挖掘出第一个区块，被称为“创世区块”，最初的 50 个比特币宣告问世，比特币自诞生之日起，经历了多次暴涨暴跌之后，其价格的变动犹如过山车一般。2011 年 1 月，1 个比特币还不值 30 美分，到了 2011 年 6 月 9 日，1 个比特币的价格涨到了 29.55 美元，半年时间涨幅约为 100 倍，此后由于比特币交易平台 Mt.Gox 遭受黑客攻击安全性受到质疑，到 2011 年 11 月，价格低至 2 美元。2012 年 12 月，世界首家比特币交易所在法国诞生，比特币价格重新上涨至 13.69 美元。2013 年 12 月，比特币价格升至 1147 美元，此后市场低迷，2015 年 8 月跌至 200 美元。2016 年，随着比特币年产量开始收缩，美国大选、英国脱欧等事件影响比特币价格飞涨，突破至 1000 美元。2017 年，比特币全年涨跌幅高达 1700%，最高价位高达 19142 美元，最低价格跌至 789 美元。2019 年，受纽交所母公司 ICE 旗下的数字通证期货交易所 Bakkt BTC 月度期货成交量不及预期影响，比特币低至 3178 美元。此后随着众多投资机构、投资人入局，比特币供应减半（每 4 年减少一半）等因素刺激，价格上涨至 62000 美元。

图1：比特币 4 年来最高最低点间涨了近 29 倍

资料来源：Wind

即使在比特币大跌时，截止 2021 年 5 月 28 日比特币 8 日均成交量依然达到 4200 多亿元，同期沪深 300 的 6 日均成交量（剔除双休日）仅为 3144 亿元。

图2：比特币 2021 年 5 月 28 日 8 日均成交量高于沪深 300

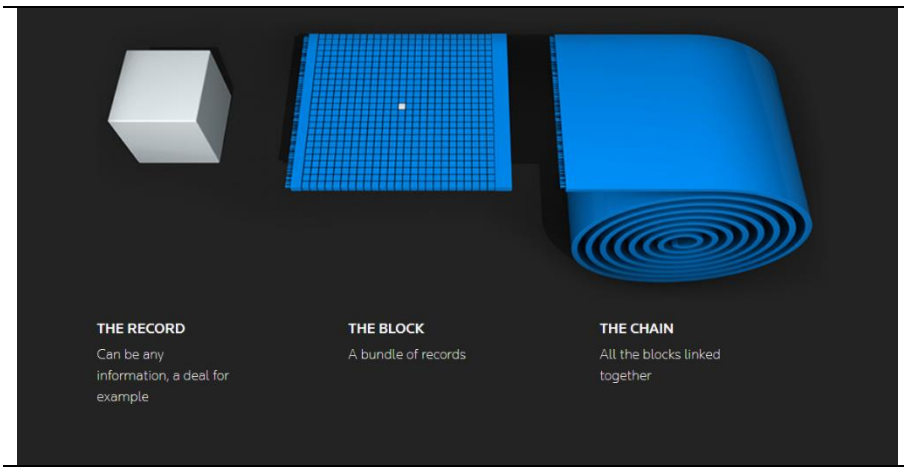


数据来源：Wind、开源证券研究所

1.1、 比特币交易流程就是交易记录编码到区块，区块上链

“交易记录”编成“区块”，区块上到“链条”。假设 A 用户（地址）向 B 用户（地址）汇款，则 A 与 B 的信息会形成一个交易记录。节点会根据自己的策略和记录中的手续费选取不同的记录，在验证电子签名为真后将各汇款信息哈希成一个 256 比特长度的字符串（如图 3 左边的方块）。然后根据区块的大小（比特币区块至多是 2MB，比特币现金一个区块最多是 8MB），节点会把相应的字符串整合到一个区块上（图 3 中的平面），采用默克尔树根（将各交易记录的哈希值俩俩哈希处理，哈希处理之后再将其哈希值与其他哈希值再次进行哈希运算）结构得出该区块的哈希值。最后节点算出 Nonce 值，率先算出 Nonce 值的节点在被其他节点验证后便可以将这自己的区块添加到主链条上“总账本”。 也就是图 3 中最右边的链条。

图3：“交易记录”组成“区块”，区块组成“链条”



资料来源：路透社

1.1.1、 比特币钱包是一个存储和管理用户密钥的数据结构

比特币的账本采用所谓的 UTXO(Unspent Transaction Output)模型，即交易记

录本身形成账本而不是账户信息形成账本。传统的账户信息形成账本就是每个用户有一个账户，每个账户里有多少钱。A 给 B 转账就是 A 账户减少钱，B 账户增加钱。UTXO 则是所有人的转账记录和每个比特币的所有前后流通信息都记录在“链”里，每个账户对应一个地址（对应一个公匙，通过一系列方程运算得出地址），一旦查询这个地址的“余额”，UTXO 就会跟踪地址前后所有记录给予“余额”。**而这个跟踪计算是由比特币钱包完成的。**

广义上比特币钱包是一个应用程序，为用户提供交互界面。狭义上比特币钱包就是储存密匙的数据结构，里面核心就是私钥/公钥这些密钥链，比特币地址由钱包对公匙计算得出。用户用密钥来签名交易，从而证明他们拥有比特币。在比特币网络中，**比特币的所有权是通过数字密钥、比特币地址和数字签名来确定的**，而不是增加自己账户里的数字。钱包（密匙对，也就是比特串对）不需要储存在网络上，可以记录在任何地方。

市面上的不同钱包类型本质就是钱包额外加上一些功能或特性。冷/热钱包便是用保存地点来区分。冷钱包保存在本地，比如个人电脑，U 盘甚至打印到纸上。热钱包便是多了一个保存在网站或者其他云平台上可同步的功能。全节点钱包就是多了在本地额外储存所有区块链的信息，而轻便钱包则是只保留自己相关的信息。中心化钱包就是依赖运行这个钱包的开发公司，储存在交易所里的钱包便是中心化钱包。

