doi:10.3969/j.issn.1002-0802.2018.01.027

比特币区块链分叉研究 *

王 健，陈恭亮

（上海交通大学 电子信息与电气工程学院，上海 200240）

摘 要：比特币是一种新型数字货币系统。它开创性地利用密码学元素和共识机制构建了一个安全的去中心化系统。区块链是比特币的核心，它利用点对点网络通信，将交易数据备份在系统中的每一个节点，从而构建成一个巨大的分布式公共账簿。由于网络的异步性和挖矿竞争的存在，比特币区块链有发生分叉的可能。分叉会破坏节点之间数据的一致性，影响系统的安全性和可用性，是非常重要的研究对象。首先介绍比特币中区块链分叉产生的原因以及比特币系统处理分叉的方法，其次分析影响分叉产生的各种因素和比特币是如何控制分叉产生的，最后列举一些基于分叉的攻击手段、改良方案以及应用场景。

关键词：比特币；区块链；分叉；共识

中图分类号：TN918；TP309　　**文献标志码**：A　　**文章编号**：1002-0802(2018)-01-0149-07

Overview on Blockchain Fork in Bitcoin

WANG Jian, CHEN Gong-liang

(School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: Bitcoin, as a new digital currency system, pioneers the use of cryptographic elements and consensus mechanisms and builds up a secure decentralized system, while the blockchain, as the core of Bitcoin, uses peer-to-peer network communications and backs up transaction data in every node of the system, thus creating a huge distributed public book. Due to asychronousness of the network and the mining competition, the blockchain in Bitcoin may be forked. Fork would destroy the data consistency of between the nodes and affect the security and usability of the system, and thus is a very important research object. Firstly, the reason for production of blockchain's fork and the method for solving forks in bitcoin system are explored. Then, the factors that affect forks and how Bitcoin controls bifurcation are analyzed. Finally, some fork-based attacks, modified solutions and application scenarios are listed.

Key words: bitcoin; blockchain; fork; consensus

0 引 言

2008 年，Satoshi Nakamoto 发表了一篇创新性的论文[1]，提出了一个全新的货币系统——比特币。传统的货币系统通常由一个统一机构或者权威第三方作为中心节点来处理所有事务，而比特币颠覆了这种设计。它利用共识和激励机制在点对点网络中维护了一个分布式公共账簿，账簿中的数据通过密码学算法来保证安全性与合法性。

区块链是比特币中具体实现分布式账簿的数据结构。它由许多区块首尾相连而成，每一个区块都记录着系统一段时间内的交易数据。系统中的每个节点会通过网络通信将区块链数据存储到本地，在

* 收稿日期：2017-09-17；修回日期：2017-12-11　Received date:2017-09-17;Revised date:2017-12-11
基金项目：国家重点研发计划“电子货币新算法与新原理研究”（No.2017YFB0802505）
Foundation Item: National Key Research and Development Program of China "Research on new algorithms and new principles of electronic currency" (No.2017YFB0802505)

共识机制作用下，各节点的区块链数据具有高度一致性。正是由于区块链数据在系统中的各节点都有备份，任何试图篡改或是伪造交易数据的攻击都难以实现。区块链安全而又去中心化，许多研究人员认为它可以有效解决中心化系统存在的构建困难、维护成本高、效率低下以及安全存在风险等问题。然而，区块链的应用并非易事，最主要的原因是区块链本身具有非常复杂的内部设计，不恰当的修改这些设计可能会影响区块链的一些安全特性。区块链分叉的处理机制是比特币系统中众多重要设计之一，关系到整个系统的安全性和可用性，是设计和应用区块链技术时必须充分考虑的因素。本文以比特币中的区块链为具体研究对象，分析其分叉产生的原因以及影响分叉产生的各种因素，并介绍一些基于分叉的攻击手段、改良方案以及实际应用案例。

