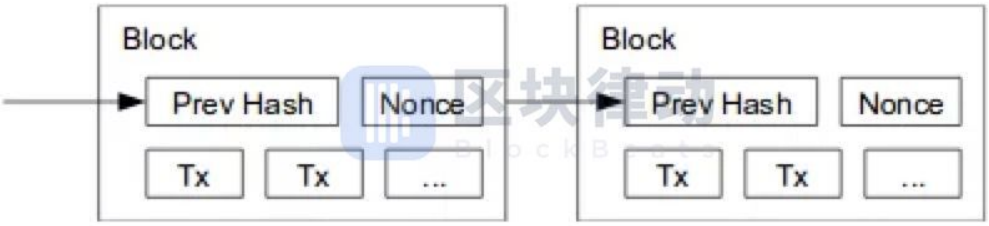
区块律动：区块链入门书单

一、这一部分都是经典的区块链开山之作，相信读完了这些你就会对区块链有了初步的了解。

1.《比特币：一个点对点的电子现金系统》：中本聪（Satoshi Nakomoto）在 2008 年发表的这篇论文开创了区块链的时代。论文中中本聪革命性地将哈希链、公钥加密、使用工作量证明进行去中心化的共识、最长链机制、挖矿激励等几个核心要素有机结合，赋予区块链巨大的能量。这篇论文可谓是所有区块链从业者的入门必读，当然了，如果你读起来吃力的话，可以在网上找一下翻译的版本。

*地址：https://bitcoin.org/bitcoin.pdf



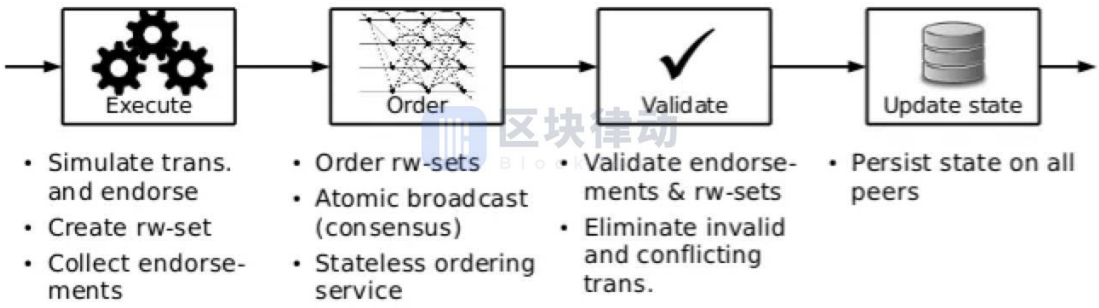
区块首尾相连就组成了区块链

2.《以太坊：下一代智能合约和去中心化应用程序平台》：准确地说，这是一本白皮书，它介绍了以太坊这个 2015 年面世的基于状态机的第二代区块链协议。以太坊拥有一个（准）图灵完备的虚拟机，它支持在区块链上进行计算，并以」燃料费用」计价，用户可以在以太坊上运行脚本（虽然这种表述有些误导性），也就是我们常说的智能合约。

*地址：https://github.com/ethereum/wiki/wiki/White-Paper

3.《Hyperledger Fabric：基于私有区块链（也叫许可区块链）的去中心化操作系统》：这是一篇 2018 年发表的同行评审文章，它介绍了当下最受欢迎的私有区块链 Hyperledger Fabric 的架构。与比特币和以太坊这些公有区块链不同，私有区块链是封闭的，只有得到许可的用户才能参与其中。这篇文章论证了将交易的执行过程与交易的验证过程分离，以及不等交易完成验证就执行交易的好处。Hyperledger Fabric 的共识机制可以支持定制化，模块化的设计。

*地址：https://arxiv.org/pdf/1801.10228.pdf



Hyperledger Fabric 架构

4.《Tendermint：关于拜占庭容错共识算法的最新进展》：这是一篇 2018 年发表的论文，文章中提出了简化的拜占庭容错（Byzantine Fault Tolernant，BFT）共识协议。这个改进的协议需要多回合的执行，每一个回合都会有一个专门的提议者。协议为便于理解和实现做出了优化，在提议者不表现出恶意行为且通信不受影响的理想情况下，它只需执行三个回合就能达成共识。同时，文章中提供了协议正确性的形式化证明。