图4：比特币钱包就是储存密匙的数据结构，核心就是私钥/公钥

资料来源：木蚂蚁论坛

1.1.2、 比特币上限 2100 万个，记账权奖励由基础和手续费组成

比特币的新产出（类似于新货币的发行）来自获得记账权奖励里的 Coinbase Generation(基础产出)。记账权奖励分为俩部分：（1）Coinbase Generation：此方式为唯一获得新比特币的方式。每次获得记账权的节点在将区块上链时，可以获得这个基础奖励。2009 年 9 月，基础奖励是 50 个比特币，每产生 210000 个区块，该项奖励就减半，又因为区块上链速度控制在一定范围（10 分钟一个），所以换算下来会每 4 年减半。**（2）手续费总和：**即该区块包含的转账的手续费总和。因此节点往往偏好手续费较高的交易记录。

比特币区块上链的速度尽量控制在 10 分钟一个：各节点靠参与竞赛获得记账权，

随着参与方的算力变化，比特币解题难度也在动态调整，目标是控制在 10 分钟上一个区块，俩周产出=6*24*14=2016 个区块，这也就是大家口头说的每 2016 个区块调整一次难度或者差不多俩周调控一次。比特币调控难度主要靠控制目标值前 x 位为 0 来调控难度。目前第 685116 个区块的难度约为 25 万亿，比特币下次的难度大约会调整到目标值前 21 位为 0，或前 84 个比特为 0。

1.2、 去中心化便是所有节点参与记账，所有交易对所有节点透明可见

何为去中心化？所有节点参与记账，比特币的所有交易对所有节点均是透明可见。去中心网络并不是最近才有的概念，早在 1969 年 4 月 7 日，“RFC 1”文档便提出了点对点(point-to-point)相关的网际网络架构。这个点对点网络的概念在 1999 年 Napster(一款音乐共享服务)的运用中开始流行。国人接触到的 BT 下载（种子下载）便是基于点对点网络架构的概念所开发出的群对群（Peer-to-Peer）协议，比特洪流共享方案。国内其他的文件共享协议还有 Gnutella,Chord 和 Pastry 等。根据 Satoshi Nakamato 在比特币白皮书的定义，比特币支付系统便是用户群对用户群交换信息（Peer-to-Peer 交换信息）的互联网体系。目前比特币采用的 P2P 网络协议便是 Gossip，而以太坊采用的是 Kademlia。**Gossip 协议的概念**出现于 1987 年 ACM 上的论文，该协议主要围绕流行病算法（Gossip,或称流言算法）去同步各个节点的数据。即一个节点状态发生变化后便会开始向周边节点发送消息，收到信息的节点又会再次向周边节点发送消息直到所有节点收到消息。流行病协议主要有俩种交互方式：反熵和谣言传播。反熵方式是随机抽取一定数量的节点，互相同步数据以此保证数据的最终一致性。但是此方式会导致网络消息数量增多，开销大。谣言传播方式是指节点接收到新信息之后一定时间内转播新信息，所以消息数量相比反熵则更少但是有小概率情况各节点信息无法达到一致性。

图5：去中心化网络更加透明，所有节点参与

资料来源：区块链技术及应用

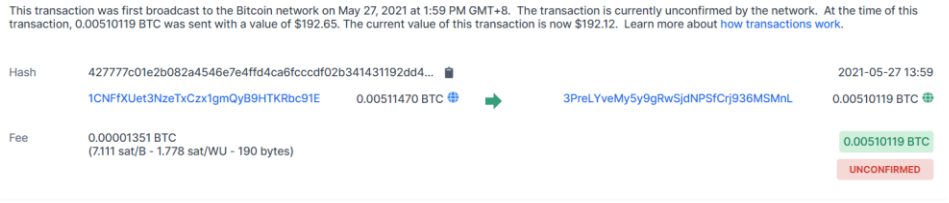
1.3、 记账方式是将“转账记录”组合成“区块”，“区块”上“链条”

何为“区块+链”的记账方式？通俗的讲便是将“转账记录”组合成“区块”。而各“区块”组合成“链条”。

“转账记录”是指一个加密地址往另外一个加密地址发送比特币的过程。如下图所示，下图中加密地址 1CNFfXUet3N zeTxCzx1gmQyB9HTKRbc91E3 PreLYveMy5y9gRwSjdNPSfCrj936MSMnL 汇款 0.00511470 个比特币，其中 0.00001351 个比特币为手续费。42777c01e2b082a4546e7e4ffd4ca6fcccdf02b34 1431192dd4d2c4affe6708 便是此笔交易的哈希码(通过一个不可逆的公式群，将此笔

