区块链与数字货币

浙江大学 杨小虎

2020年12月8日

03 数字货币与区块链生态

比特币之后的数字货币与区块链发展

- 竞争币、山寨币
  - Litecoin 莱特币
  - Dogecoin 狗狗币
- 新一代公共区块链平台
  - Ethereum 以太坊
  - EOS
  - ……
- 面向企业应用的区块链平台
  - R3 CEV
  - HyperLedger Fabric
  - Hyperchain
  - 蚂蚁链

- 开发策略
  - 复制、修改开源代码
  - 全新开发
- 技术创新
  - 可编程、可开发
  - 共识算法
  - ……
- 融资创新
  - 代币发行融资（ICO）

区块链形态

联盟链（Consortium Chain）

对产业或者国家的特定清算和结算用途，容易进行控制权限设定，更高的可扩展性。

公有链（任何人）

任何人都可以参与，容易部署应用程序，全球范围可以访问，不依赖于单个公司

私有链(内部链)

由单独的个人或者组织拥有，对组织内部的审计和测试有用。

区块链项目融资

- ICO(Initial Coin Offering)意为首次代币发行，本质是一种产品众筹，是项目对构建基于区块链的产品或服务的承诺。区块链项目完成之前，通过公开售卖部分平台的Token募集资金用于创始团队的开发工作。

- **通证（Token）**是一个区块链生态里的一种权益证明。在经济体系下常被作为区块链生态内的流通的货币，如比特币、以太坊。通常情况下，Token一经发行，便严格按照区块链代码执行，不受个人或机构控制。

世界各国对ICO的态度

国家	态度
美国	各州各有规则，金融监管机构态度不一致
英国	监管机构持观望态度，参与ICO者风险自负
俄罗斯	反对加密货币，正在构建监管框架
中国	全面禁止ICO
日本	允许ICO，相对较活跃

国家	监管政策
美国	• 立法支持投资，鼓励区块链的发展 • 2017年Circle在波士顿，Ripple在旧金山，Coinbase在纽约州都分别获得了数字货币许可证BitLicense • 2017年2月美国亚利桑那州通过区块链签名和智能合约合法性法案 • 美国国会宣布成立国会区块链决策委员会，特朗普政府呼吁发展区块链技术在公共部门中的应用 • 在比特币的态度上，美国也是鼓励投资并实施严格的监管
中国	• 2016年2月，中国的央行行长周小川表示数字货币必须由央行来发行，区块链式研发数字货币可选的基础教育。 • 2016年12月份，国家将区块链列入了十三五国家信息化规划。 • 2016年10月，工信部发布了2016中国区块链技术和应用发展白皮书。 • 2017年9月，中国人民银行等七部委联合发文认定ICO是一种未经批准的非法公开融资的行为，涉嫌非法发售代币票券，非法发行证券，以及非法集资金融诈骗传销等违法行为。
欧盟	• 2016年3月，欧洲央行ECB在《欧元体系的愿景——欧洲金融市场基础设施的未来》这个咨询报告中公开宣布正在探索如何使用区块链技术为己所用。 • 2016年1月19日，英国政府率先发布了长达88页的《分布式账本技术：超越区块链》的白皮书，同时积极评估区块链技术的潜力，考虑它将用于减少金融欺诈降低成本的领域。 • 德国在2016年11月份联合德意志联邦银行和法兰克福金融管理学院召开区块链技术机遇与挑战的大会，大会的主要目的都是对分布式账本的潜在运用展开研究，包括跨境支付跨行转账以及贸易数据的存储等。
新加坡	• 新加坡金融管理局在2016年6月，推出了沙盒机制Sandbox，只要任何在法律规定的受保护中注册的金融科技公司，在事先报备的情况下，允许从事和目前法律法规有所冲突的业务，并且及时以后被官方终止相关业务，也不会追究其相关的法律责任。 • 通过这种沙盒的机制，新加坡政府能够在可控范围内鼓励企业进行各种区块链的金融创新。
日本	• 2016年3月份，日本内阁通过投票将比特币和数字货币均视为数字等价货币。 • 2017年4月1日，日本实施了《支付服务法案》，正式承认比特币是一种合法的支付方式，对于数字资产交易所提出了明确的监管要求。 • 2017年7月，日本新版消费税正式生效，比特币交易将不再需要缴纳8%的消费税，
韩	• 韩国对区块链目前持支持的态度，对比特币以太坊等数字资产在加强监管.。 • 2016年2月，韩国央行在报告中提出鼓励探索区块链技术。

