Fractal Core：一个服务于通证经济的去中心化系统

Fractal 团队*

v 0.1

摘要：本文提出了一种以支持通证经济的发展为首要目标的公有链系统，该系统采用DPOS共识机制，保证系统的去中心化与效率之间的平衡。Map-Sidechain是系统的核心机制，用户可以方便的将各种类型的资产映射到Fractal主链上，也可以根据自身需求创建各类型的、异构的、甚至单节点的侧链。用户可以自行创建侧链，也可以购买“侧链服务商”的服务，以降低开发及维护成本。通证经济需要以较低的成本支持区块链领域商业模式的创新以及现有商业模式向区块链世界的迁移，这也是创立Fractal 系统的初衷。

1 引言

技术水平的进步，使得人类的经济活动和社会形态不断随之发生变化。随着互联网技术的爆炸式发展，人们对更加便捷、安全、去中心化的价值交换手段的需求催生了以比特币(Bitcoin)[1]为代表的加密货币[2, 3]热潮。

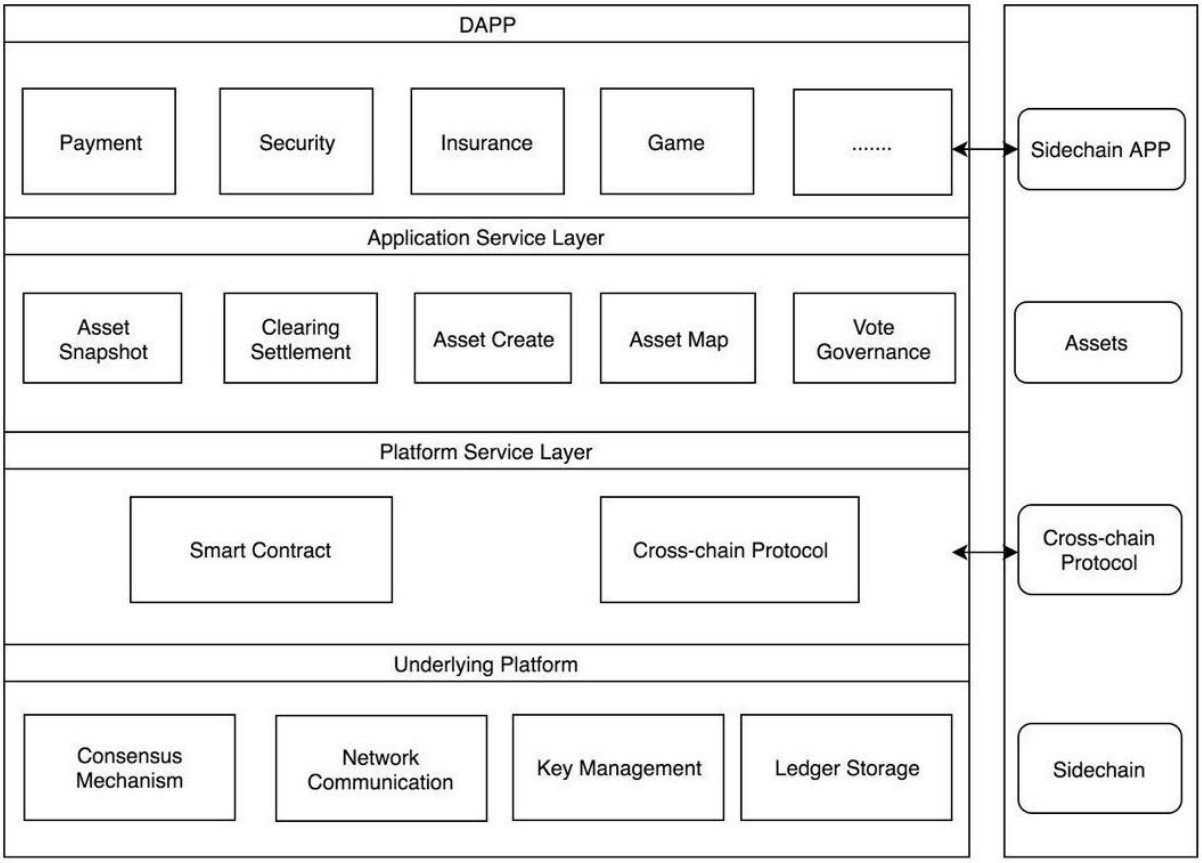
自从比特币流行以来，加密货币行业迅速发展演进，先是出现了不同种类的加密数字货币(Coin)，之后随着以太坊(Ethereum)[4]的诞生以及ICO[5]的兴起，通证(Token)开始大规模被发行及交易。通证作为“可流通的加密数字权益证明”，是区块链提升传统商业模式效率的关键[6, 7, 8]。然而，迄今为止，大多数通证经济[9]的实践仅仅止步于ICO。ICO本质上是一种融资行为，对通证经济来说，到这一步是远远不够的。证券化通证ST(Security Token)[10]正在试图解决ICO 的诸多先天不足，使数字资产真正进入主流视野。ST 有很多显著的优势，比如简化合格投资者身份认证，将不同国家的监管规则编纂进智能合约[11, 12]，从而使KYC和AML 机制自动化。随着创新的不断涌现，通证经济的发展空间不可限量。