交易信息变成固定长度的字符串，SHA-256 产出 256-bit（32 bytes）长度的产出）。

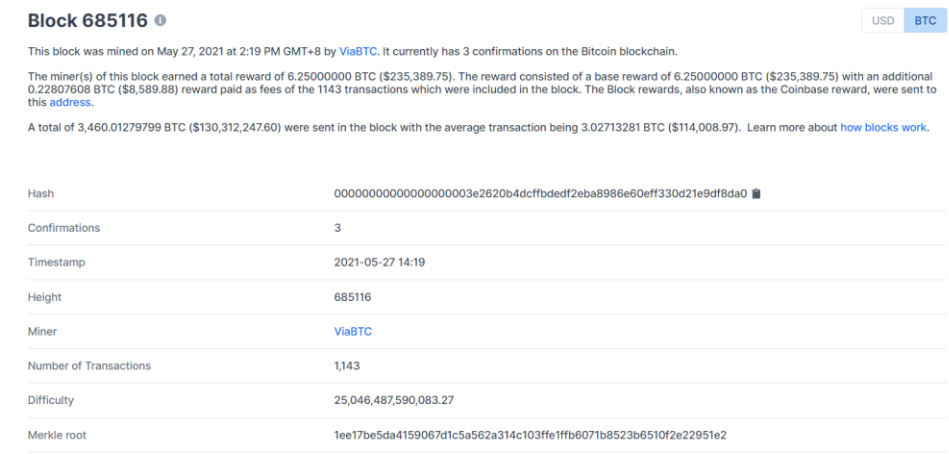
图6：任何一笔交易包含交易方地址，金额，手续费时间等信息



资料来源：Blockchain.com

“区块”便是在把转账记录转换成哈希码后，将各转账记录归纳到一个“区块”里。区块的产生是由节点自主选择的，一般根据手续费的高低确认优先级。在 2017 年 8 月 1 日前，每个区块的限定大小是 1MB，在该天硬分叉后比特币的区块大小最大 2MB，比特币现金的区块大小容量最大为 8MB。一般一个 1MB 的比特币区块包含 1000 多笔交易。下图可以看出这个第 685116 区块于 2021 年 5 月 27 日 14：19 由代号 ViaBTC 的矿工/矿场抢先算出 Nonce 值获得了记账权。此区块包含了 1143 笔交易记录（交易哈希码）。该区块的默克尔树根为 1ee17be5da4159067d1c5a562a314c103ffe1ffb 6071b8523b6510f2e22951e2。此矿工/矿场因此获得了 6.25 个 Coinbase Generation 产生的比特币(基于比特币规则，现阶段对于该区块的基础奖励)，和该区块所有的手续费的总和 0.22807608 个比特币。此个板块的记账权收益结合当前比特币价格约为 243979.63 美元。当前区块的求解难度为 25,046,487,590,083.27（约 25 万亿），相对应的是下一次难度调整求解要算出一个 Nonce，使得目标值前 21 个为 0。

图7：第 685116 个区块包含 1143 笔交易，基础奖励是 6.25 个比特币



数据来源：Blockchain.com

“链条”是由各种已求解已验证的区块组成，相当于一本“书”。拥有记账权的节点将“区块”记到“链条”上相当于在全球“总账本”上加“一页”。

1.4、 比特币采用工作证明（POW）来获酬，激励各方积极将区块“上链”

节点组织好区块后需要完成工作证明以获得记账权，即拥有将这个区块记到“总账本”的权利，以此来获得奖励。比特币采用的是工作证明（POW），即通过完成一道题来与其他节点获得共识。因为多数电子货币是基于公有链技术，即任何人都有权力参与记账。为了杜绝参与者恶意阻碍或者干扰整个区块链记账的一致性，每个

时间点只有一个区块可以上链。而至于哪个区块上链则取决于共识算法。各个电子货币的共识算法不尽相同，比特币采用工作证明作为共识算法，即哪一个节点率先完成工作便拥有了记账权。比特币的共识算法便是求解 Nonce 值。率先算得 Nonce 值便可获得记账权，奖励 Coinbase Gneration 的基础奖励和这个区块所有手续费的奖励。

2、 比特币依赖哈希算法、数字签名、共识算法等技术

2.1、 哈希运算通俗的理解就是一堆公式用来产出对应比特串

哈希运算通俗的理解就是一堆运算公式：主要将信息转换成另外一个信息（散列值，哈希代码等）。这个过程往往会减少储存空间，提高以后信息交换的效率。比特币中的哈希函数特指加密哈希函数。加密哈希函数可以把输入的信息转换成固定长度的输出，且每个比特的输入变化会影响输出值，并且很难从输出值反推回输入值。加密哈希函数主要满足以下特点：

（1）计算效率高(computationally efficient)：正向计算时，单位时间可以完成更多任务，SHA-256 在常规电脑上每秒可完成 2000 万次正向运算

（2）输入敏感(input sensitivity)：每个比特输入的变化都会带来几乎所有输出值的变化

（3）防碰撞(Collision Resistance)：碰撞（不同输入产生相同输出）的现象要少

（4）信息隐藏程度高(Hide information)：不能从结果推断出输入的长度，偶数等任何有关输入信息的痕迹

（5）逆向困难（Irreversible）:不可从产出的哈希值反推到输入的信息

目前比特币采用的 Sha(Secure Hash Algorithm,安全散列算法)-256 是最广泛使用的密码散列函数之一，SHA-256 主要包含以下步骤：

（1）补位：将输入转换成二进制比特，再加长度补充到 mod 512=448.补充规则为先补充“1”，再添加 0 到满足要求为止。长度超过 2^64 则将长度分成 512 的块。

（2）取常量：SHA-256 包含 64 个基础常量，这些常量是由自然数中前 64 位质数的平方根取前 32 比特而来。

（3）迭代计算：使用 6 个计算方程计算得出 32 位字，经过 64 步迭代后产出 256 比特长度的输出。

图8：SHA-256 就是对输入字符补位，取常量和迭代计算

- First, eight variables are set to their initial values, given by the first 32 bits of the fractional part of the square roots of the first 8 prime numbers:

$$H_1^{(0)} = \texttt{0x6a09e667} \quad H_2^{(0)} = \texttt{0xbb67ae85} \quad H_3^{(0)} = \texttt{0x3c6ef372} \quad H_4^{(0)} = \texttt{0xa54ff53a}$$
$$H_5^{(0)} = \texttt{0x510e527f} \quad H_6^{(0)} = \texttt{0x9b05688c} \quad H_7^{(0)} = \texttt{0x1f83d9ab} \quad H_8^{(0)} = \texttt{0x5be0cd19}$$

- Next, the blocks $M^{(1)}$, $M^{(2)}, \ldots, M^{(N)}$ are processed one at a time:
  For $t = 1$ to N
  - construct the 64 blocks W_i from $M^{(t)}$, as explained above
  - set

$$(a, b, c, d, e, f, g, h) = (H_1^{(t-1)}, H_2^{(t-1)}, H_3^{(t-1)}, H_4^{(t-1)}, H_5^{(t-1)}, , H_6^{(t-1)}, H_7^{(t-1)}, H_8^{(t-1)})$$

  - do 64 rounds consisting of:

$$\begin{aligned} T_1 &= h + \Sigma_1(e) + Ch(e, f, g) + K_i + W_i \\ T_2 &= \Sigma_0(a) + Maj(a, b, c) \\ h &= g \\ g &= f \\ f &= e \\ e &= d + T_1 \\ d &= c \\ c &= b \\ b &= a \\ a &= T_1 + T_2 \end{aligned}$$

