区块链 (http://39.106.3.150/tags/#1559363594390)

初识区块链技术

Posted by Palmer on 06-05，2019

区块链为什么要白皮书?

1.白皮书是什么

白皮书(英语：White Paper)通常指具有权威性的报告书或指导性文本，用以阐述、解决或决策。当初中本聪撰写了白皮书，就是为了赋予比特币以严肃性和权威性。但是区块链项目的白皮书和政府的官方文件又有区别，它更像一个企业的商业融资计划。在一份企业的商业融资计划中应该有的内容，区块链项目白皮书里面也都有介绍，比如，项目介绍，团队介绍，技术介绍，商业模式，融资金额等等。

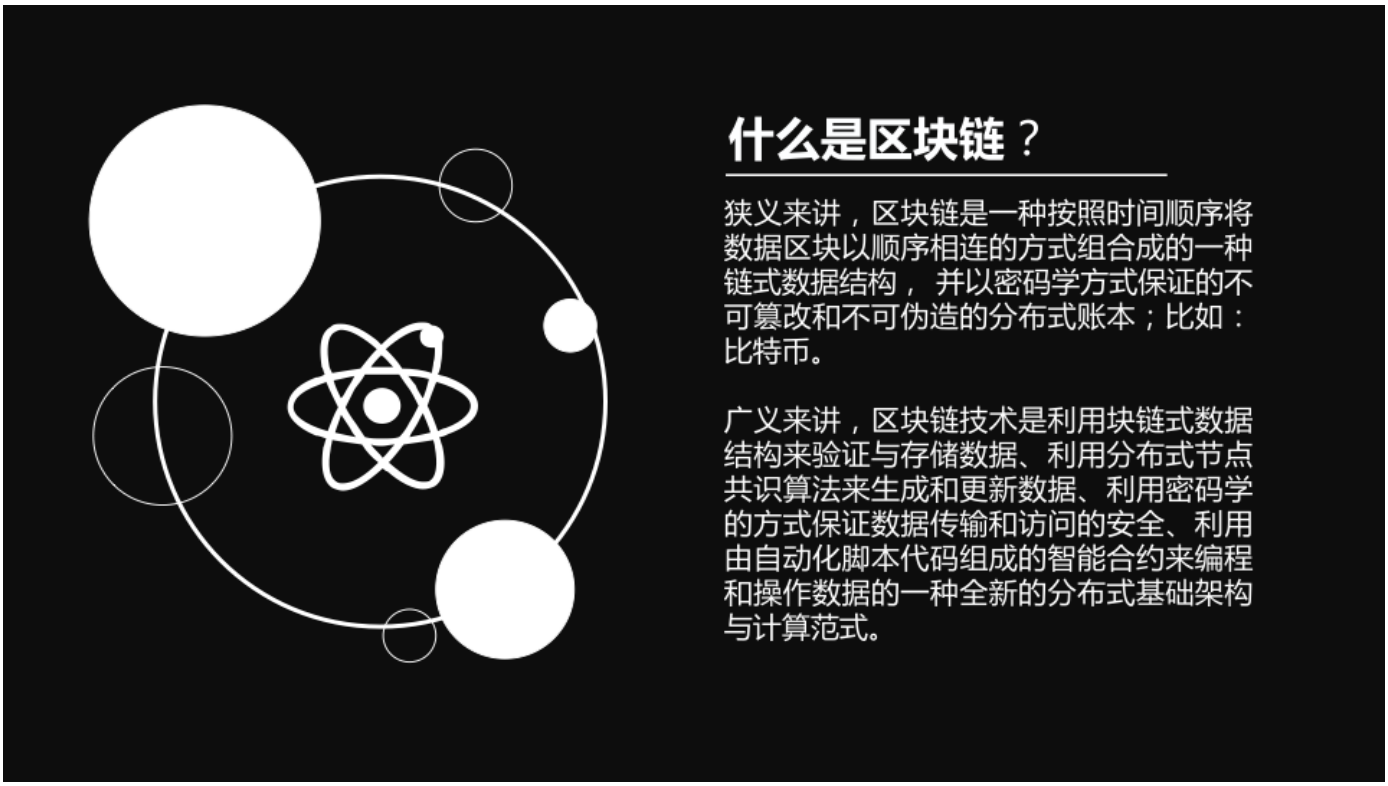
2.第一份白皮书

2008年11月1日，中本聪的《比特币——一种点对点的电子现金系统》是区块链世界的第一份白皮书，也标志着比特币的底层技术区块链诞生了。在这个白皮书中，中本聪用他严谨理智的语言描述了一种全新的数字货币系统，并清晰明确的说明了这个项目的目的是什么——解决在没有中心机构的情况下，总量恒定货币的发行和流通问题。通过这样一个白皮书，比特币成为了一个能够持续运行的项目。