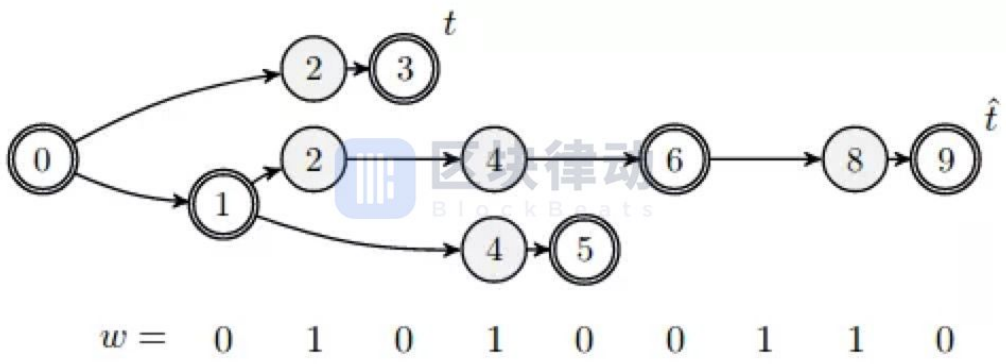
*地址：https://arxiv.org/pdf/1807.04938.pdf

5.《Swirlds 哈希图共识算法》：哈希图是一个 2016 年提出的基于有向无环图（Directed Acyclic Graph，DAG）的协议，该共识协议使用了一个基于 gossip 的算法，可以提供可证明的拜占庭容错共识。在理想没有故障的情况下，该协议可以做到无需领导，异步且快速地建立共识，与其他协议相比，它可以以最少的通信量达到整体的排序。使用到有向无环图的协议还包括 IOTA，Spectre。

*地址：https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

6.《Ouroboros：一个可证明安全的权益证明区块链协议》：这篇 2017 年发表的论文介绍并从数学的角度分析了对应于区块生成的按回合运行的同步协议 Ouroboros，该协议以分批次的方式运行。Ouroboros 专为被誉为区块链 3.0 的 Cardano 区块链开发。在每个回合的开始阶段，权益相关者组成的委员会使用安全多方计算来为该时段选择一个区块生产者的随机序列，并选取下一回合的委员会。每个用户被选择成为区块生产者的概率取决于他所投入的权益。