  - compute the new value of $H_j^{(t)}$

$$\begin{aligned} H_1^{(t)} &= H_1^{(t-1)} + a \\ H_2^{(t)} &= H_2^{(t-1)} + b \\ H_3^{(t)} &= H_3^{(t-1)} + c \\ H_4^{(t)} &= H_4^{(t-1)} + d \\ H_5^{(t)} &= H_5^{(t-1)} + e \\ H_6^{(t)} &= H_6^{(t-1)} + f \\ H_7^{(t)} &= H_7^{(t-1)} + g \\ H_8^{(t)} &= H_8^{(t-1)} + h \end{aligned}$$

  End for

- The hash of the message is the concatenation of the variables H_i^N after the last block has been processed

$$H = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}.$$

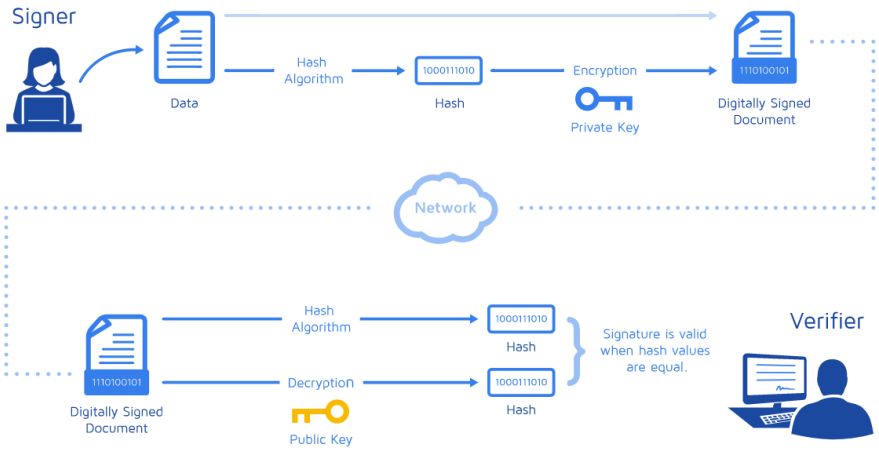
资料来源：SHA-256 公开资料库

2.2、 数字签名主要应用于发送记录和核实发送记录

数字签名主要应用于发送交易记录和核实发送记录。数字签名并不是生活中的签名（不是通过图像扫描录入物理签名的电子版），而是通过非对称加密算法对签名信息进行处理，私匙处理信息，然后任何人可以使用公匙来核验此记录的真实性。具体表现为通过数字签名获得一把公匙和一把私匙（可以理解为 2 组比特串/数字），两把钥匙之间有一定的数学联系（取决于电子签名的方案，但是很难通过公匙反推到私匙）。私匙只有本人知道，而公匙是公开的。电子签名这个动作相当于把私匙与信息内容进行一定的方程运算。核验时，把公匙与信息内容进行运算可以确认信息是不是准确。通过此类方案电子签名过的文件便有了独特性，一旦公匙不能验算，则此文件不是该公匙对应的私匙所签。

多数数字签名方案就是通过私匙与文件的哈希值运算来加密，而解密或者确认只能通过公匙与加密了后文件运算来解密。签名者先对文件/文档进行哈希函数处理得到哈希值（此案列中，签名者想让所有人验证信息是他发的，但是不想让大家知道文件的内容，故发送者先对文档内容进行哈希运算），再将私匙与文档的哈希值组合一起再进行加密运算得到新的签名文件。验证者获得了签名文件和公匙。验证者只要将签名文件进行哈希运算得到哈希值（一组数字/比特串）。再使用公匙对文档进行签名方案的解密运算得到一组数字/比特串。如果哈希值与解密运算的结果相同，则在该方案里，我们可以确定签名者的确用这个公匙相对应的私匙对此文档签名了，并且避免了验证者看到文档的内容。

图9：通过私匙与文件的哈希值运算来加密，只能通过公匙与文件运算来解密



资料来源：DocuSign

数字签名算法主要分为三类：（1）**以 RSA 为首的质数分解原理算法。**当前的应用一般推荐 2048 以上长度的私匙。但是随着计算能力的不断提升，大家认为质数分解类的数字签名算法会被破解。（2）**离散对数算法。**因为难以寻找离散对数的解，离散对数算法分配一对密匙来互相验证。核心算法是 G^(ab) mod P=Z 。G 为原文件，ab 为一对密匙（一公一私），P 为一个大质数，Z 为加密后的文件（签名后的文件）。发送者签名文件实际便是算出 Z 和给予 G^(a)的值，验证者凭借 b 计算 G^(ab)mod P=Z 与发送者的 Z 一致来验证签名。（3）**椭圆曲线算法。**因为目前数学界很难解决椭圆曲线离散对数问题。A=BG,A 和 B 为椭圆曲线 Ep 上的点，B 小于 G 的阶（nG=O ∞）的正整数，已知 B 和 G 非常容易求 A.但是如果已知 A 和 G，求 B 会非常困难。因此一般 B 会作为私匙，A 会作为公匙。比特币交易采用的 ECDSA 便是椭圆曲线算法的一种。

图10：ECDSA 运用椭圆加密算法加密

- 1.Alice选定一条椭圆曲线E，并取椭圆曲线上一点作为基点G 假设选定E29(4,20)，基点G(13,23) ，基点G的阶数n=37
- 2.Alice选择一个私有密钥p（p<n），并生成公开密钥K=pG 比如25，K= pG = 25G = (14,6)
- 3.Alice将E和点K、G传给Bob
- 4.Bob收到信息后，将待传输的明文编码到上的一点M（编码方法略），并产生一个随机整数r（r<n,n为G的阶数） 假设r=6 要加密的信息为3,因为M也要在E29(4,20) 所以M=(3,28)
- 5.Bob计算点C1=M+rK和C2=rG C1= M+6K = (3,28)+6*(14,6)=(3,28)+(27,27)=(6,12) C2= 6G =(5,7)
- 6.Bob将C1、C2传给Alice
- 7.Alice收到信息后，计算C1-kC2，结果就应该是点M C1-kC2 =(6,12)-25C2 =(6,12)-25*6G =(6,12)-2G =(6,12)-(27,27) = (6,12)+(27,2) =(3,28)

