Tedu.cn
达内教育

区块链基础

Unit01 区块链概述

Contents目录

01 区块链价值和意义

区块链的价值和意义

区块链是 21 世纪最具革命性的技术之一

20年后，我们就会像讨论今天的互联网一样讨论区块链

下一次产业革命区就在区块链

为什么区块链受到如此的追捧？　到底什么是区块链?

区块链的价值和意义

据世界银行的一份报告统计，每年全球跨境支付市场(国际汇款)流动资金为7000亿美金，平均手续费比例为10%，也就是有700亿美金的支出去往了外汇中介手中。而且需要数天的时间。

采用基于区块链技术的比特币系统支付，交易费几乎为零，1个小时可以确认，因为按网络传输的字节收费。历史上最大一笔交易额1.5亿美元。

所以，我们可以说：

区块链技术的出现，改变了千百年来落后的信用机制

02 区块链的起源和定义

区块链的起源定义

区块链的起源

区块链技术起源于化名为“中本聪”的学者在2008年发表的论文《比特币: 一种点对点电子现金系统》。

区块链是比特币的底层技术，比特币是区块链的第一个应用

区块链的起源定义

区块链的定义

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

--摘自《中国区块链应用技术发展白皮书》

Unit02 区块链实现原理

Contents目录

01 区块数据结构

区块数据结构

1. 一个时间段内的交易数据形成一个账单，称为区块。
2. 每个区块都包含前一个区块的hash值(账单编号)，形成一个链式结构的账本，称为区块链。
3. 这个链式结构的账本存储在多个不同的网络节点中，形成一个分布式的账本。

02 产生区块

产生区块

创建区块的源动力-挖矿

1. 处在比特币网络节点的人为什么愿意去记录交易，形成账本?

记录交易会得到奖励！记录交易打包成区块并添加到区块链的过程，称为挖矿。

挖矿的人称为矿工。矿工们在挖矿过程中会得到两种类型的奖励： 创建新区块的新币奖励， 以及区块中所含交易的交易费。

2. 既然有奖励，大家都来挖矿形成区块，以谁的为准?

记账又快有准确的人通过竞争胜出，获得区块的记账权。，有了记账权，才会得到奖励

产生区块

3 竞争胜出的条件-工作量证明

根据块数据计算获取满足条件的块Hash

03 区块传输

区块传输

1.每个节点依据综合标准对每个交易进行独立验证。保证只有有效的交易才会在网络中传播，而无效的交易将会在第一个节点处被废弃。

2. 每个节点独立的对新区块进行校验并组装进区块链。当新区块在网络中传播时，每一个节点在将它转发到其节点之前， 会进行一系列的验证。确保只有有效的区块会在网络中传播。