莱特币 Litecoin

- 2011年发布
- 出块速度：2分半
- 货币总量：到2140年达到8,400万
- 工作量证明算法：scrypt
- 首次上线时间：2011年11月9日
- 创始人：李启威 Charlie Lee 前谷歌工程师
- 网站： https://litecoin.org/

狗狗币 Dogecoin

- 出块速度：60秒
- 货币总量：到2015年达到100,000,000,000（1,000亿）
- 一致性算法：scrypt
- 网站： https://dogecoin.com/

Scrypt算法

- 由FreeBSD黑客 Colin Percival开发的，原来是用于密码抗rainbow table攻击设计的。
- Scrypt计算所需时间长，而且占用的内存也多，使得并行计算多个摘要异常困难。
- Scrypt也是一种符合区块链PoW共识机制的算法。Scrypt算法过程中也需要计算哈希值，但是Scrypt计算过程中需要使用较多的内存资源。
- 可以抗ASIC挖矿（ASIC resistance）
- ASIC（Application Specific Integrated Circuit ）专用集成电路芯片

Scrypt算法

scrypt

```
Input:
        P Passphrase, an octet string.
        S Salt, an octet string.
        N CPU/Memory cost parameter, must be larger than 1,
                a power of 2, and less than 2^(128 * r / 8).
        r Block size parameter.
        p Parallelization parameter, a positive integer
                less than or equal to ((2^32-1) * hLen) / MFLen
                where hLen is 32 and MFlen is 128 * r.
        dkLen Intended output length in octets of the derived
                key; a positive integer less than or equal to
                (2^32 - 1) * hLen where hLen is 32.
Output:
        DK Derived key, of length dkLen octets.
Steps:
 1. Initialize an array B consisting of p blocks of 128 * r octets
    each:
     B[0] || B[1] || ... || B[p - 1] =
       PBKDF2-HMAC-SHA256 (P, S, 1, p * 128 * r)
 2. for i = 0 to p - 1 do
       B[i] = scryptROMix (r, B[i], N)
     end for
 3. DK = PBKDF2-HMAC-SHA256 (P, B[0] || B[1] || ... || B[p - 1],
                                    1, dkLen)
```

scryptBlockMix

```
Parameters:
        r Block size parameter.
Input:
        B[0] || B[1] || ... || B[2 * r - 1]
               Input octet string (of size 128 * r octets),
               treated as 2 * r 64-octet blocks,
               where each element in B is a 64-octet block.
Output:
        B'[0] || B'[1] || ... || B'[2 * r - 1]
               Output octet string.
Steps:
  1. X = B[2 * r - 1]
  2. for i = 0 to 2 * r - 1 do
       T = X xor B[i]
       X = Salsa (T)
       Y[i] = X
     end for
  3. B' = (Y[0], Y[2], ..., Y[2 * r - 2],
           Y[1], Y[3], ..., Y[2 * r - 1])
```

scryptROMix

```
Input:
        r Block size parameter.
        B Input octet vector of length 128 * r octets.
        N CPU/Memory cost parameter, must be larger than 1,
                a power of 2, and less than 2^(128 * r / 8).
Output:
        B' Output octet vector of length 128 * r octets.
Steps:
  1. X = B
  2. for i = 0 to N - 1 do
       V[i] = X
       X = scryptBlockMix (X)
     end for
  3. for i = 0 to N - 1 do
       j = Integerify (X) mod N
             where Integerify (B[0] ... B[2 * r - 1]) is defined
             as the result of interpreting B[2 * r - 1] as a
             little-endian integer.
       T = X xor V[j]
       X = scryptBlockMix (T)
     end for
  4. B' = X
```