以太坊的目标是成为去中心化应用的平台，然而无论从设计目的还是实际性能来讲，以太坊都无法承载通证经济未来的成长。尽管当前区块链行业发展迅猛百花齐放，但还没有出现一个有影响力的、以支持通证经济的发展为首要目标的底层平台。

Fractal是FCoin数字资产交易平台联合一些通证经济的坚定支持者共同发起的公链项目，将不仅仅支持FCoin自身对于通证经济的实践和探索，更以支持整个通证经济的未来发展为核心目标。Fractal Core是Fractal项目的第一个核心产品，具备一个高性能公链所需要的基础功能，包括高效的共识机制及智能合约，同时内生支持Token的发行、流通、分红、及以投票为核心的各种社

*邮箱：team@fractalproject.com

区治理功能。另外，通过灵活的映射-侧链机制，Fractal系统可以将现实世界任意类型的资产映射至Fractal并通过侧链机制实现高效的流通和多样化的治理。



Fractal Core 整体架构图

2 FToken(FT)

FToken(FT)由原FCoin Token升级而来，既是FCoin 数字资产交易平台的权益代表，也是Fractal公链生态的权益代表。FCoin Token最初通过“交易即挖矿”及“预发行解锁”的机制，完成了接近50亿FT[1]的社区化发行。如今，FT的发行阶段已经结束。尽管FT进行了品牌升级，未来也不会有新的FToken发行。