3.不诚实的矿工所产生的区块将被拒绝，这不但使他们失去了奖励，而且也浪费了本来可以去寻找工作量证明解的机会，因而导致其电费亏损。

04 交易的签名验证

交易的签名和验证

在数学和密码学中，有一个数字签名（digital signature）的概念，算法可以保证：

1)当数据从发送方传送到接收方时，数据不会被修改；

2)数据由某一确定的发送方创建；

3)发送方无法否认发送过数据这一事实。

为了对数据进行签名，我们需要下面两样东西：要签名的数据(发送方、接收方和数值)和私钥。

为了对一个签名进行验证，我们需要以下三样东西：被签名的数据、签名和公钥。

公钥之所以可以验证，是因为它由私钥唯一生成。

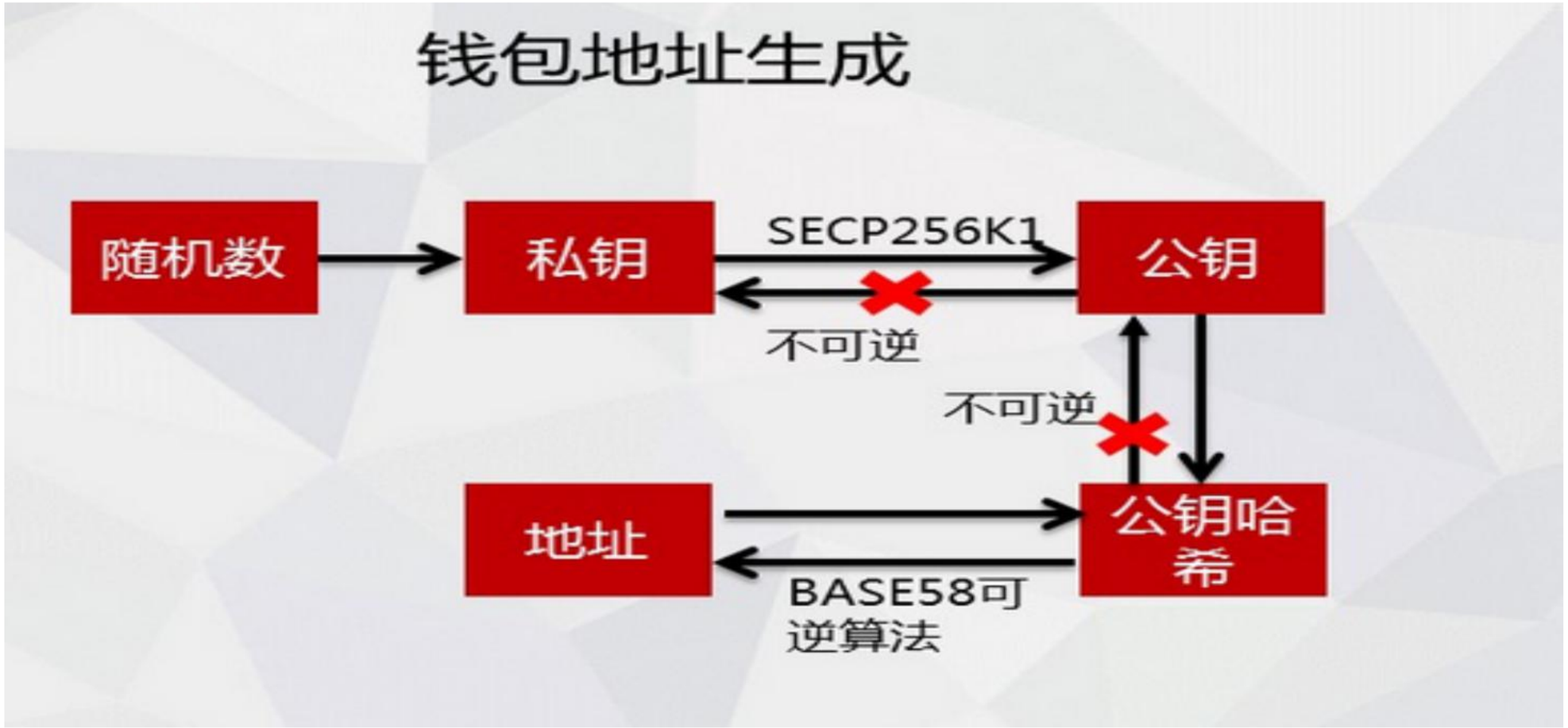
交易的签名和验证