数学原来上能解密是因为:C1-kC2=M+rK-krG=M+rkG-krG-M

资料来源：博客园开发者网站

2.2.1、 比特币地址由钱包里储存的公匙产生

数字密钥实际上并不是存储在网络中，而是由用户生成并存储在一个文件或简单的数据库中，称为钱包。存储在用户钱包中的数字密钥完全独立于比特币协议，可由用户的钱包软件生成并管理，而无需区块链或网络连接。对公匙进行一系列方程

运算便得到了比特币地址，当别人往这个地址汇比特币，就算拥有了这些比特币。怎么证明拥有？理论上不用证明，因为比特币账本里没有账户的概念。一定要证明的话就用数字签名(私匙运算)证明。只要下次这个汇款提供证明，那么钱就算转出去了（只要能自由转账，即使没有验证自己是否拥有比特币这个动作但是转出的时候能够核验就等于变相的证实了自己拥有）。

钱包对公匙“加工”获得比特币地址：

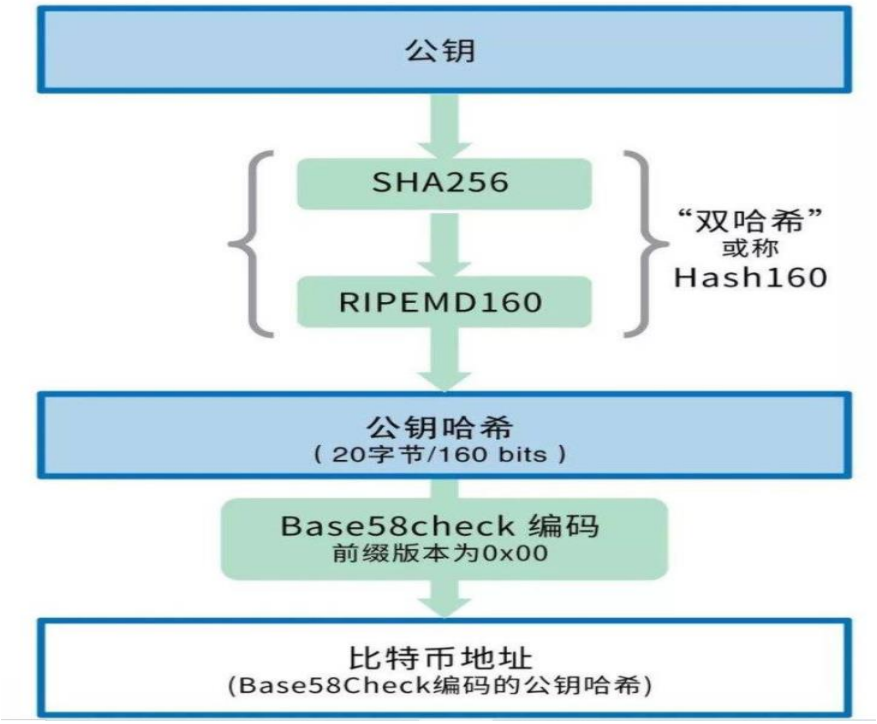
（1）对公钥进行加密：对公钥进行两次哈希运算，第一次通过 SHA-256 算法得到运算结果后，对结果再进行一次 RIPEMD-160 运算，最终得到的结果就是所谓的加密版的公钥

（2）对加密版公钥添加网络标识字节：比特币一共有两个网络：主网和测试网。如果我们需要生成一个主网地址，就要在加密版公钥开头添加 0x00

（3）添加校验值：校验值是通过对第二步得到的结果运行两次 SHA-256 哈希运算，然后取最终哈希值的前四个字节得到，把这个校验值添加到第二步结果的末尾，得到的就是钱包地址了。有了校验值，钱包软件就很容易帮我们判定地址有没有填错或者损坏了。

（4）使用 Base58 编码来表示：十六进制字改成 Base58 格式。

图11：钱包对于公匙进行一系列转换，从而生成比特币地址



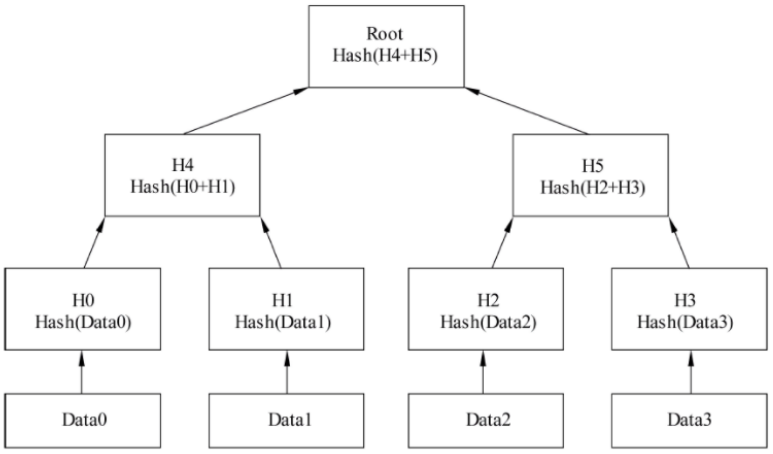
资料来源：博客园开发者网站

2.3、 比特币区块采用默克尔树结构

默克尔树就是一种数据结构，一般形态为二叉树。默克尔树的叶子可以储存数据块也可以是数据块的哈希值。如果下图是一个区块，那么最底下的 Data0,Data1,Data2 和 Data3 便可以对应 4 笔不同的交易记录。然后将各交易记录进行哈希运算，得出的 H0,H1,H2 和 H3 便是记录对应的哈希码。然后俩俩再配对进行

哈希运算得出 H4 和 H5，步骤重复再配对进行哈希运算，便得到这个区块的默克尔树根，也就是图中的 Root。这便是一个只有 4 笔交易记录的区块的默克尔树根产生的过程。

图12：区块上的默克尔树结构便是交易哈希码俩俩组合，哈希运算后再组合



资料来源：区块链技术及应用

默克尔树的结构带来的优势：（1）比对极其有效率。一般一个区块有上千笔交易，如果各交易正常无异常，我们可以直接比对默克尔树根值来一次确定上千笔记录。（2）定位修改点极其方便。一旦发现树根变化了便可以对比 H4 和 H5 的情况定位出错的区域，如果 H5 出错则对比 H2 和 H3，如此循环（假设区块里有数千笔）很快便可以发现修改了的地方。