Salsa20/8

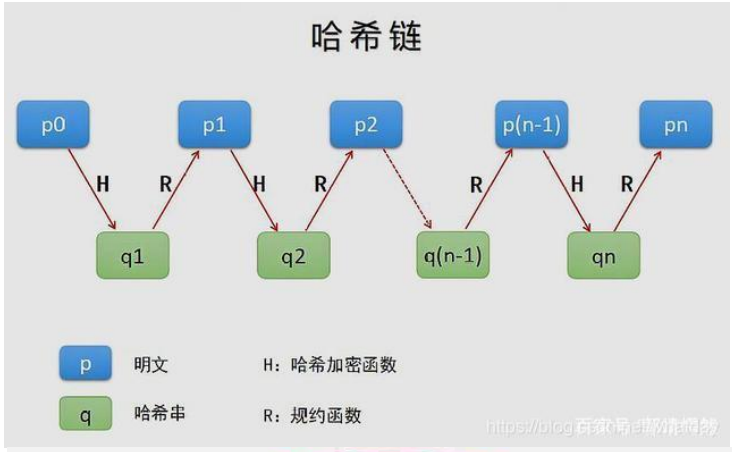
```
#define R(a,b) (((a) << (b)) | ((a) >> (32 - (b))))
void salsa20_word_specification(uint32 out[16],uint32 in[16])
{
    int i;
    uint32 x[16];
    for (i = 0;i < 16;++i) x[i] = in[i];
    for (i = 8;i > 0;i -= 2) {
        x[ 4] ^= R(x[ 0]+x[12], 7); x[ 8] ^= R(x[ 4]+x[ 0], 9);
        x[12] ^= R(x[ 8]+x[ 4],13); x[ 0] ^= R(x[12]+x[ 8],18);
        x[ 9] ^= R(x[ 5]+x[ 1], 7); x[13] ^= R(x[ 9]+x[ 5], 9);
        x[ 1] ^= R(x[13]+x[ 9],13); x[ 5] ^= R(x[ 1]+x[13],18);
        x[14] ^= R(x[10]+x[ 6], 7); x[ 2] ^= R(x[14]+x[10], 9);
        x[ 6] ^= R(x[ 2]+x[14],13); x[10] ^= R(x[ 6]+x[ 2],18);
        x[ 3] ^= R(x[15]+x[11], 7); x[ 7] ^= R(x[ 3]+x[15], 9);
        x[11] ^= R(x[ 7]+x[ 3],13); x[15] ^= R(x[11]+x[ 7],18);
        x[ 1] ^= R(x[ 0]+x[ 3], 7); x[ 2] ^= R(x[ 1]+x[ 0], 9);
        x[ 3] ^= R(x[ 2]+x[ 1],13); x[ 0] ^= R(x[ 3]+x[ 2],18);
        x[ 6] ^= R(x[ 5]+x[ 4], 7); x[ 7] ^= R(x[ 6]+x[ 5], 9);
        x[ 4] ^= R(x[ 7]+x[ 6],13); x[ 5] ^= R(x[ 4]+x[ 7],18);
        x[11] ^= R(x[10]+x[ 9], 7); x[ 8] ^= R(x[11]+x[10], 9);
        x[ 9] ^= R(x[ 8]+x[11],13); x[10] ^= R(x[ 9]+x[ 8],18);
        x[12] ^= R(x[15]+x[14], 7); x[13] ^= R(x[12]+x[15], 9);
        x[14] ^= R(x[13]+x[12],13); x[15] ^= R(x[14]+x[13],18);
    }
    for (i = 0;i < 16;++i) out[i] = x[i] + in[i];
}
```

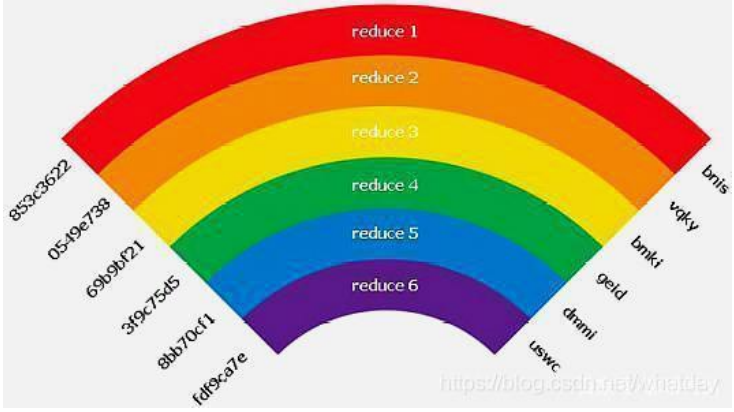
Rainbow table – 高效的密码攻击方法

密码长度为7时的破解

字符集	字母	字母+数字	字母+数字+常用符号	全部字符集
哈希链长度	2,100	2,400	12,000	20,000
哈希链个数	8,000,000	40,000,000	40,000,000	100,000,000
表单数量	5	7	13	20
成功率	99.9%	99.9%	99.9%	99.3%
文件大小	640MB	4,480MB	8,320MB	32,000MB
最大生成时间	17小时	5d天14小时	52天	332天
最大破解时间	7秒	14秒	11分	48分