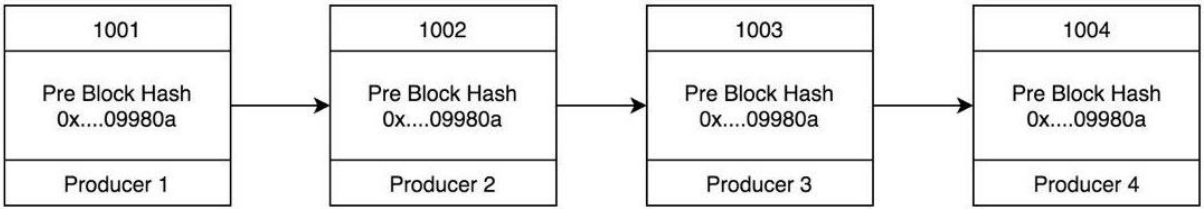
[1]具体数字参见ftoken.com

3 共识机制

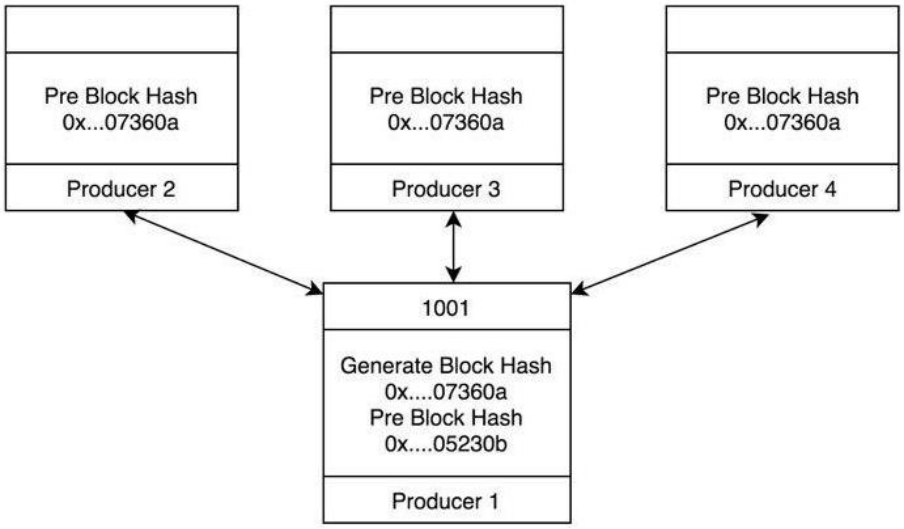
DPOS是一种借鉴了代议制的共识设计，能够做到兼顾去中心化和效率，在区块链实践中得到了广泛的使用和证明。

最初Bitshares的DPOS共识机制[13]由101个见证节点组成，见证节点是被社区选举的可信节点，任何一个持有Token 的用户都可以参与投票和竞选见证节点的过程，在每一轮投票结束后，票数最高的101个见证节点负责生产区块。选举的根本目的，是通过每个节点的投票选举出社区里对项目发展和运行最有利的用户，在项目初期，如果见证节点数量过多，可能会导致缺乏足够的投票吸引力来完成选举，因此我们初期不会选举出101个见证节点，随着系统用户的增加，逐步选举出更多的见证节点。见证节点由FT 持有者定期投票选出，FT 持有越多，投票的权利越大。

传统DPOS(基于石墨烯技术)[14]使用随机的见证节点出块顺序，出块速度为3秒，如果有6个见证节点，则需要2/3以上见证节点确认交易，交易确认时间总共需要12秒。



为了加快确认速度，我们借鉴了EOS的BFT[15]改进，允许见证节点收到新区块后立即进行确认，当收到2/3见证节点确认时，则认为区块不可推翻，能够使交易确认不可逆的时间缩短至三秒。