3.白皮书的意义

一个区块链项目的白皮书，就展示了，这个项目，向市场展示它的商业模式，技术实力团队能力，发展愿景，等等。这是投资者判断，这个项目好坏优劣的，非常重要的依据，也是，区块链项目团队实力的，综合展现。对于投资人而言，区块链项目的白皮书能够提供关于这个项目绝大部分的信息，从而帮助他们做出有价值的投资决定。而对于项目团队来说，撰写一份区块链项目白皮书也能够为这个项目众筹资金打下非常好的基础。

区块链定义



区块链格式

区块链的四种特征

一：去中心化

二：开放性 自治性

三：交易透明 匿名交易

四：不可篡改 可追溯

区块链的几种分类

一：公有链

公开透明，世界上任何任何个体或团体都可以在公有链发送交易，且交易能够获得该区块链的有效确认。每个人可以竞争记账权

二：联盟链

半公开，群体或者组织使用的区块链。需要预先设定某几个节点为记账人，每个区块的生成由所有预选记账人共同决定，其他节点可以交易，但是没有记账权。

三：私有链

完全封闭，仅采用区块链技术进行记账，记账权不公开，且只记录内部的交易，由公司或个人独享。

区块链工作流程

一：全网广播新的数据记录

二：接收节点对收到的数据记录进行初步合法性检验，放入区块

三：全网节点执行共识算法，对区块的合法性、正确性达成共识

四：达成共识后，区块被纳入区块链统一存储

区块链hash算法

主流哈希算法：SHA-256算法。长度固定，不能解密，可以将任何长度的信息解析成固定长度的字符串。特点：

1、就算输入的的值只改变一点，输出的哈希也会有巨大的变化

2、只有完全一样的输入值才能得到完全一样的输出值

3、输入值和输出值没有规律，所以不能通过输出值算出输入值