Rainbow table原理





以太坊（ Ethereum ）

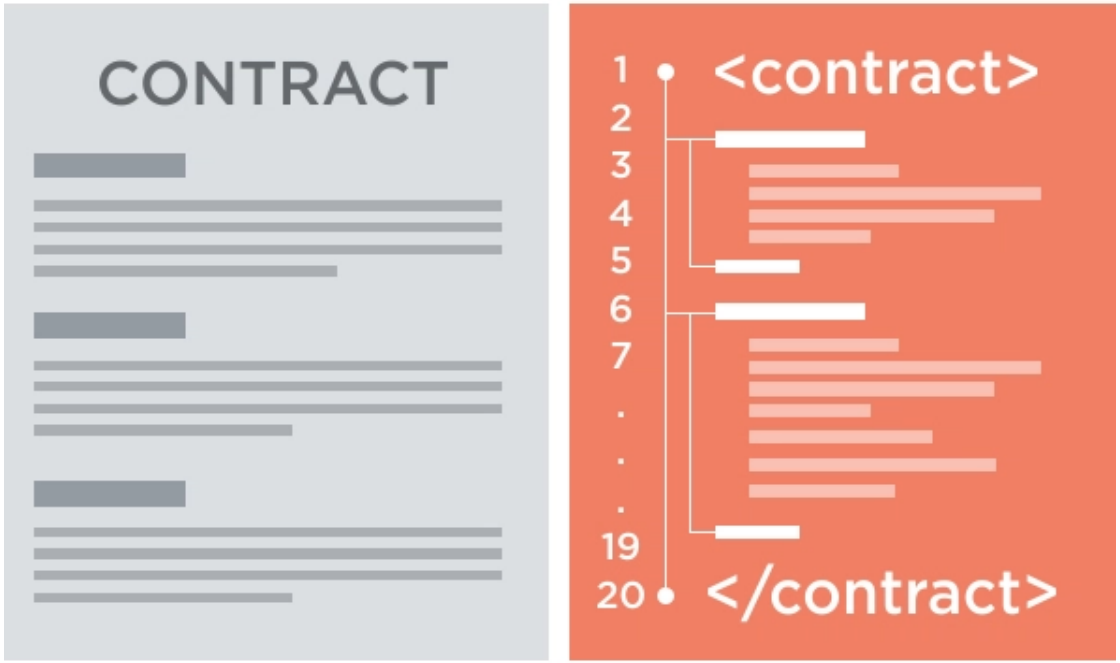
- Ethereum（以太坊）是一个平台和一种编程语言，使开发人员能够建立和发布下一代分布式应用。Ethereum可以用来编程，分散，担保和交易任何事物：投票，域名，金融交易所，众筹，公司管理， 合同和大部分的协议，知识产权，还有得益于硬件集成的智能资产。

- 网站：
  https://www.ethereum.org/

Vitalik Buterin

智能合约

- 基于区块链技术的智能合约系统
  - 智能合约是内嵌于区块中的自定义程序逻辑
  - 当满足一定条件，区块中的程序逻辑会被触发执行合同约定的指令（比如资产清算、赔偿、交割等）。



超级账本 HyperLedger

- 创立于2016年 ，由30个创始公司会员和一套技术和组织治理机构组成。
- 是一个为了提高跨行业的区块链技术的开源合作项目。它是由Linux基金会主导的全球合作项目，包括了金融、银行、物联网、供应链、制造和科技产业的领导者。
- 宣称“自从互联网诞生以来，除了互联网本身，没有比区块链技术更广泛、更根本的革命性技术了”。
- HyperLedger Fabric，一个许可区块链平台，带有chaincode，由Digital Asset和IBM提出。
- 网站： https://www.hyperledger.org/

R3 CEV

- R3CEV是一家总部位于纽约的区块链创业公司,R3是由其发起的区块链联盟，成员主要有全球金融巨头组成。
- 产品：
  - Corda, an open-source blockchain platform
  - Corda Enterprise, a commercial version for enterprise usage
- 网站： https://www.r3.com/