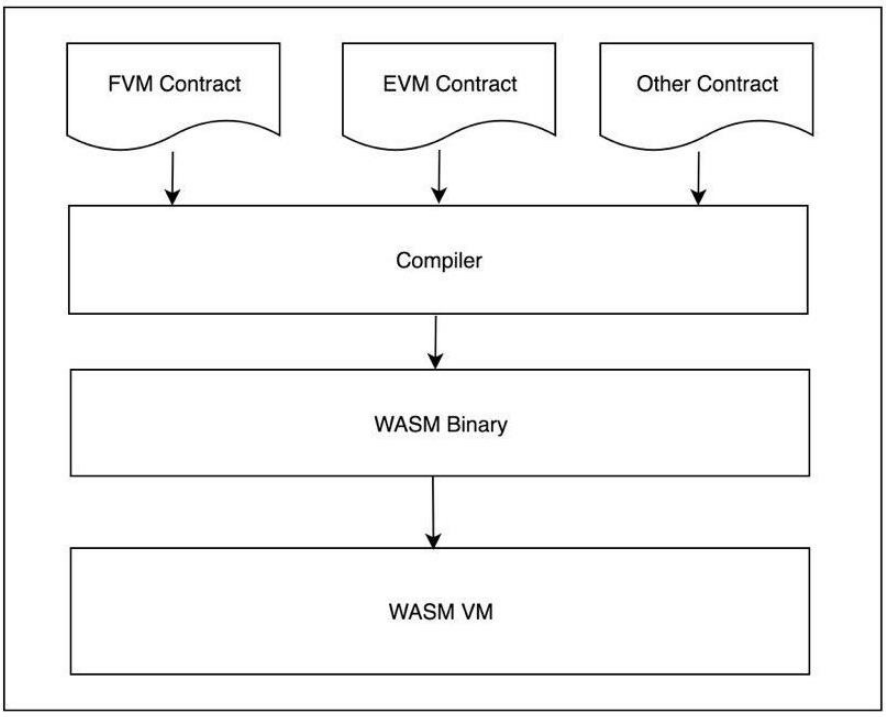


4 智能合约

Fractal智能合约虚拟机(FVM)基于WebAssembly(一种基于堆栈虚拟机的二进制指令格式，简称WASM)，可以使用C/C++，Go，Rust，Java，JavaScript等多种编程语言，便于让各种语言开发者开发智能合约应用。

WASM拥有近乎原生的执行速度，成熟的开发社区及工具箱，是目前最好的智能合约引擎底层技术之一。以太坊的下一代虚拟合约引擎EWASM也正在往此方向发展，因此EVM也可以方便的接入Fractal。

Fractal智能合约底层提供了大量API供开发者和用户调用，其中囊括了加密算法、系统、区块、数据库、账户资产、交易、消息等丰富功能，为各种应用场景中的DAPP应用打下了坚实的基础。



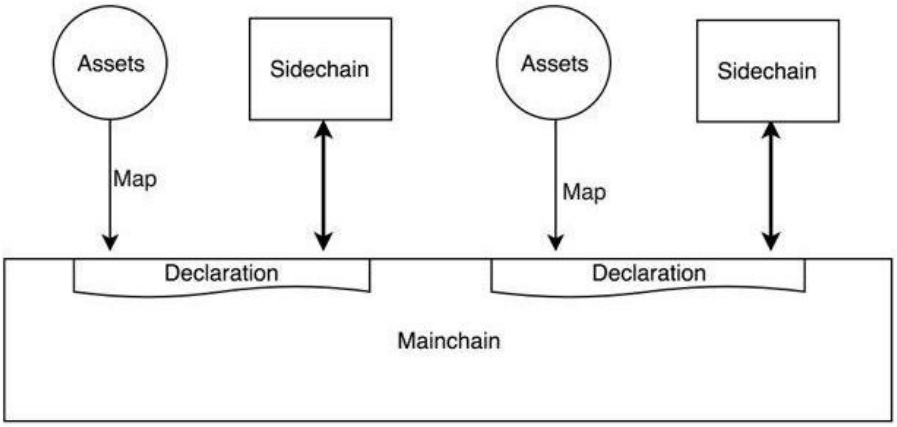
5 Map-Sidechain机制

Map-Sidechain机制的核心有两个，一是映射(Map)，二是侧链(Sidechain)。Map-Sidechain机制的运作方式为：

第一步是Map：在Fracal Core主链上创建一个类型为“声明”的特殊合约，并在该声明中完成新Token的初始发行。Map创建者可以在声明内容中附上映射资产的相关说明或证明，以提升声明的效力。

第二步是Sidechain[2] ：在Map 声明下创建侧链合约，侧链的部署及运行需在符合Fractal技术规范的前提下，由Map创建者自行完成，也可以向侧链服务商直接采购相关服务。

Map机制起的作用主要是，让Fractal系统外的资产通过映射的方式在Fractal建立权属关系并自由流通。需要注意的是，由Map的创建者自身来保障资产的真实、有效。映射机制仅起到公开登记的作用，系统不关心也不保证资产的真实性及有效性。Sidechain的作用主要是：一、获得大规模并行的能力，提升系统承载，使得Fractal生态不受制于主链的性能。二、实现自定义的、甚至为零的交易手续费，大幅降低用户的参与门槛。三、依据资产映射创建者的意愿实现定制化的功能及内部治理需求。



