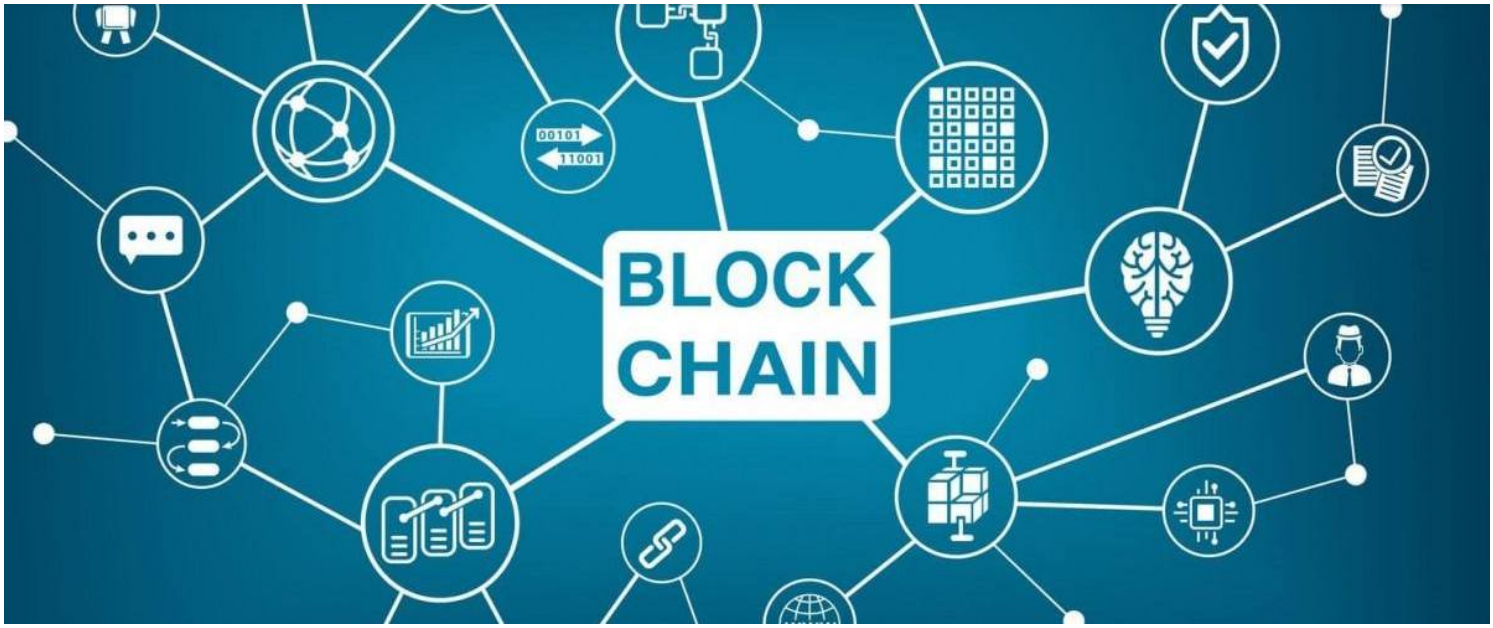

5分钟学会区块链 - 关于区块链的一切 All About Blockchain

长脚
Think different

本文攻略：解惑区块链，如何开发一个区块链项目

建议玩家等级：币圈，技术小白，学生党，初级码农

PART 1: 区块链是什么 What is Blockchain

举个栗子：杰克马、雷布斯、坡尼马、强东哥四个好朋友经常一起打麻将，每局结束都用支付宝相互结算。某天聪明的雷布斯提议以后每局结束由他计算输赢金额并告诉大家，大家各自都记在自己的账本上，每记完 1024 条就发起一次审计投票，只要有三个人同意认可这批记录，就把这批记录归档成一页并且编号留存，最后再根据这批记录结果一次性结算，于是大家都同意了这个 good idea。