*地址：https://eprint.iacr.org/2016/889.pdf



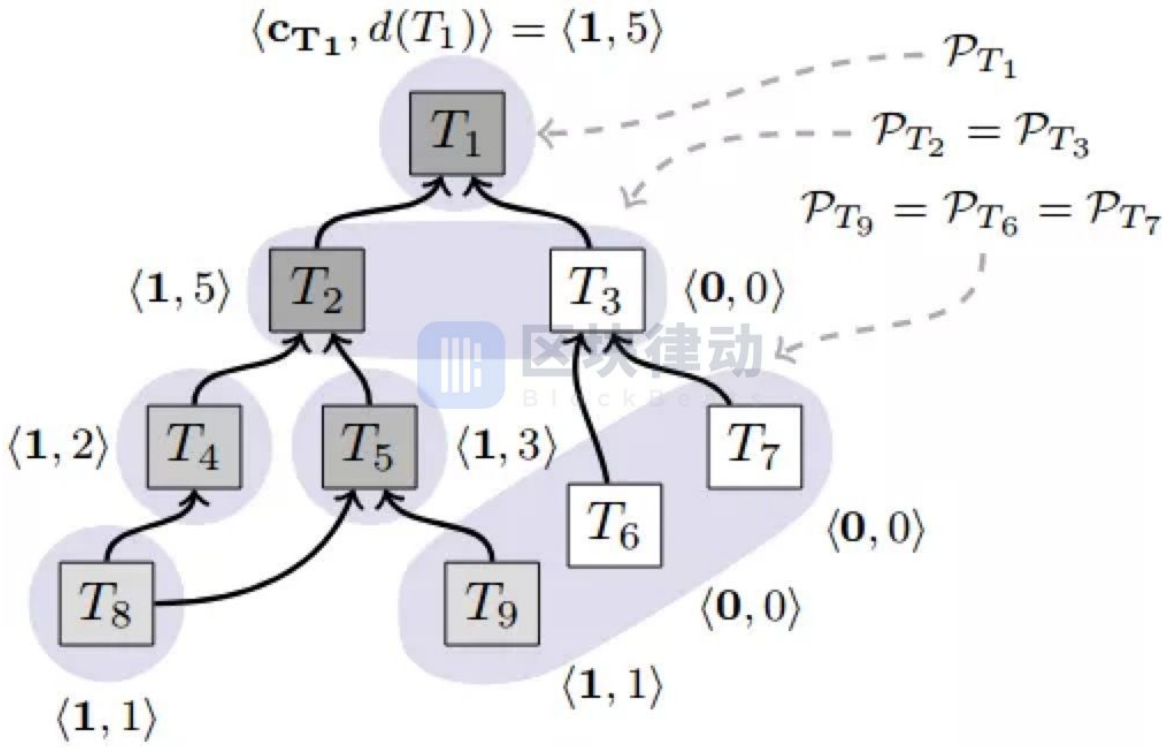
Ouroboros 上的分叉

7.《Algorand：加密货币高可拓展性拜占庭容错共识协议》： Algorand 发表于 2018 年，它提供了一种改进的拜占庭容错协议机制，即使用可验证随机函数（Verifiable Random Function, VRF）以隐秘且非交互的方式来选择一部分用户参与共识。这个协议参考了权益证明机制的思想，按照每个参与者投入的货币价值给予其相应的权重。该协议的亮点在于可扩展性，它可以支持很高的交易吞吐量并避免了工作量证明区块链在计算上付出的昂贵代价。

*地址：https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf

8.《Avalanche：一种亚稳态的新共识协议》： 这篇由匿名组织「火箭团队」撰写的论文于 2018 年发表。它提出了一种无需领导的，基于 gossip 协议，使用有向无环图的概率共识协议。与其他区块链协议相比，Avalanche 协议表现出更好的通信复杂度，因而具有更强的可扩展性。同时，论文中还论证了协议的安全性和存活能力。然而，在 Avalanche 协议的设计中考虑到了女巫攻击，但没有考虑到区块链的激励机制。不过好在，基于有向无环图的区块链协议 Perlin 在 Avalanche 共识的基础上解决了这些问题。

*地址：https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV



由 Avalanche 建造的有向无环图

9.《大零币 Zerocash：来自比特币的去中心化匿名支付》： 2014 年发表的这篇论文展示了如何使用零知识简洁的非交互式知识论证（零知识证明，zk-SNARKs）来实现去中心化的匿名交易，其中交易的发起方、接收方、交易的金额都是保密的。

*地址：http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf

10.《乌龟和野兔共识（Tortoise and Hares Consensus）：针对激励兼容，可扩展性的加密货币 Meshcash 框架》：这篇 2017 年发表的论文结合了基于工作量证明的公有区块链拜占庭容错共识协议（慢速的乌龟）与可能会出错但运行快速的共识协议（快速的野兔）。该协议在降低平均共识建立时间的同时，即使在最坏的安全状况下，它也能保证最终结果的一致性和不变性。它是一种区块的有向无环图协议。

*地址：https://eprint.iacr.org/2017/300.pdf

二、 这一部分主要是区块链各细分领域的研究成果，希望能够帮助你找到自己的兴趣点。

11.《比特币闪电网络 (Lightning Network)：可扩展的区块链链下即时支付》：这篇 2016 年发表的论文讲述了如何使用「第二层」微支付通道实现比特币的链下交易。闪电网络中的交易会被延时发送到区块链主网上，从而使更快速，可拓展性更强的比特币交易成为可能。（以太坊上也有一个类似的网络：雷电网络（Raiden））。