Map机制是实现通证经济的核心机制。Sidechain是实现Fractal生态多样化，以满足通证经济多样化需求的关键。

以某Bitcoin地址上的btc向Fractal的映射为例：

(1) 映射资产：在Fractal主链创建声明并用FT对应的私钥签署，同时将所有权证明作为声明内容的一部分，比如用该btc 地址对应的私钥签名该声明的内容。

(2) 创建侧链：在该声明下创建侧链合约，侧链的部署及交易处理，将由创建者完成(也可向侧链服务商采购资源)。

(3) 侧链可以实现一个特殊的赎回交易，允许侧链中任意地址可以通过签名实现赎回操作。在赎回交易发出后，资产映射创建者负责将Bitcoin主链上的原生资产即btc完成转移。

以映射某网站的所有权为例：

用主链FT的私钥签署声明，并将所有权证明作为声明内容的一部分，如将签名后的声明放置于网站每个页面的页尾，并附上链接。

以上举例仅仅是为了说明声明的可行性，并不规定特定的声明样式，也无法保证所有声明的证明力。不同类型的资产，需要根据资产的特性，去研究实施不同的声明方法，必要的时候还需要引入第三方机构，以提升声明的证明力。

[2]Sidechain的技术规范，请参见Fractal Core技术白皮书

6 交易手续费

目前的公链生态中，交易手续费成了一个绕不开的话题。比特币(Bitcoin)网络的交易手续费持续上涨，已经远远谈不上“接近免费”。而以太坊(Eethereum) 网络一旦交易量增大，交易手续费成本会迅速上升，给Token交易者、应用开发者创造多样性商业模式带来了很大障碍。免费的交易，是我们最需要的，然而现实情况是，即使不考虑交易打包者的利益，对于去中心化的公链来说，考虑攻击成本，免费的交易对于恶意攻击者也是缺乏防御力的。

Fractal主链的交易手续费与经典区块链手续费收取模式类似，会依据交易的大小约定基础的转发及打包手续费。另外，在交易逐渐增多并且超过一个区块的容量时，区块打包者可以选择按照手续费缴纳的多少来选择优先打包“价值”更高的交易。

主链交易手续费仅仅是Fractal网络的一部分。Fractal的亮点在于它的Map-Sidechain机制，这个机制将创造出大量的、异构的、甚至是单节点的侧链，这些侧链可以依据提供服务的性质，制定自己的手续费方案及相应的区块链架构。为了支持某些类型的商业场景，免手续费交易的机制会在侧链生态中大规模的涌现。这种情况通常是，侧链的运营方可以从其他上层的应用获得收入，而不需要依赖手续费，他们将负责承担由于免费带来的服务器压力，以及发展抵御恶意攻击的能力。

7 激励机制

由于FT已经完成了发行，不再增发，所以Fractal主链并没有“新币奖励”。见证节点的收益主要来自于：

(1) 见证节点将获得其打包交易的交易手续费的20%，而另外80%将定期分配给FT的持有者。

(2) Fractal系统鼓励见证节点竞选者成为侧链服务商。稳定的见证节点表现，是其获得客户青睐的有力背书。

8 通证权益

Token是可流通的加密数字权益证明，包含三个要素：权益、加密、流通。分红与投票功能正是Token权益的体现。

在Fractal中，FT既是代表FCoin平台权益的通证，也是代表Fractal生态权益的通证，不但可以获取FCoin交易所的手续费分红，还能参与Fractal见证节点的竞选、社区治理等活动，并获得Fractal主链80%的手续费分红。Fractal公链内生支持链上资产的发行。代表链上资产的Token可以交易、转账，支付，投票治理，也能够被销毁，既可以在主链上流通，也可以跨链流通，通过跨链协议进行资产的转移、创建和销毁。