1 区块链简介

区块链是比特实现去中心化的技术核心，是比特币中最重要的概念之一。下面将主要介绍区块链的相关一些基本概念和数据结构等背景知识。

1.1 交易

在传统的交易模式中，用户往往会有一个凭证用来表示自己的账户。中心系统会将账户和用户所持有的金额数目相关联，并在发生交易后对金额进行变更和记录。这种方式的优点是便于用户管理自己的资产，查询历史流水；缺点是用户的账户和身份信息极其容易被绑定，增大了遭遇针对性攻击的可能。比特币中不再使用账户这一概念，而是通过未经使用的交易输出（Unspent Transaction Output，UTXO）的数据结构来构建交易。如图 1 所示，比特币中一笔交易大致可以分为输入、输出和交易哈希三个部分。其中，输入、输出部分都是一系列 UTXO 的集合。每一个 UTXO 都包含金额大小（Amount）、索引值（Index）、锁定脚本（Lock Script）等信息。在构建交易时，付款方首先需要提供作为交易输入部分的一些 UTXO，然后将找零和支付金额用 UTXO 的方式来构造作为输出部分。交易输入部分的 UTXO 都是从其他交易的输出中选取的，付款方必须指明输入 UTXO 所在的交易哈希值和索引值，以便证明这些 UTXO 确实存在而不是凭空创造的。为了保证交易的安全性，付款方还必须证明自己确实是这些 UTXO 的持有者，而收款方必须能够保证只有自己可以在未来使用这笔交易输出中属于自己的 UTXO。比特交易使用锁定脚本和解锁脚本来满足上述两项安全需求。这些脚本采用签名技术产生，其中锁定脚本在交易数据中被公开，而解锁脚本由用户私密保管，只有在使用 UTXO 时，用户才把解锁脚本写到交易中。比特币中脚本签名所使用的协议有 P2PKH（Pay To Public Key Hash）、P2PK（Pay To Public Key）、多重签名等。这些签名算法所使用的公钥和私钥都是按照比特币规范生成的。用户使用特定范围内的随机数作为私钥，利用 secp256k1[2] 所规定的椭圆曲线和点对私钥计算后得到对应的公钥。

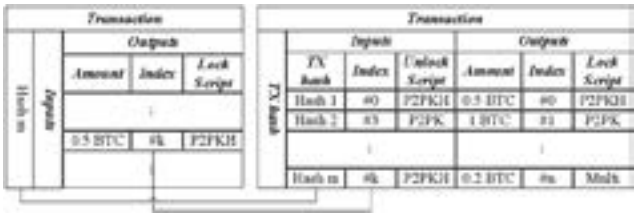

图 1 Bitcoin 交易结构

基于 UTXO 实现的方式使得比特币中的多方交易变得简单，参与方只需要提供输入 UTXO 或者创建输出 UTXO，就可以参与到同一笔交易中。另一方面，UTXO 还保证了参与交易用户的信息安全，每一个 UTXO 都会拥有不同的签名，而用户往往同时拥有多个 UTXO，攻击者几乎无法将用户身份和 UTXO 关联。但是作为代价，用户必须小心维护自己未使用的 UTXO 的解锁脚本，因为一旦解锁脚本丢失，用户就无法使用与之对应的 UTXO，里面的金额也将会永久冻结。

在比特币中，一笔交易需要等待确认才具有合法性，在介绍区块时会具体解释确认过程。交易一旦被验证并确认后，其输入部分的 UTXO 将不能再用来作为其他交易的输入，防止重复消费问题的发生。比特币中，一笔交易的输入 UTXO 金额总和往往略大于输出 UTXO 的金额总和，两者的差值被称为交易费。交易费可以使该笔交易在系统中更快地被确认。

1.2 区块

区块是比特币中用来记录和确认交易信息的数据结构。它是由比特币系统中一些称为矿工的节点产生的，而矿工构造区块的过程被称为挖矿。

比特币区块的结构如表 1 所示，主要可以分为区块头部和交易数据两大部分。在一笔交易被创建后，用户会通过点对点网络向全网广播这笔交易，而矿工们则会收集并验证这些交易数据，

并将其中合法的交易信息存储在本地交易池中。在交易数目达到一定量后，矿工开始用这些交易数据构造区块。矿工首先会确定要产生的区块应该包含哪些交易数据，并计算交易数据的 Merkle 值作为区块交易数据的校验。一般来说，矿工会尽可能多地优先选择交易费较高的交易，因为一旦矿工挖矿成功，这些交易费都将由他获得。随后，矿工会根据自己的挖矿协议以及前一个区块数据，填充区块头部的版本、前驱区块哈希值以及区块时间。随后，矿工会获取系统当前的难度值，填入 nBits 字段。这一数值是由系统设定用于调整挖矿难度的数值。一个合法区块的哈希必须符合难度值的要求，在后面介绍影响分叉产生因素时将详细解释这一数值。最后，矿工开始遍历随机数 Nonce，试图获得哈希符合当前系统难度值的区块。这一步是挖矿环节最主要的工作。比特币挖矿采用 sha256 算法作为区块的哈希算法，这一算法目前没有明显的攻击策略和漏洞，矿工们只有通过暴力搜索来寻找符合系统难度值的区块哈希值，这要求矿工具有非常强大的计算能力。而在某些难度值较大的情况下，矿工甚至不得不去调整一些交易数据的组合，以获得更大的哈希搜索范围。

