blockchain

# Factom—<http://factom.org/>

* 利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录方式
* Factom维护了一个永久不可更改的、基于时间戳记录的、区块链数据网络。大大减少了进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。
* 免费电子书的“古腾堡”计划: 通过4个哈希值在区块链上记录28000本书
* 利用区块链技术助力各种各样应用程序的开发，包括审计系统，医疗信息记录，供应链管理，投票系统，财产契据，法律应用，金融系统等
* 帮助美国银行节约170亿美元的成本
* 防止索尼公司的图片泄露丑闻的发生
* 7万亿美金的土地交易市场
* 创造新的应用程序，并把数据保存在区块链上面，同时不用受到直接把数据写入比特币区块链的各种限制：例如写入的数据速度，成本，大小等限制。我们致力于让每一位开发者都有使用区块链技术的能力，并借此开发出下一代的应用程序。
* 源码: <https://github.com/FactomProject/>

# 以太坊—https://www.ethereum.org/

* 去中心化的智能合约平台
* 彩色在块链之上构建智能资产和定制货币及资产管理系统的最初尝试是在比特币协议之上叠加新的协议
* 努力在比特币协议之上建立更高级协议,正如在 TCP 之上建立 HTTP,是值得赞赏的,也确实是走向更 高级的去中心化应用的正确道路。然而,在比特币协议之上创建彩色币和元币的尝试更象是在 SMTP 上创建 HTTP
* 以太坊并不以取代前述的彩色币或元币协议为目的,而是旨在成为一个提供超强脚本系统的优秀底层协议,在其上可以创建任意高级的合约,货币及其它去中心化应用
* 以太坊重新定义了自己的区块链结构, 交易结构, hash 算法和挖矿算法
* 以太坊内建货币—以太币
* 应用:
  + 子货币---代替法币, 黄金, 债券等, 以太币和子货币交易
  + 金融衍生品
  + 身份和信誉体系
  + 去中心化自治机构(DAC)
* 脚本—图灵完备的脚本

# 小蚁—<https://www.antshares.com>

* 小蚁是基于区块链技术，将实体世界的资产和权益进行数字化，通过点对点网络进行登记发行、转让交易、清算交割等金融业务的去中心化网络协议
* 通过网关引入法币
* 对接实体金融, 身份认证和电子签名, KYC 和 AML
* 超导交易
* 隐私地址
* 原生资产---小蚁股和小蚁币
* 记账机制:
  + 小蚁使用类似比特币的区块链来记录数据
  + 共识机制—中性记账 使用小蚁股投票选出记账人, 使用 ssss 方案(密码共享)达成共识, 防止合谋
  + 1, 计算记账人数, 选出记账人 N+1个
  + 2, 每个记账人都产生一个随机数, 通过 ssss 分成 N 份, 用每个记账人的公钥加密, 广播
  + 3, 每个记账人使用私钥解密自己公钥加密的那份, 并广播( 一共解出 N 份)
  + 4, 记账人收到 K 个解密就能解出随机数, 最后得到 N 个随机数
  + 5, 加上自己, 一共N+1个随机数合并就是新区块的随机数( 如何合并?应该对记账人排序, 然后顺序合并)
  + 广播随机数同时也广播交易, 当2/3的记账人区块中的交易达成一致, 生成新区块
* 小蚁的共识机制币 ripple 的简单, 同样不需要花费资源达成一致

# 共识系统—[https://conSsensys.net/](https://consensys.net/)

* 聚焦以太坊, 为开发者和终端用户提供各式各样的程序和工具创建区块链系统

# Ripple—<https://ripple.com/>

* 是一个全球的结算网络: Ripple 提供全球金融解决方案，让全世界像如今交换信息这般交换价值 - 创造互联网价值 (IoV)。Ripple 解决方案让各银行直接即时交易并且准确无误地结算，从而降低总结算费用。世界各地的银行与 Ripple 合作以完善其跨境支付产品，加入不断增长的全球金融机构和做市商网络，为互联网价值奠定了基础。
* Ripple 的问题是去中心化不彻底, 需要用户选择代表—信任的 Validater, 但是有可能被代表. 这和比特币完全去中心化的情况不同.
* Ripple 的第二个问题是需要用户对网关的信任. 网关类似银行, 任何人都可以作为网关. 银行都可能作恶, 不可信, 更何况个人.

# circle—<https://www.circle.com/zh>

* 利用比特币在任何地方发送和接收资金
* 发款和收款应该像使用电子邮件或短信那么简单。Circle 让付款变得即时、安全和全球化。
* 在几分钟内，您就可以在任何地方与任何人进行发款和收款操作。您还可以轻松关联您的银行帐户、借记卡或信用卡。
* Circle 为客户资金的全部余额提供保险，以防 Circle 的数字或物理数据储存被破坏，导致客户的比特币丢失或被盗（当然这种情况不太可能发生）。该保险由高评级全球承销商提供。
* email 用户名绑定你的 bitcoin 地址
* 你的 bitcoin地址绑定借记卡或者信用卡
* 必须是美国发行的借记卡和信用卡
* 应该只支持美元和 bitcoin 支付
* 你可以支付和接收 bitcoin 和美元
* 可以用美元够买只接收 bitcoin商家的商品
* 没有源码
* 支持 iOS 和 android 客户端

# SPV--[http://8btc.com/thread-15128-1-1.htmlh](http://8btc.com/thread-15128-1-1.html)

# gocoin--<https://en.bitcoin.it/wiki/Gocoin>