示意图

05 比特币钱包

比特币钱包

钱包、私钥、公钥、地址之间的关系



Unit03 完整交易流程

Contents目录

01 完整交易流程

完整交易流程

1、产生交易

2、全网广播

3、被签名加密

4、全网节点验证并接收

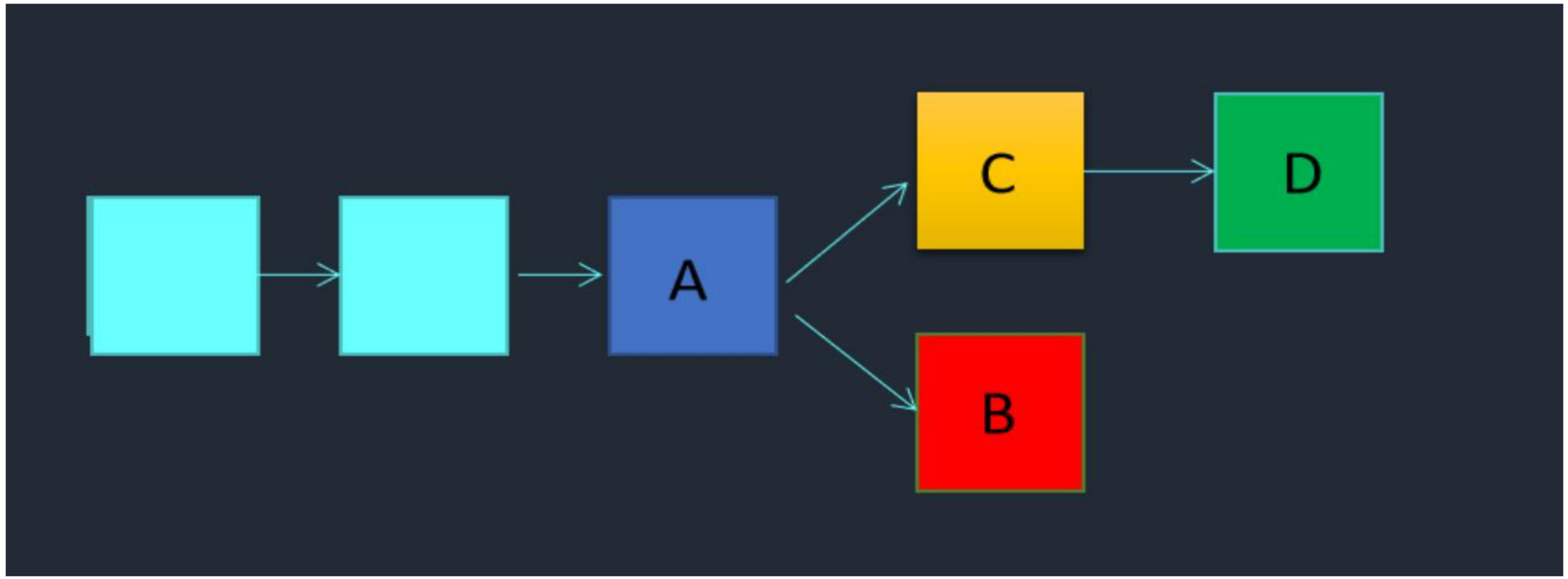
5、挖矿节点验证并添加到区块

6、被足够的后续块确认有效

02 区块链分叉

输入文字信息

从理论上来说，两个区块的分叉是有可能的，这种情况发生在因先前分叉而相互对立起来的矿工， 又几乎同时发现了两个不同区块的解。然而，这种情况发生的几率是很低的。单区块分叉每周都会发生， 而双块分叉则非常罕见。比特币将区块间隔设计为10分钟，是在更快速的交易确认和更低的分叉概率间作出的平衡。