Fractal公链的资产发行方能方便的进行分红发放。基于分红模块，发行方可以制定各种各样的策略来扩展自己的生态。甚至开展保险、借贷、众筹等业务，或创造一系列的金融衍生品。投票也是体现通证权益的核心功能，资产发行方可以制定并通过智能合约实施相关的规则，使得Token的持有者可以方便的基于投票模块参与社区治理。

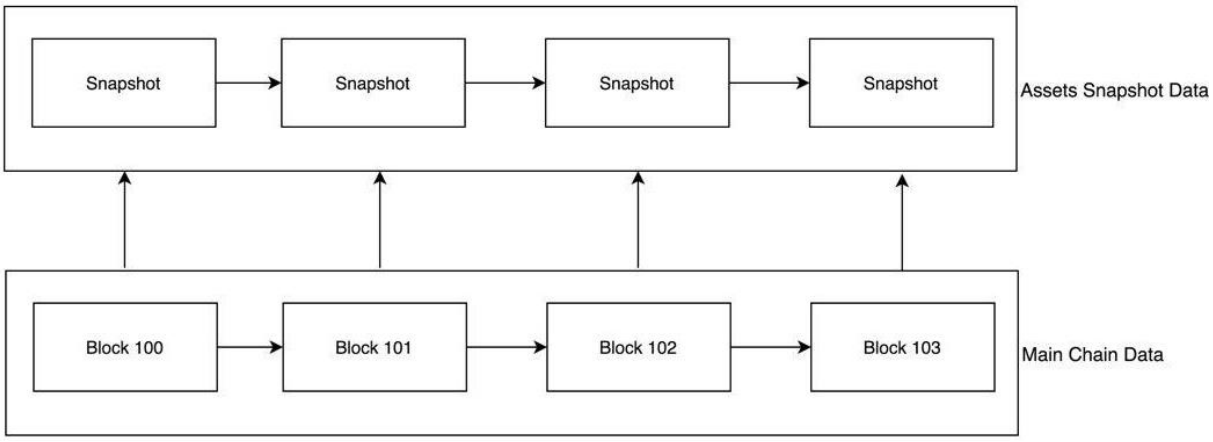
FCoin交易平台将成为Fractal的典型场景，FCoin本身的分红(参考FCoin白皮书)以及投票等社区化自治属性都将得到Fractal完整的支持。

9 快照

区块链系统本身是一套优雅的金融清算、结算系统，然而由于存储规模的限制，目前多数的区块链系统只存储了最为必要的清算结果数据，并没有存储某时刻镜像这类的冗余数据。而分红、投票等权益的行使，通常需要以某些时间点的快照数据为基准。

由此需求，Fractal设计了资产快照功能。每个区块的产生可以理解为链上的一次清算，区块的时间即是对每次清算的时间戳。因此我们可以记录链上每个区块产生时，链上所有资产的快照数据。保存快照数据有较高的成本门槛，因此快照数据只会在见证节点或是侧链供应商节点存储，并可以根据实际情况自行删除历史数据。如果资产发行方有使用快照的需求，可以向见证节点或是侧链供应商采购相关服务。

在投票期间，资产快照可以抵押成选票，用来参加社区治理。由于资产的交易是实时的，如果基于链上的实时数据投票，会产生资产复用投票的漏洞。公平起见，Fractal的投票机制基于某个时间点的快照数据，快照API也可以被合约调用。投票完成时，被使用的快照资产会被投票合约锁定，锁定期直到投票结束为止。



10 侧链服务商

从商业上理解，如果将Fractal比做“基础电信网络”，那么侧链服务商就类似“云计算”提供商。对于Fractal生态来说，侧链服务商是一个至关重要的角色。

通证经济的发展需要多样化的区块链实现形式，以满足不同商业机构的需求。这样多样化的生态，并不能被事先设计，也不是某一条公链能够单独支持的。我们引入了侧链服务商这个角色，让他们由商业利益驱动，根据市场需求，提供多样化的侧链产品，以满足不同场景、不同客户的需求。