EOS

- Enterprise Operating System
- EOS.IO 软件引入一种新的区块链架构设计，它使得去中心化的应用可以横向和纵向的扩展。 这通过构建一个仿操作系统的方式来实现，在它之上可以构建应用程序。 该软件提供帐户、身份验证、数据库、异步通信和跨越数百个 CPU 内核或集群的应用程序调度。 由此产生的技术是一种区块链架构，它可以扩展至每秒处理百万级交易，消除用户的手续费，并且允许快速和轻松的部署去中心化的应用。
- 共识机制：DPOS
- 热点不断：宣称区块链3.0、ICO融资40亿美元、竞争超级节点、爆出若干安全漏洞
- 网站： https://eos.io/

数字货币钱包

- “钱包”是指用于存储和管理用户密钥的容器，钱包里没有“钱”，钱包软件一般还控制用户访问权限，管理密钥和地址，跟踪余额以及创建和签署交易。
- 全节点：Bitcoin Core
- SPV轻钱包，只维护与自己相关的区块链数据
- 中心化钱包（在线钱包），依赖自己的中心化服务器，如blockchain.info
- 硬件钱包、冷钱包

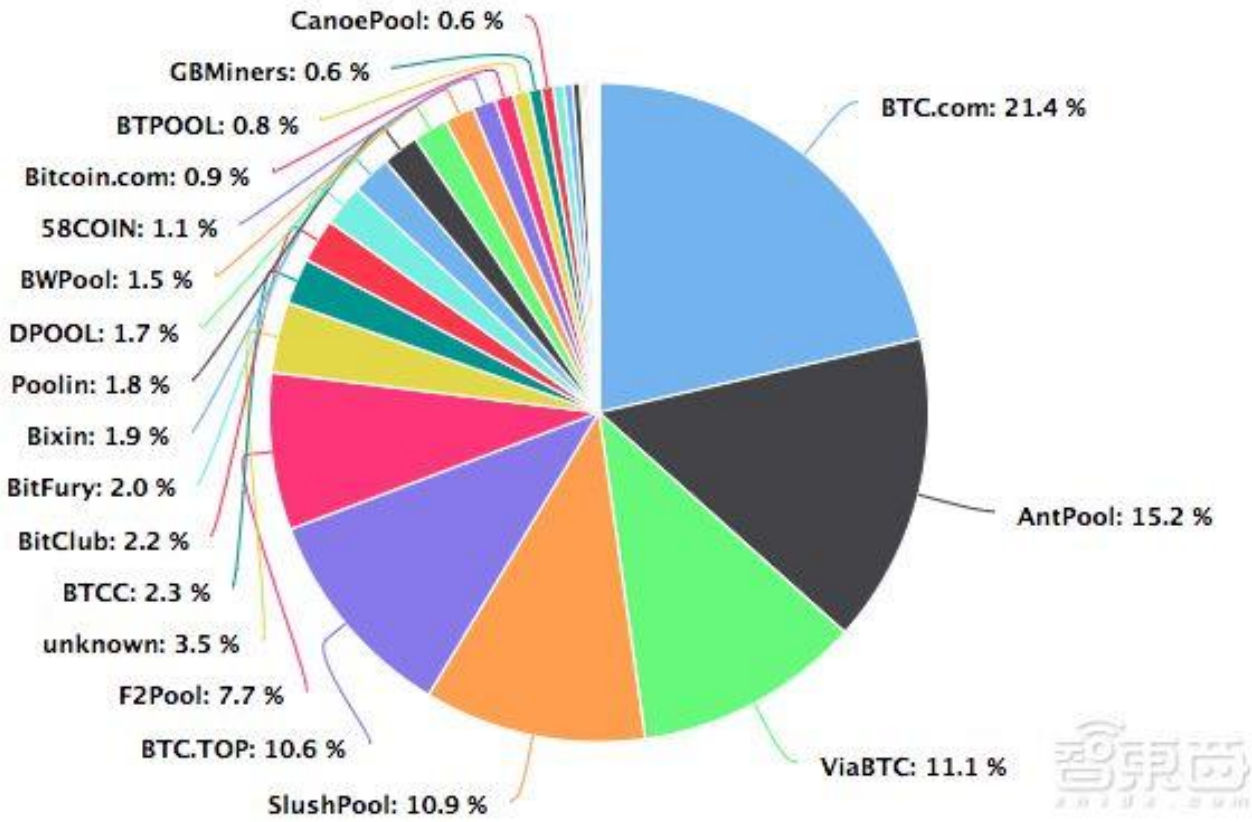
数字货币交易所

- 目前全球有超过 1.2 万家数字货币交易所，头部20家占90%市场收入
- Mt.Gox， 2010年成立于日本，早期最有名的比特币交易所，2011年被黑客攻破
- Binance 币安
- OKCoin / OKEx
- Huobi火币
- Upbit，成立于韩国