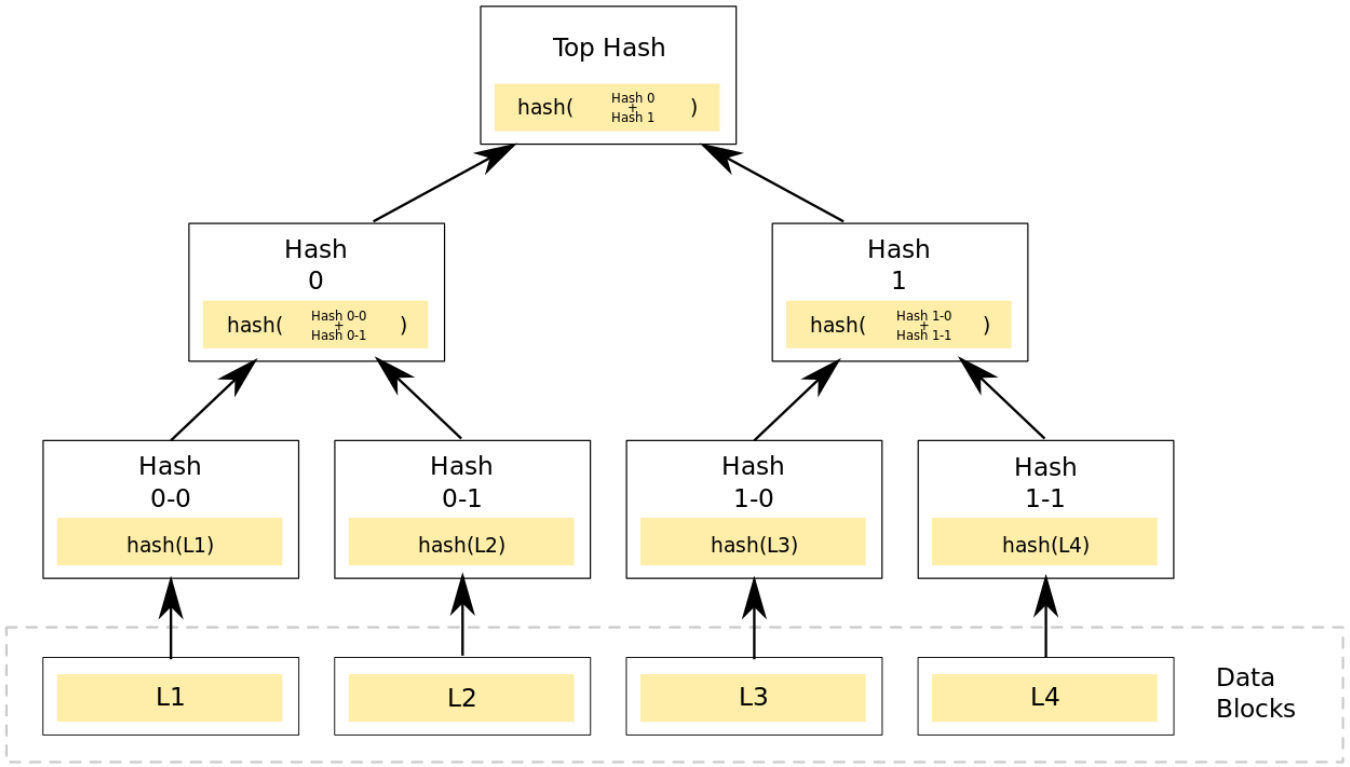
梅克尔树

Merkle Tree，通常也被称作Hash Tree，顾名思义，就是存储hash值的一棵树。Merkle树的叶子是数据块(例如，文件或者文件的集合)的hash值。非叶节点是其对应子节点串联字符串的hash。

Merkle Tree 由 Hash List演化而来：

在点对点网络中作数据传输的时候，会同时从多个机器上下载数据，而且很多机器可以认为是不稳定或者不可信的。为了校验数据的完整性，更好的办法是把大的文件分割成小的数据块（例如，把分割成2K为单位的数据块）。这样的好处是，如果小块数据在传输过程中损坏了，那么只要重新下载这一快数据就行了，不用重新下载整个文件。

怎么确定小的数据块没有损坏哪？只需要为每个数据块做Hash。BT下载的时候，在下载到真正数据之前，我们会先下载一个Hash列表。那么问题又来了，怎么确定这个Hash列表本身是正确的哪？答案是把每个小块数据的Hash值拼到一起，然后对这个长字符串在作一次Hash运算，这样就得到Hash列表的根Hash(Top Hash or Root Hash)。下载数据的时候，首先从可信的数据源得到正确的根Hash，就可以用它来校验Hash列表了，然后通过校验后的Hash列表校验数据块。

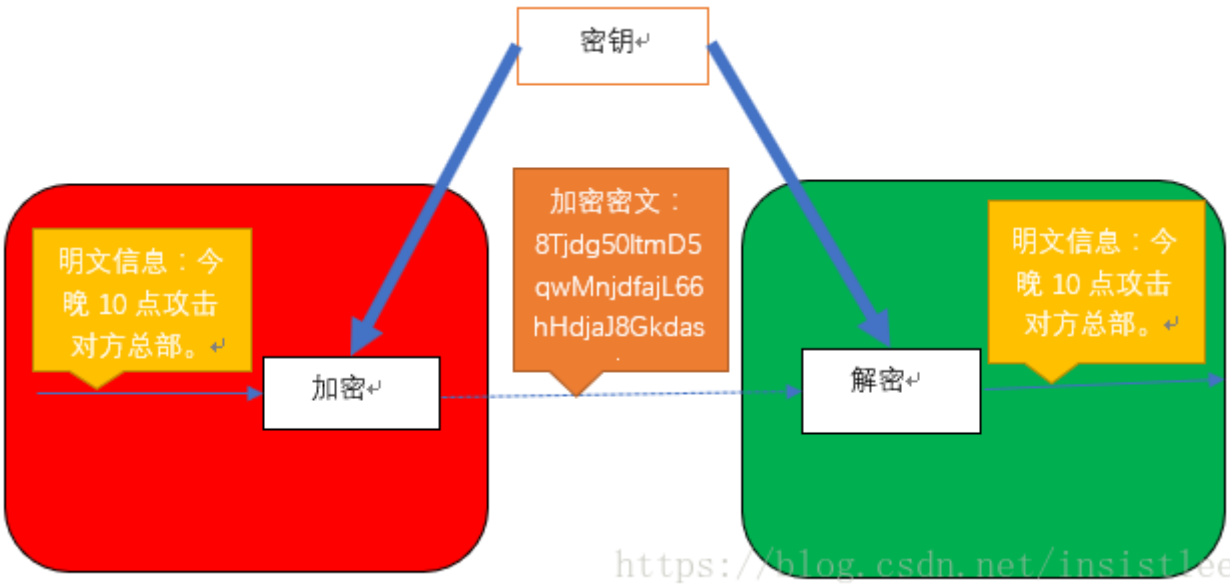


http://blog.csdn.net/wo541075754

区块链加密技术

加密简单而言就是通过一种算法将明文信息转换成密文信息，信息的的接收方能够通过密钥对密文信息进行解密获得明文信息的过程。根据加解密的密钥是否相同，算法可以分为对称加密、非对称加密和对称加密和非对称加密的结合。 **对称加密**