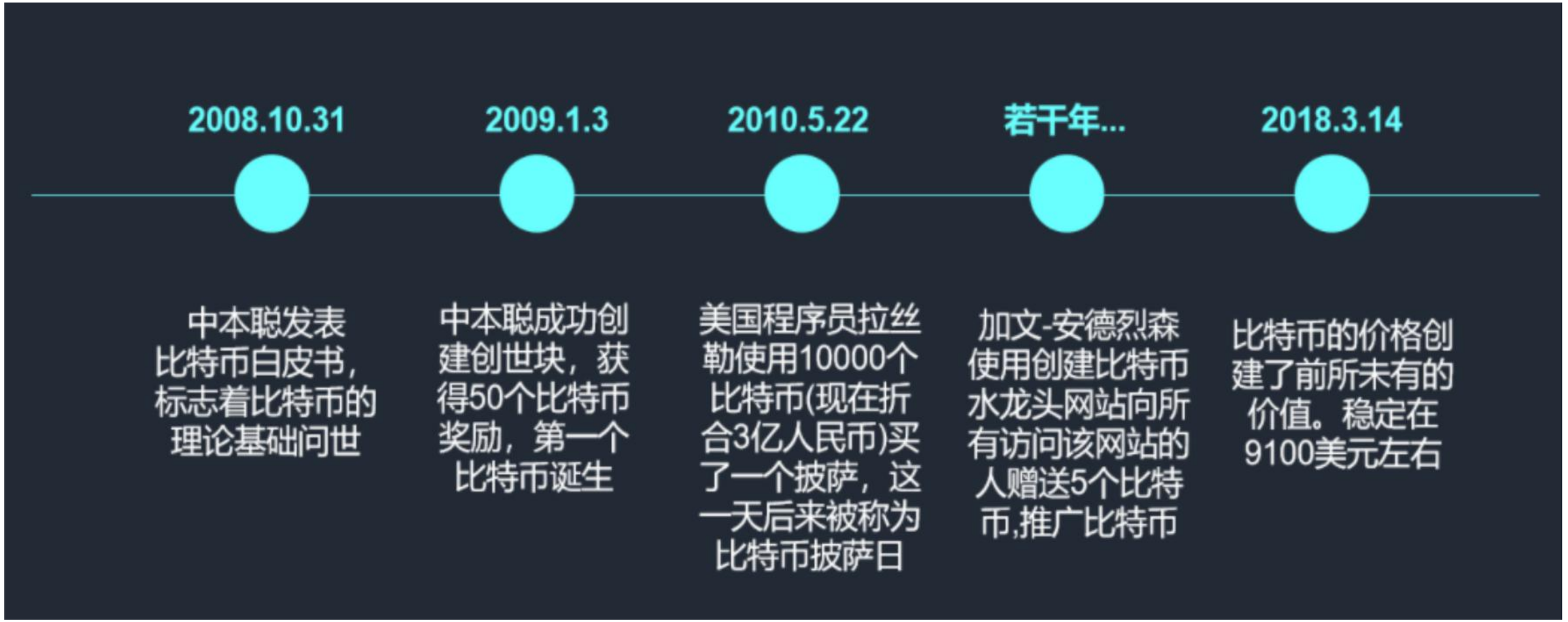


Unit04 区块链的发展

Contents目录

01 比特币的发展历程

比特币的发展历程


2008.10.31
中本聪发表比特币白皮书，标志着比特币的理论基础问世
2009.1.3
中本聪成功创建创世块，获得50个比特币奖励，第一个比特币诞生
2010.5.22
美国程序员拉丝勒使用10000个比特币(现在折合3亿人民币)买了一个披萨，这一天后来被称为比特币披萨日
若干年...
加文-安德烈森使用创建比特币水龙头网站向所有访问该网站的人赠送5个比特币,推广比特币
2018.3.14
比特币的价格创建了前所未有的价值。稳定在9100美元左右

02 区块链的发展历程

区块链的发展


各区块链时代底层技术特代表及竞争关系
区块链1.0
可编程货币
去中心化
及数字货币
比特币
莱特币
区块链2.0
可编程金融
智能合约
及金融应用
以太坊
区块链3.0
可编程社会
全领域应用
及生态搭建
潜在革新者
升维攻击
革新换代
区块链2.5创业项目代表
小蚁NEO
量子链
其他底层
平行竞品
巨型互联网公司
BAT等
投资并购
直接竞争

03 区块链的分类

区块链的分类

公有链	联盟链	私有链
任何人均可自由参加和退出	加入和退出需要联盟授权	权利完全控制在一个组织内
世界不可信	组织不可信	队友不可信

-从分类上我们再次看到区块链本质上解决的是信任问题！

04 区块链的现状和展望

区块链的现状和展望

2018年已过了大半，币圈跌跌荡荡，而链圈的人在等待凤凰涅槃，熊市专心做技术，牛市才能一展身手、冲破云霄！

在科研方面，国外更加重视核心问题的技术突破，而国内更加关注区块链应用的业务场景。

区块链上面的很多数据是链下资产在链上进行的数字化映射，如何保证链下和链上实时同步和实时相符？谁来负责上链？虽然区块链是可信的，但有时负责上链的人并不可信。

区块链的发展不能大而全，就和当前的互联网发展一样，区块链的发展也是渐进式的，初始阶段，小而美的封闭场景更实际，成功的可能性更大，无数个小而美的场景聚集起来，聚少成多，才能走向全面发展。

关注达内科技官方微信

谢谢观赏！