2.4、比特币采取的共识算法是工作证明类，计算 Nonce（挖矿）

多数电子货币都是基于公有链技术，即任何节点都可以参与记账。可以想象一堆人记账，众节点很难保证一致性和正确性。由于在去中心化 P2P 网络中，参与的节点自身状态，信息量和网络情况不尽相同，为了保证大家的共识，众节点需要一个规则来保证记账的正确。因此共识算法应运而生，**共识算法就是一套规则，在单位时间里，共识算法选出一个节点记一部分的账，然后大家监督。**

比特币采用的共识算法便是 POW（Proof of Work,工作证明）类共识算法：各节点参与竞争，赢家获得记账权，记完这一笔账变各节点再次参与竞争。比如说比特币一节点率先算出 Nonce 值后可以将一个区块（1000 多笔交易记录）上链（记到总账上）。下一个区块又要各节点再次参与竞争谁先算出 Nonce 值。基本上难度会上下调控到差不多 10 分钟一个区块上总账的频率。而我们这个 Nonce 值便是一种工作证明的数字化体现。此外，只要保证诚实节点占总算力的 50%以上，当前最长链的下一个区块也是诚实节点产生的。工作凭证并非都是算 Nonce 值，其他一些电子货币比如说质数币便是计算下一个大质数。工作凭证类算法提高了支付系统的安全性，延续了区块的生长但是带来极大的计算开销。剑桥大学最新统计，单比特币一种电子货币的工作证明竞争（挖矿）就消耗了 1213.8 亿千瓦的电，相当于 1.7%的中国用电总量，超过了希腊、丹麦、匈牙利和冰岛 4 个欧洲国家的总和。

图13：鄂尔多斯市的矿场年产 13 万个比特币（折合近 300 亿），耗电 500 万千瓦时

资料来源：数码科技评论员

PO*凭证类共识算法：为了解决大能量消耗，很多方案采取其他一些属性（持币数量、持币时间、计算资源，*便是指代某种资源）来定义出相应节点在一个时间段来记部分账，而非单纯的算题最快者才能记账。这些方案虽然降低了总体的投入，但是因为不够公平、过于集中化、未被大量验证等等原因没有足够的流行起来。

BFT(Byzantine Fault Tolerance，拜占庭容错类算法)是指各节点定期选出领导者来记账，其他节点验算。一旦有领导节点出错，其他节点可以推票推翻原节点选出其他节点。此类方案极大的减少了工作证明带来的计算支出，但是极大的增加了沟通成本。业界普遍认为此类方案最多承受 100 个节点。

结合可信执行环境的共识算法是软硬结合，指在与普遍操作系统（Rich OS）并存一个可信执行环境，该环境绝对安全，无法被外部干预。可信执行环境能访问的软硬件资源是与 Rich OS 完全分离，保证安全性。通过可信执行环境对区块链节点进行限制，很大程度上可以规避不良节点和恶意操作。

2.4.1、 带入 SHA-256 算法算出 Nonce 值（挖矿）

所谓的挖矿就是将上一个区块的哈希值+本区块的默克尔树根，再加一个 Nonce 值组合的字符，排列进行哈希运算之后得出前 X 位等于 0 的哈希值。通俗的讲电脑就是暴力破解不断往 SHA-256(上区块哈希值，默克尔树根，Nonce)=前 X 位为 0 的方程不断的代入数值，直到得出前 X 位为 0 的值就可以宣告自己得出 Nonce，并且发布出来。通过验算后便可以获得记账权和记账奖励。

3、 比特币产业链主要集中在硬件厂商和交易平台

3.1、 上游是硬件厂商，是以比特大陆、嘉楠科技为首的算力单元生产商

基于竞争工作证明，目前硬件设施是以比特大陆（蚂蚁矿机系列）、嘉楠科技（阿瓦隆系列）为首的算力单元生产商，为辅的有众多的风扇、排线、温控等设备商。

图14：蚂蚁矿机 S19Pro 是目前市面上最受欢迎的矿机之一

资料来源：比特大陆官网

（1）嘉楠科技作为全球区块链第一股，在 2019 年 11 月 21 日于美国纳斯达克上市，股票代码 CAN。**公司目前主营业务为销售针对 SHA-256 计算的计算单元，并配套算力单元出租和矿池运维等服务**，公司 2020 年收入从 14.23 亿人民币下滑至 4.48 亿人民币。公司目前最新款的阿瓦隆 A1246 集成了 360 个针对 SHA-256 计算的集成电路，算力达到了每秒 90 万亿次哈希运算，耗能 0.04w/GHs。假设在呼和浩特运行 A1246 竞争比特币的工作证明，以当地每度电 0.427 元（6.7 美分）计算，结合当前约 25 万亿的难度，6.25 个比特币的基础奖励，每比特币 38753 美元，在加入矿池（以矿池为单位，获得奖励后根据矿池内算力加权均分）后每天净收益为 11.66 美元，约人民币 67.14 元，其中每天收入 17.42 美元，支出电费 5.76 美元。**如果系数保持不变，一年每台 Ava1246 挖矿比特币的净收益约为 4256 美元，折合人民币 27110 元。阿瓦隆最新的矿机方案是简化内部结构，以方便更换算力板，配备液冷方案，一个液冷槽可以浸泡 90 台设备。**

图15：阿瓦隆 A1246 在上述条件中的比特币挖矿收益可达每年 4258 美元

AvalonMiner 1246's Profits At This Difficulty

Share this configuration

Period	Mined BTC	Mined USD	Electricity Costs (USD)	Profit
Daily	0.00045	$17.42	$5.76	$11.66
Monthly	0.013486	$522.61	$172.80	$349.81
Yearly *	0.164076	$6,358.41	$2,102.35	$4,256.07

资料来源：加密货币挖矿收益计算器

（2）**比特大陆同样是主营算力芯片，围绕算力单元打造算力云和矿池运维等业务。公司还未上市，Investopedia 报道 IPO 估值大约在 400 亿美元到 500 亿美元之间。**公司最新的蚂蚁矿机 S19Pro，算力达到了每秒 110 万亿次哈希运算，耗能