让我们通过栗子来通俗的理解区块链背后那些高不可攀的名词：

- Transaction：事务。账本上的每一笔记录，都代表了一个系统 Transaction。
- Block：区块。每 1024 笔记录归档成一页，每一页都代表了一个系统 Block，每一个 Block 都记录了 1024 个 Transaction。（1024只是栗子中约定的，这个数字每个项目自由发挥）
- Broadcast：广播。每局结束后，由雷布斯向大家宣布输赢金额，大家听到以后各自记录，账本只记录四人麻将输赢有关的记录，不记录其它无关消息。一个节点收到消息会进行验证，通过验证后会进行全网广播，其它节点收到广播后进行同样的验证，并记录下来。
- Consensus：共识机制。每次审计 1024 条记录，只有至少三个人都投认可票，这批记录才会被认为有效并提交。系统每写 1024 个 Transaction 就发起一次公投，超过 2/3 投票认可后被认为有效、并提交为新的 Block（这部分会在 PART 4 详解）

续记录。系统每写 1024 个 Transaction 就 Commit 一次，Commit 成功后会产生一个系统 Block。

- Hash：哈希值，具有全局唯一性。账本每记录完一页，会计算出一个全局唯一编号，作为该页的归档编号，同时也将该页码记录在新一页的第一行。每次 Commit 会计算出一个全局唯一 Hash 值作为该 Block 签名，同时也记录在下个 Block 初始位置。
- Chain：链。账本记录的每一页都标有归档编号和上一页的归档编号，这样所有的页都按归档编号的先后顺序装订在一起形成了一个完整的账本，一直可以从当前页追溯到第一页，只要大家愿意，这个账本可以记录三生三世，没有长度限制。系统的每一个 Block 都有各自唯一的 Hash 值，同时也记录了上一个 Block 的 Hash 值，形成了一个完整有顺序的 BlockChain，这也是区块链名称的由来。
- Query：查询。四个人都能查询账本里的每一笔记录。

PART 2: 区块链革命 Blockchain Revolution

理解了区块链，再顺便理解一下为什么区块链被舆论认为是一场革命，一场去中心化的革命。

“中心化”是什么？栗子中，四个人原本相信的转账记录是来自支付宝，转账记录由支付宝统一管理，四个人都只对支付宝的转账记录达成共识。“中心化”就是所有记录都在支付宝手上，它远在云端。

“去中心化”又是什么？栗子中，自从有了雷布斯的提议以后，四个人人手一本账本，大家对转账记录的共识从原来的支付宝那里转移到了自己手上的账本，这是一本经过大家审核完全可信任的账本。“去中心化”就是所有记录都在自己的账本上，就在自己身边，那这个时候支付宝转账记录又是什么？Who cares?

再顺便理解一下区块链鼻祖，比特币。

“中心化”是什么？所有的流通货币都是由金融或者政府机构发行控制管理的，几百年来亘古不变，货币使用者都必须对发行机构的权威性达成共识，才会去兑换和使用发行的货币。

“去中心化”又是什么？比特币是虚拟货币，如果只是某某论坛里的虚拟货币那几乎不会有人相信他是可以流通且有价值的。但因为区块链的共识机制特性，栗子中的账本和现实中的比特币都具有被使用者共识的特性，每一枚比特币从诞生到消费，从一个账号转移到任意一个其他账号，这些记录都被所有参与用户共同记录并且通过审计。那么想象一下，全世界人如果都在用比特币，那么美元是什么？美联储又是谁？Who cares?

当然PO主还是希望区块链技术用于各个领域，给各个领域带来好的发展，而不是去做一些违背社会秩序和发展的项目，做了也未必能成功。

PART 3: 区块链安全吗 Blockchain Security

我们再把栗子举起来：

假设杰克马、雷布斯、坡尼马、强东哥四个好朋友都是君子，不会有人作弊，那么账本肯定是非常可靠安全的。但人与人之间的信任总是那么脆弱，某天强东哥趁大家不注意，偷偷改写了自己的账本，甚至还偷改了杰克马和坡尼马的账本，企图在审计投票时让自己的假账通过大家的共识，当然最后被杰克马和坡尼马都识破了，因为签名和字迹不一样。强东哥这种行为我们有个很洋气的名词称之为 **拜占庭（Byzantine）**。

再假设某天因为强东哥账本忘记在家里了没带，所以那天他只能打麻将不能和大家一起正常记账。

那么，区块链看似靠谱的共识机制，在这两种情况发生时是否真的安全?