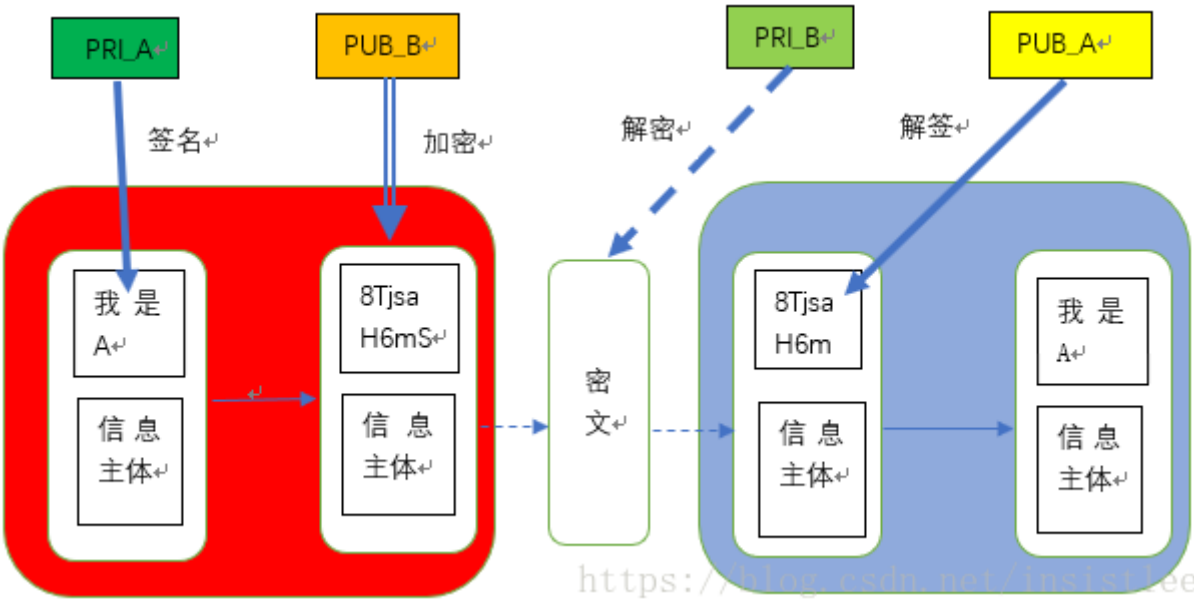
对称加密的加密解密方使用相同的秘钥，这种方式的好处在于加解密的速度快但是秘钥的安全分发比较困难，常见对称加密算法有DES,AES,...



https://blog.csdn.net/insistlee

非对称加密

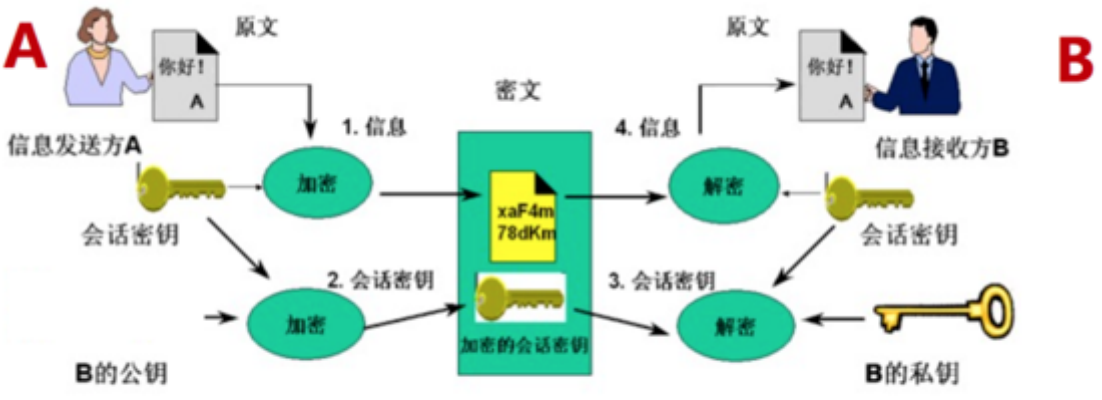
非对称加密体系也称为公钥体系，加解密时加密方拥有公钥和私钥，加密方可以将公钥发送给其他相关方，私钥严格自己保留。例如银行的颁发给个人用户的私钥就存储在个人的U盾里；非对称加密中可以通过私钥加密，他人能够使用公钥进行解密，反之亦然；非对称加密算法一般比较复杂执行时间相对对称加密较长；好处在于无秘钥分发问题。常见的其他非对称加密算法有RSA,ECC,区块链中主要使用ECC椭圆曲线算法。