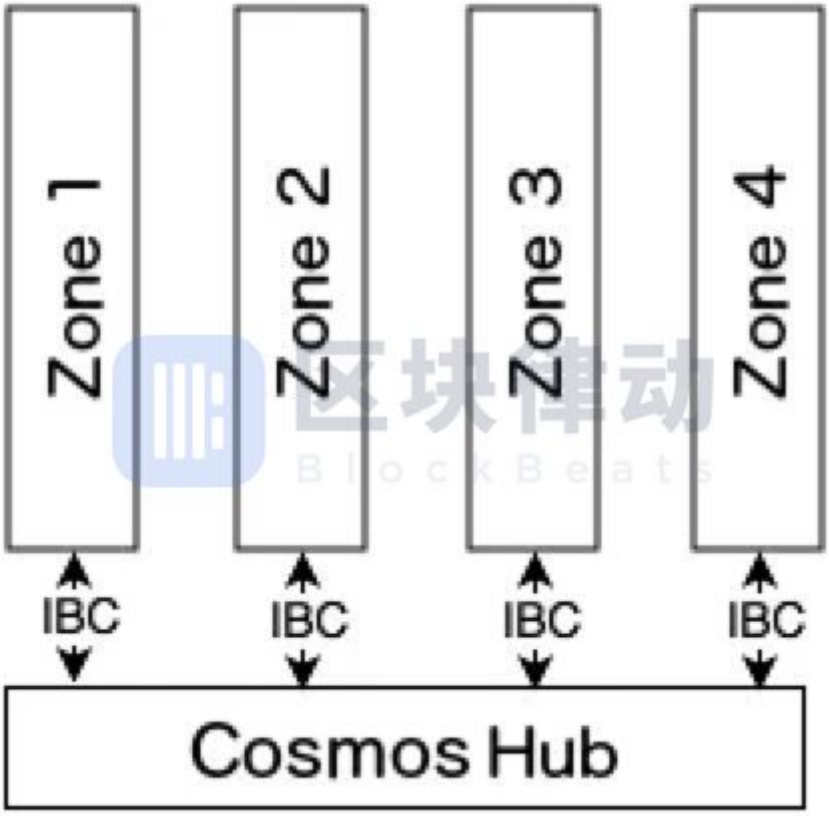
*地址：https://lightning.network/lightning-network-paper.pdf

12.《原子交换（Atomic Swaps）》： 一种在不同区块链/去中心化账本平台之间交易加密货币的解决方案。

*地址：https://en.bitcoin.it/wiki/Atomic_swap

13.《Cosmos：去中心化账本网络》：这篇论文提出使用基于 Tendermint 的集线器（hub）使不同的去中心化账本（分区）可以使用跨区块链通信（IBC）协议相互发送交易。这项工作旨在提升不同区块链平台之间的互操作性，并简化那些基于分片技术的可拓展性解决方案的部署。

*地址：https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md



集线器和分区

（**区块律动小编按：**相关阅读《Cosmos 中国区负责人 & IRISnet 创始人 Harriet Cao：未来我们不可能用一条大公链解决所有的问题》）

14.《Truebit：区块链的可扩展验证解决方案》： 这篇论文通过激励机制以及使用一种新颖的验证博弈来实现链下的计算验证，从而在以太坊上实现了一个可拓展的计算框架。

*地址：https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf

15.《Ripple 共识协议》：一种使用可信的子网络组旨在实现低延迟交易的拜占庭容错共识协议。它最多可以在（n-1）/ 5 的参与者为恶意参与者的情况下建立共识，这个数据稍微弱于传统拜占庭容错共识协议的（n-1）/ 3。目前 Ripple 共识协议已广泛应用于金融行业。 *地址：https://ripple.com/files/ripple_consensus_whitepaper.pdf

16.《Tezos：一个可以自我修正的加密账本》：这份 2014 年发表的白皮书介绍了 Tezos 以管理为中心的理念。通过使用一个基于权益证明的种子产生协议，Tezos 允许权益相关者为区块链上的修正进行投票，甚至这个投票过程也可以被修正。2017 年发表的一篇关于 Tezos 的最新论文介绍了其使用应用程序开发语言 OCaml 的设计和实现，以及其旨在促进交易的验证并提供更高的安全性且具有形式化语义（formal semantics）的智能合约开发语言 Michelson。