矿机

	2017年企业营业收入（包括矿机和其它收入）	2017矿机市场占有率
比特大陆 Bitmain	25亿美元	66.6%
嘉楠耘智 Canaan	13.08亿人民币	20.9%
亿邦科技	9.79亿人民币	10.9%

矿池


CanoePool: 0.6 %
GBMiners: 0.6 %
BTPOOL: 0.8 %
Bitcoin.com: 0.9 %
58COIN: 1.1 %
BWPool: 1.5 %
DPOOL: 1.7 %
Poolin: 1.8 %
Bixin: 1.9 %
BitFury: 2.0 %
BitClub: 2.2 %
BTCC: 2.3 %
unknown: 3.5 %
F2Pool: 7.7 %
BTC.TOP: 10.6 %
SlushPool: 10.9 %
ViaBTC: 11.1 %
AntPool: 15.2 %
BTC.com: 21.4 %

Factom 公证通

- 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。利用区块链技术帮助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。
- Factom是用一种去中心化的方式来收集，打包，安全保护数据，并把数据锚定到比特币的区块链上。
- 网站：https://www.factom.com/

Coinbase

- Founded in June of 2012, Coinbase is a digital currency wallet and platform where merchants and consumers can transact with new digital currencies like bitcoin, ethereum, and litecoin.
- $217M raised from world's leading investors
- 2017年1月17日，纽约金融服务部门（NYDFS）负责人宣布，已通过比特币交易平台Coinbase的牌照申请。2015年1月27日，Coinbase比特币交易所开张。
- 网站：https://www.coinbase.com/

Coinbase

Coinbase 的牌照列表

范围	类别	获取途径
地域范围	美国各州	取得50个州的转账交易牌照（Money Transmitter License）
	纽约州	取得数字货币交易所颁发的BitLicense，和取得数字托管牌照
	美国联邦	正在申请国家银行特殊牌照(Special National Bank Charter)
	全球	取得33个国家合法经营许可，以及英国和欧盟的E-Money牌照
上下游产业链	支付	自营Coinbase Commerce，并收购2家支付公司获得支付牌照
	储蓄	通过Coinbase Ventures 收购Compound公司获得储蓄经营许可
	贷款	通过Coinbase旗下关联公司投资Dharma公司获得贷款经营许可
	金融衍生品交易	通过Coinbase旗下关联公司投资dYdX公司获得衍生品交易资格
	另类资产交易	收购Venovate Marketplace公司拥有另类资产交易资格
	券商交易	收购Keystone Capital公司拥有券商交易资格的牌照
	投资顾问牌照	收购Digital Wealth公司拥有投资顾问执照

来源: 官网和网络搜集

Coinbase

Coinbase 的生态	
类别	名称
普通客户交易平台	Coinbase Consumer
专业客户交易平台	Coinbase Pro
机构客户交易平台	Coinbase Prime
数字货币存管	Coinbase Custody Trust Company
钱包	Coinbase Wallet
支付	Coinbase Commerce，Celo, Spacemesh
储蓄	Compound
指数基金	Coinbase Asset Management
金融衍生品交易	dYdX
稳定币	USDC （Co-Founder），Reserve
合规和反洗钱	Distributed Systems, Abacus
贷款	Dharma
另类资产交易平台	Venovate Marketplace
券商交易	Keystone Capital， Paradex
投资顾问牌照	Digital Wealth
比特币应用	earn.com

来源: 官网,diar.co和网络搜集

Ripple

- RippleNet,一个分布式的P2P清算网络，基于区块链技术记录所有交易活动，连接全球金融机构，支持快速低成本的全球汇款。
- XRP 瑞波币，Ripple网络中的基础货币，它作为整个Ripple网络中唯一的通用货币，可以在整个Ripple网络中流通。
- 网站：https://ripple.com/

谢谢！