https://blog.csdn.net/insistlee

对称加密与非对称加密的结合

这种方式将加密过程分为两个阶段，阶段一使用非对称加密进行秘钥的分发使得对方安全地得到对称加密的秘钥，阶段二使用对称加密对原文进行加解密。



加密例子

https://blog.csdn.net/insistlee

共识机制

区块链节点达成全网一致的机制，可以保证最新的区块被准确的添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。

POW:通过评估你的工作量来决定你获得记账权的几率，工作量越大，就有获得此次记账权利

POS：通过评估你代币的数量和持有时常来决定你获得记账权的几率。类似股票分红制度，持有股票相对较多的人获得更多的分红

DPOS:与POS原理相似，只是选了一些“人大代表”。区别在于节点选举诺干代理人，由代理人验证和记账。

区块链在财务产品中的应用

财务工作的本质是信息的获取、存储、加工与分析。区块链技术则在本质上是一种分布式的信息处理方式，和财务的核心职能直接相关。区块链可以实现与帐本完全同名，并且没有一个中心的地方记帐，进入区块链系统后，每个人都在做实时记录，备份，且不可篡改。除了全新的记账模式，区块链技术还可以帮助智能合同实现真正的落地。一个合同就是一串代码，在预先设定的时点或者目标完成的时点就自动执行合同，其间不需要任何的人为干预。

德勤在最新报告《财务2025》中指出，未来企业财务部门将演化成运营自动化的“财务工厂”，区块链则是推动财务管理“自动化”的核心技术基础之一。 区块链技术可以改进企业所有内外部财务管理流程。原料采购与付款、应收款项管理、应付款项管理、总分类账管理、企业对账甚至是公司内部工资管理，都可以用区块链技术来提升管理效率。

企业和企业在交易过程中，通过将所有交易数据上链，形成一个上下游企业可以共享的交易账本。该账本可以实时记录交易情况，上下游合作企业能够在区块链账本上查看账本的实时变动，避免出现记账错误和因账务不明而需要直接对账的情况。

另外，记账是自动化过程。企业和企业在签订交易合约时，就会在区块链上签订智能合约——设定好交易的自动流程。当交易双方在规定的时间内履行了各自的职责，区块链上记录了交易信息，便会自动触发下一步交易行动。整个交易过程实现了智能化和规范化，交易双方不需要引入第三方监控交易，就能保证交易高效规范地进行。

区块链账本不仅能够实时记录交易情况，并且可以永久保存记录且不会被轻易篡改。一旦区块链中的某一环遭到黑客攻击，参与交易的企业会立刻知晓，区块链也会自动断裂，确保区块链其他链环的数据安全。

从财务审计及监管机构的角度来看，由于区块链依赖的是自动执行的“智能合约”，而且记录在区块链的交易数据不可撤销和篡改，已经有不少审计和监管机构表示，区块链技术将节约财务审计时间，提升财务合规管理水平。

← PREVIOUS POST (HTTP://39.106.3.150/ARCHIVES/1559882472736)

NEXT POST → (HTTP://39.106.3.150/ARCHIVES/LINUX)

...

撰写评论...

上一页 下一页

FEATURED TAGS **(http://39.106.3.150/tags/)**

java 8 (http://39.106.3.150/tags/#java-8) java8 (http://39.106.3.150/tags/#java8)
redis (http://39.106.3.150/tags/#redis) 监控 (http://39.106.3.150/tags/#1561876610222)
全链路 (http://39.106.3.150/tags/#1561876610220) 容器 (http://39.106.3.150/tags/#1560852708518)
开源框架 (http://39.106.3.150/tags/#1560569459781) Spring (http://39.106.3.150/tags/#spring)
设计模式 (http://39.106.3.150/tags/#1559888728999) linux (http://39.106.3.150/tags/#linux)
SpringBoot (http://39.106.3.150/tags/#springboot) 大数据 (http://39.106.3.150/tags/#1559363598973)
区块链 (http://39.106.3.150/tags/#1559363594390) Java (http://39.106.3.150/tags/#java)

FRIENDS

(https://github.com/PowehiEdge)

Copyright © powehi
你的世界不止在眼前