*地址：https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf

17.《EOS.IO》：EOS.IO 是一个于 2018 年面世的加密货币和去中心化应用程序开发平台。在共识机制方面 EOS.IO 使用了委托权益证明 (DPOS)。为了提高区块链的性能，消除用户的手续费以及加入区块链链下的治理，EOS.IO 在去中心化的程度和安全性对链下治理的依赖程度上做出了折中。

*地址：https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

18.《Bancor 协议》：这种复杂的协议可以以编程的方式计算盈亏，从而在通证的价格达到给定值时自动买入或卖出通证。

*地址：https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf

（**区块律动小编按：**Bancor 协议自出现以来，大致发展出三类应用方向，即解决长尾 Token 流动性问题，稀缺资源分配问题，及 Token 融资问题。相关阅读《BES 内部深度 - Bancor 算法及 IBO 的未来》）

19.《通证注册表（Token Curated Registries）1.1》：一个旨在创建并维持通证经济的机制，用来激励去中心化的管理。

*地址：https://medium.com/@ilovebagels/token-curated-registries-1-1-2-0-tcrs-new-theory-and-dev-updates-34c9f079f33d

20.《Augur》：一个去中心化预言机（oracle）和基于通证的预测市场平台，Augur 巧妙地设计了激励机制来促使通证持有者提供诚实和准确的报告。

*地址：https://www.augur.net/whitepaper.pdf

三、这一部分就是进阶版了，主要是一些基于区块链的解决方案和区块链的最新研究成果。

21. Blockstack：一种区块链的分层架构设计。

*地址：https://blockstack.org/whitepaper.pdf

22.Plasma 协议：智能合约的第二层可拓展性解决方案。

*地址：https://plasma.io/plasma.pdf

（**区块律动小编按：**相关阅读《如何区分侧链、Plasma 和分片？》）

23. 双重存款托管（Dual-deposit escrow）：一种在没有可信任第三方的情况下买卖数字资产的解决方案。

*地址：https://arxiv.org/abs/1806.08379

24. Holochain：一种基于代理的去中心化账本解决方案。

*地址：https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf

25. NEM：一种专为公有区块链设计的重要性证明（proof of importance）协议。

*地址：https://www.nem.io/wp-content/themes/nem/files/NEM_techRef.pdf

26. Decred：一个混合了工作量证明和权益证明的共识机制。

*地址：https://docs.decred.org/

27. 流数据支付协议（Streaming Data Payment Protocol）：一种应用层协议，主要用来进行加密货币小额支付和基于区块链的存储。

*地址：http://anrg.usc.edu/www/papers/streamingDataPaymentProtocol_2018.pdf

28. DDM：一个去中心化的实时数据市场。

*地址：http://blockchain.usc.edu/wp-content/uploads/2018/08/decentralized-data-marketplace-smart-cities.pdf

29. 海洋协议（Ocean Protocol）：一个面向人工智能的去中心化数据和服务交换协议。

*地址：https://oceanprotocol.com/tech-whitepaper.pdf

30. Mimblewimble / Grin：一个旨在提高区块链交易效率和隐私性的提案，该提案的具体实施造就了一种新的区块链协议。

*地址：https://github.com/mimblewimble/docs/wiki/A-Brief-History-of-MimbleWimble-White-Paper

（**区块律动小编按：**关于 Grin 的中文资料见《Mimblewimble 和 Grin 简介》、《Grin/Mimblewimble 致比特币持有者》，更多其他细节见 https://github.com/mimblewimble/grin/tree/master/doc）

31. Bulletproofs：一种性能更好的零知识证明机制，在那些隐私交易中很有用。

*地址：https://eprint.iacr.org/2017/1066.pdf

32. R3 Corda：一种面向金融交易场景的去中心化账本技术。

*地址：https://medium.com/p/3c00dfc66404/edit

33. Dfinity：一个旨在构建去中心化虚拟区块链计算机的协议。

*地址：https://dfinity.org/static/dfinity-consensus-0325c35128c72b42df7dd30c22c41208.pdf