29.5J/THs。在上述同等条件下，每天净收益为 16.63 美元，约人民币 106 元，其中每天收入 21.29 美元，支出电费 4.66 美元。**如果系数保持不变，一年每台 S19 Pro 挖矿比特币的净收益约为 6072 美元，折合人民币 38679 元。在比特币工作证明板块（求算 SHA-256 Nonce 值方面），目前市场上每千瓦时收益最高的前 4 款矿机均出自比特大陆蚂蚁系列矿机。分别为 S17 Pro, S19，S19 Pro, S19j，在上述条件中（额外假设 1 年报废）净收益收益分别对应为$0.14/KWH，$0.13/KWH，$0.13/KWH 和$0.11/KWH。**

图 16：蚂蚁矿机 S19 Pro 在上述条件中的比特币挖矿收益可达每年 6072 美元

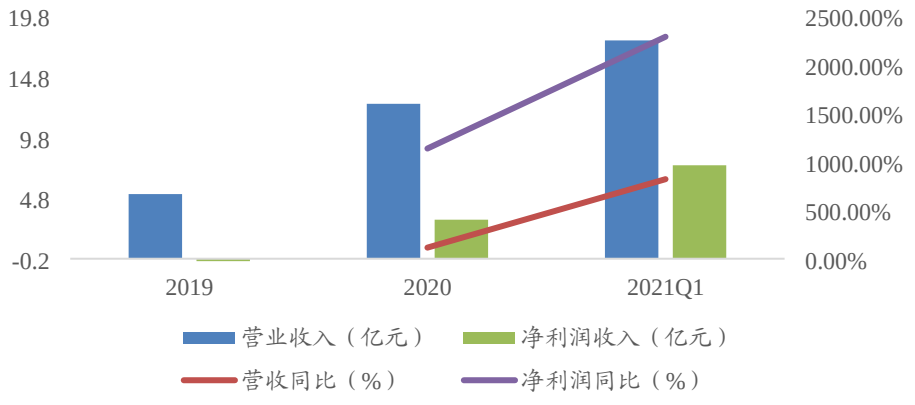
资料来源：加密货币挖矿收益计算器

3.2、 下游是加密货币交易平台，以 Coinbase 为首，零售券商为辅

目前所有加密货币包括比特币并没有完全被社会认可，投机属性占比更重。这就意味着我们无法使用这些货币在现实中真正流通，目前加密货币的流通途径主要是在加密货币交易所将加密货币转换成各国货币。因此**目前交易平台可以被认为是比特币的“应用端”，使用加密货币的地方。**

Coinbase 是美国交易量最大的加密货币交易所，并于 2021 年 4 月 13 日在纳斯达克交易所上市。公司收入主要来自交易服务（手续费）和认购服务。2019 年到 2020 年收入从 5.3 亿美元增长到了 12.7 亿美元，更为疯狂的是 2021 年 1 季度收入达 18 亿美元，同比增长 844.82%，超 2020 年全年收入的近 50%以上。公司披露自身平台将 100 多个国家，4300 多万零售客户，7000 个机构和 115000 个生态系统参与到加密货币的交易中来。

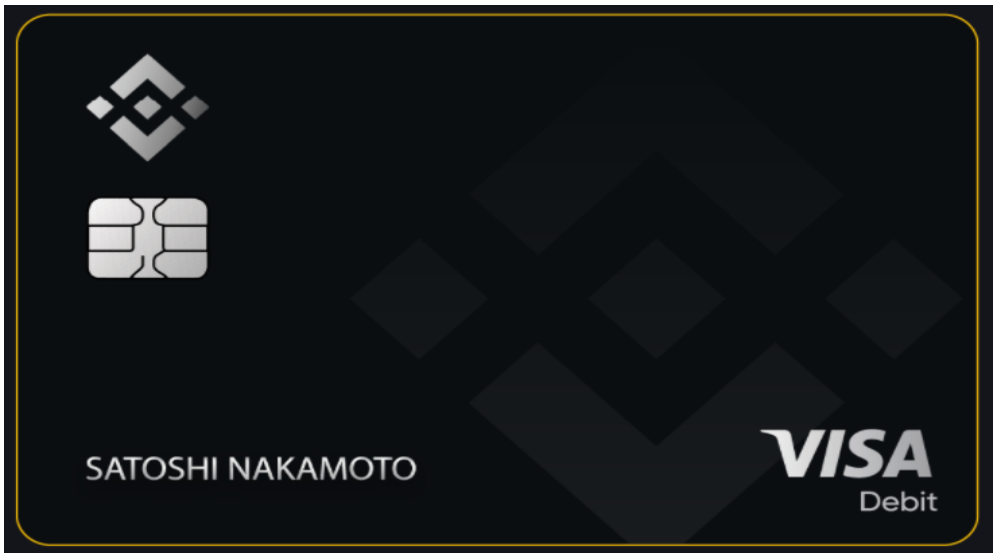
图 17：Coinbase 一季度营收 18 亿美元，同比增长 844.82%，已超 2020 年收入



数据来源：Wind、开源证券研究所

币安交易所（Binance）由加拿大籍华人赵长鹏创立。公司暂未上市。公司除了交易业务，矿池租赁业务以外还推出了加密货币 Visa 卡和 Mastercard 卡，自称为全球加密货币交易量最大速度最快的加密货币交易所。用户在现实付款刷卡时，时时将电子货币转换成所需的现实货币支付。此举在各大加密货币交易平台中属于新颖战略，也对加密货币的推行起到了推动作用。

图18：0 手续费和最高 8%返现的币安 Visa 卡有望推动加密货币的普及



资料来源：Wind

火币交易所由前甲骨文员工李林创立。公司暂未上市。公司自称近 24 小时（常规日 5 月 28 日晚 9 点），在平台上交易的数字资产交易近 740 亿美元（按照万一手续费预估 24 小时收入 740 万美元），加密货币交易量全球前三，客户破千万。