情况一：一群人在做同一件事，遇到其中某些人因各种原因无法正常参与工作，但这件事情仍然可以继续进行且结果不受到任何影响，我们称之为 **非拜占庭容错**

情况二：一群人在做同一件事，遇到其中某些人非但不正常参与工作，还背叛了大家，蓄意做出有损大家利益的事情，好在大家能有效遏制坏人的破坏行为，这件事情仍然可以继续进行且结果不受到任何影响，我们称之为 **拜占庭容错（Byzantine Fault Tolerance）**

接下来，让我们通过 PART 4 来思考区块链是否真的安全。

PART 4: 区块链共识机制 Blockchain Consensus

从字面意思理解，共识机制就是大家共同认可一套安全可靠的审计规则，只有通过这套审计规则的数据大家才会一起认可并记录归档。那么这样安全又可靠的审计规则有哪些呢?

1. 拜占庭容错（Byzantine Fault Tolerance）：栗子中四人共同认同账本的规则是基于四人投票，只有三人认同就审计通过，这个规则就是基于拜占庭容错设计的。拜占庭容错规定至少有2/3的投票通过，数据才会被提交，并且可以允许少于1/3的坏蛋在故意搞破坏。至于1/3和2/3这两个数字是怎么得来的，请穿越去 拜占庭
2. 工作量证明（Proof of work）：这就是大家熟悉的比特币挖矿，通过与或运算，计算出一个满足规则的随机数，即获得本次区块记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储

这里PO主只列出了其中2种共识机制，还有好几种机制PO主也在学习中，有兴趣的玩家可以自行找度娘学习。

还是回到区块链是否安全的问题，结论是只要低于所使用共识机制的容错率，他就是安全可靠的，这个好像是废话。

那容错率高了怎么办？我们拿工作量证明来说，一个坏蛋如果要对区块进行造假，他就必须满足一个条件，每次都得比全世界所有人都先计算出满足规则的随机数，这也意味着坏蛋的计算能力要至少占据全世界计算总能力的50%，什么概念？就是全世界如果有100万台电脑在计算区块随机数（挖矿），这个坏蛋必须有其中的50万台才能至少保证有可能每次都第一个计算出新的区块随机数（挖矿）。好了，现在的你是否可以放心安心的去购买比特币了，希望机智的你可以抄到底。

PART 5: 区块链项目开发准备 Prepare for Blackchain Develop

铺垫了那么多，总算该到了PO主最擅长的撸代码部分了。PO主会先给各位有志于做区块链项目的玩家布置一些开工前的准备工作：

1. 学会GO语言：如果你是一名程序猿，不管是哪家语言的，学习GO语言对你来说简单的很，认真花三天时间包会。如果你是一名零基础，请找一名程序猿来让他学，然后告诉他你想实现什么。
2. 理解区块链：PO主只是根据个人理解把区块链通俗的做了解释，希望各位玩家还花点时间在区块链理论的海洋里自己遨游一下，如果PO主有理解错误之处，也希望各位来指正和补充，跪谢。
3. 亲自看到 GO 代码输出 Hello World，并且知道 go get 是什么命令
4. 再推荐几款IDE给各位玩家，VS Code, Atom, Sublime，总有一款适合你
5. 最后，当你都掌握了以上内容，可以开始预习 Tendermint 框架，我们将站在巨人的肩膀上进行

关于区块链的一切，PO主理解完了。关于开发的一切，我们下篇文章见。

如需合作或转载请联系本文作者，跪谢

编辑于 2018-01-21

区块链(Blockchain)

文章被以下专栏收录

5分钟从小白到极客 进入专栏

推荐阅读

用你听得懂的话聊下BlockChain

赏味不足 发表于赏味不足

Blockchain专栏

曹旭阳

区块链技术的应用？区块链原理？

区块链技术的应用？区块链就是一个去中心化的信任机制。过去区块链主要应用在比特币上，一直到最近半年，区块链已经渐渐开始有了一些其他应用，特别是在金融领域。 通俗一点说，区块链技术...

五五

基于java开源区块链Blockchain相关项目介绍

案秀云 发表于案秀云

4 条评论 切换为时间排序

写下你的评论...

克洛迪亚亚特鲁 8 个月前

下一篇文章是什么时候

赞

长脚 (作者) 回复 克洛迪亚亚特鲁 8 个月前

两三天内更新

1 查看对话

余余 7 个月前

非常棒，请收下我的赞，谢谢！

赞同 17 4 条评论 分享 收藏

有爱的大羚羊 5 个月前

任何一种比特币都局限在产生它的特定区块链中。既然有这种局限性，比特币怎么能与真实货币相提并论?

赞

赞同 17 4 条评论 分享 收藏