从技术角度看，资产映射的创建者可以自己实现并维护和发展侧链，但多数情况下，这样做的成本较高。事实上，很多场景下对功能的需求是类似的，因此专业的侧链服务商能够提供更低成本、更可靠的侧链服务。

11 数字资产交易平台

数字资产交易平台是当前区块链生态的重要组成部分，也是未来通证经济的重要组成部分。然而现有的交易平台却饱受不透明、中心化严重的指责。于是，去中心化的交易平台成为了研究热点，其中以BTS[3]为代表。然而交易平台对于撮合效率、订单集中度的天然需求，使得去中心化交易平台举步维艰。

我们认为，这种交易平台去中心化的实现路径是有问题的，去中心化交易平台的实践不可能一蹴而就。有些人基于以支付为目的的公链项目，来实现去中心化交易平台，是注定要失败的，因为支付和交易所的需求大不相同。

利用Fractal的Map-Sidechain机制，我们可以非常方便的找到一条推动交易平台向透明甚至去中心化方向发展的路径。比如，我们可以将平台持有各类数字资产，全部映射为Fractal侧链，并在侧链采用并行、高效的共识机制完成交易平台内部清算系统的“上链”。这样，我们可以为交易平台的每个用户的每一种资产，对应一条Fractal侧链的一个地址，实现交易平台初步的透明化。更进一步，我们还可以尝试把交易平台的撮合系统，发展为Fractal的一个侧链。通过上述方向持续的探索实践，我们可以将数字资产交易平台从一个不透明、中心化严重的架构，向完全透明、中心化与去中心化相结合的架构转变。

12 结论

Fractal Core是一个面向应用层的区块链框架，目标是作为一整套有效的底层工具，推动通证经济的发展。首先，我们为Fractal系统引入了高效的DPOS共识协议，保障系统的去中心化与效率间的平衡。之后，我们引入对于Fractal Core最为重要的Map-Sidechain机制。通过Map，现实世界的各类型资产的拥有者，可以非常方便的通过标准化的声明机制，将资产映射到Fractal的主链上，在Map完成以后，就可以通过创建自己侧链或者购买侧链服务商的资源，构建符合自身需求的底层

[3]https://bitshares.org/

机制与经济模型。从商业角度看，引入“侧链服务商”，可以创造出大量丰富的，符合现代商业规律及互联网精神的商业模式，并以此推动通证经济的深入发展。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[2] Hileman G, Rauchs M. Global cryptocurrency benchmarking study[J]. Cambridge Centre for Alternative Finance, 2017.

[3] Narayanan A, Bonneau J, Felten E, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction[M]. Princeton University Press, 2016.

[4] Buterin V. A next-generation smart contract and decentralized application platform[J]. white paper, 2014.

[5] Conley J P. Blockchain and the economics of crypto-tokens and initial coin offerings[R]. Vanderbilt University Department of Economics, 2017.

[6] Swan M. Blockchain: Blueprint for a new economy[M]. ” O’Reilly Media, Inc.”, 2015.

[7] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. Work Pap. – 2016, 2016.

[8] Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world[M]. Penguin, 2016.

[9] Pazaitis A, De Filippi P, Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed[J]. Technological Forecasting and Social Change, 2017, 125: 105-115.

[10] Blockchain for investors. What are Security Tokens?[EB/OL]. https://blockgeeks.com/guides/security-tokens/, August, 2018.

[11] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE symposium on security and privacy (SP). IEEE, 2016: 839-858.

[12] Luu L, Chu D H, Olickel H, et al. Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 254-269.

[13] Larimer D. Delegated proof-of-stake (dpos)[J]. Bitshare whitepaper, 2014.

[14] Schuh F. Graphene Documentation[J]. 2017.

[15] EOS.IO 技术白皮书[EB/OL]. https://github.com/EOSIO/Documentation/blob/master/zh-CN/TechnicalWhitePaper.md, July, 3, 2017.