除了专门交易加密货币的交易所，各国越来越多的券商也都开始支持比特币与现实货币的交易，例如最受散户欢迎的美国持牌券商罗宾汉（Robinhood），美国第二受散户欢迎的持美股牌照的中国券商微牛（Webull）都支持比特币等数字货币的交易。世界头部的互联网券商盈透（Interactive Brokers）和嘉信(Charles Schwab)等券商虽不支持购买比特币等加密货币的现货但是支持比特币等加密货币的期货交易。

4、 各国对比特币接受程度不一，但是都对其技术充满热情

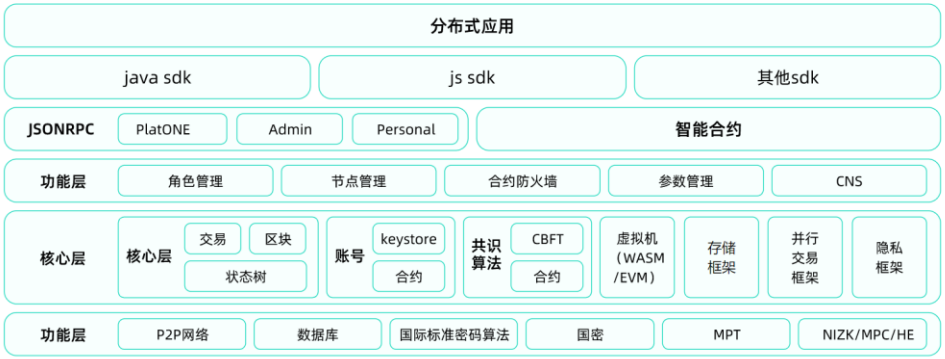
总的来说，没有人知道哪一款加密电子货币会被真正的流通起来，从而取代不断放水的美元，成为世界货币。但是**比特币的记账技术和配套算法降低了社会交易成本，提高了社会效率和提升了交易的透明性。**

降低社会交易成本：区块链网络中所有信息多方共识，可信和不可篡改，简化了传统交易中审查、确认等流程，甚至不需要重复的对账和结算，从而降低了交易成本。

提升社会效率：当前金融系统是一个复杂庞大的系统，跨行跨国汇兑往往需要很多的中间层，漫长的交易链条加上不统一的监管，使得交易效率低下。

交易的透明性：公有链的技术可以让所有人查询账本，利用加密地址可以隐藏身份。这就保证了交易的透明同时保证了个人的隐私。

图19：区块链技术架构可以降低交易成本、提升社会效率和保证透明性



资料来源：矩阵元

中国：虽然中国对于加密货币如比特币、以太币本身秉持慎重和反对态度，但是政府和企业对于加密货币所运用的区块链技术展现出浓厚的兴趣并且支持区块链等技术的发展。

2014 年起，中国央行就开始致力于 DCEP(中国央行数字货币系统，Digital Currency Electronic Payment)的研究，俗称数字人民币。

2016 年 3 月 10 日，中国人民银行表示加密货币为非法定数字货币，不建议投资者购买。

2017 年 9 月 4 日，央行等七部门联合叫停以 ICO 融资为代表的代币发行融资。同年，中国人民银行邀请各银行和机构共同开发数字人民币系统。

2020 年 4 月，数字人民币系统在深圳、成都、苏州和雄安进行试运行。

美国：美国对于加密数字货币持积极态度，重心放在加强对数字货币交易的监管。2018 年美国众议院召开第二次区块链听证会，将区块链上升到“变革性技术”，探讨区块链在金融和政商的应用。

2014 年加州通过了 AB129 法案，包括数字货币、积分和优惠券的美元替代品味合法货币。同年，纽约将加密货币管理和比特币牌照相关法规纳入《纽约金融服务法律法规》，启动对比特币的监督。

2015 年纽交所入股 Coinbase,获批成立比特币交易所，美国以纽约州为代表的比特币监管立法初步完成。

2021 年 4 月 13 日 Coinbase 在纳斯达克交易所上市。

韩国：韩国从一开始的明令禁止加密数字货币改为积极支持。

2017 年 9 月，韩国政府规定全国禁止 ICO。

2018 年，1 月 12 日，4 万群众请愿罢免金融监管局主席。同年 2 月，法院裁定比特币可以通过交易所兑换成货币，比特币可以作为一种商家支付手段，应该具有经济价值。同年 3 月，韩国政府计划取消 ICO 禁令，允许一定条件下的代币销售。

图20：众多韩国民众依靠比特币买房，禁止比特币交易引来群众请愿

资料来源：视觉中国

日本：日本从一开始便支持加密货币，只是在 2018 年黑客盗窃事件后监管趋严。

2016 年 5 月 25 日，日本国会正式承认加密数字货币为合法致富手段并将其纳入法律法规体系之内。

2017 年 3 月，日本正式承认比特币作为法定支付的地位。同年 4 月承认加密货币的合法支付地位，所有投资者会受到法律保护。

2017 年 11 月，日本政府发起 ICO，振兴地方经济。

2018 年 3 月，黑客事件后日本金融厅开始大力整顿数字货币市场。

5、 受益标的

表1：相关受益标的估值表

股票代码	股票名称	股价（5 月 31 日）	EPS(元)		PE（倍）		评级
			2021 年 E	2022 年 E	2021 年 E	2022 年 E	
CAN.O	嘉楠科技	53.50	1.12	1.88	47.77	28.46	未评级

数据来源：Wind、开源证券研究所（嘉楠科技为 Wind 一致预期预测数据，汇率使用 2021 年 5 月 31 日：1USD=6.3690RMB）

6、 风险提示

区块链技术发展不及预期。区块链是一种新技术，尚处于发展初期，区块链技术、生态、工具和应用正在快速发展和演进。

区块链应用不及预期。区块链的落地不只是技术问题，还涉及到法律、经济等多方面的因素，需要更多人的参与和推动。

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为境内专业投资者及风险承受能力为C4、C5的境内普通投资者。若您并非境内专业投资者及风险承受能力为C4、C5的境内普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。
因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%～20%；
	中性（Neutral）	预计相对市场表现在－5%～＋5%之间波动；
	减持	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡	预计行业弱于整体市场表现。
备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。		

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。