表 1　比特币区块结构

字段		描述	大小 /Byte
Magic Number		魔术数，总是 0xD9B4BEF9	4
Block Size		区块的大小	4
Block Header	Version	区块版本	4
	Previous Block Hash	256 bit 前驱区块哈希值	32
	Transaction Merkle Root Hash	区块中交易 Merkle 树根的哈希值，256 bit	32
	Time	当前区块的时间	4
	nBits	难度值相关参数	4
	Nonce	随机数，挖矿遍历使用	4
Transaction Counter		交易数目	1 ~ 9
Transactions		交易数据	可变

矿工挖矿成功后，会向全网广播其构建的区块。系统中的节点会验证和确认这个区块，并将合法的区块添加到区块链的尾部，并把它继续向外传播。挖矿成功的矿工除了获得区块中所有包含的交易费外，还会额外获得一个系统设定的奖励费，用作挖矿工作的回报。奖励费是通过一个没有输入的特殊交易来实现的，这种交易也被称为 Coinbase 交易。在交易费和奖励费的激励下，矿工会不断投入计算力量争取成功挖矿，区块链也得以不断延伸，从而记录下更多的交易信息。

2　区块链分叉的产生

假设比特币的网络是同步的，且不存在多个矿工同时挖出一个合法区块的情况，那么系统中的区块会依次不断产生并添加到区块链尾部。在这种状态下，系统中的所有节点所存储的区块链数据一致。在验证一笔交易的时候，节点可以通过遍历搜索区块链的数据来确认交易中的 UTXO 是确实存在且没有被重复使用，而攻击者几乎没有方法能够修改或是伪造数据。然而，比特币是基于点对点网络建立的系统，区块的传播必然存在延时，且矿工之间的挖矿工作相互独立，存在同时挖矿成功的可能。在这种情况下，系统将不再处于理想状态。

考虑延时和竞争的情况下，假设当前区块链的长度为 l，链尾部区块为 b。在某一时刻，矿工 Alice 首先挖出了区块 b_a 并开始向全网传播 b_a。与此同时，系统中的另一位矿工 Bob 也在对长度为 l 的区块链进行挖矿，恰巧 Bob 在 b_a 传达到他之前独自挖出了一个区块 b_b。他并不知道区块 b_a 已经被挖出，于是开始向全网传播 b_b。这时网络中同时有两个区块 b_a 和 b_b 在传播，且这两个区块都指向同一个前驱区块 b。随着这两个区块被不断转发，系统中的节点将会分别以 Alice 和 Bob 为中心维护着两个长度同为 l+1 的链 $chain_a$ 和 $chain_b$，但两者尾部区块并不相同。最终，网络中在 Alice 和 Bob 中间的一些节点最终会收到来自两边试图延伸同一个区块链的不同区块。这些节点会将两个区块都追加在区块 b 处，这就是区块链的分叉。

分叉是区块链必须解决的问题，因为如果任由分叉不断延伸，那么攻击者可以分别在 $chain_a$ 和 $chain_b$ 上同时使用 b 区块以及之前区块交易中的 UTXO 进行重复消费。不仅如此，分叉状况下，只有少数中间节点能够察觉到分叉的存在，大部分不

知情的节点会继续在各自的链上挖矿。对于全网而言，节点的计算能力实际上被割裂，这将直接降低区块的产生速率，影响系统性能。比特币处理区块链分叉方法是先让节点继续在两条链上继续挖矿，一旦有一条链的高度超过了其他支链，那么这条链就会胜出成为主链，而其他支链将会被抛弃。这些被抛弃链上的区块不再有任何意义，被称为孤块。这种处理分叉的方法实际上就是比特币的共识，即所有节点都遵循的一个公开规范。共识也是去中心化系统解决竞争问题的主要方式之一。

由于分叉的存在，区块链中尾部的一些区块并不是绝对安全的，因为它们存在着被新的分支超越的可能。但是，随着后续新区块的不断追加，它们被新的分叉超越的可能性会呈指数式下降。基于这一情况，比特币中一笔交易的确认往往需要等待该交易所在区块能够有一定数量的后续区块，这导致了比特币中的交易确认并不是实时的，其过程通常需要几个区块产生的时间。

3 影响区块链分叉的因素

前面提到了分叉产生的条件是一个区块还在传播时另一个区块被发现并传播。Christian Decker 等人在研究比特币的网络[3]时，针对这一事件给出了一个关于分叉的数学模型。假设在比特币的网络中能够在每个节点设立观测点来检测区块的传播，那么当一个特定区块开始传播后，观测点会先后收到该区块。如果定义 $f(t)$ 为从区块开始传播 t 时间后接收到区块的观测点的百分比，当前系统挖出一个区块事件的概率为 P_b，那么区块传播时产生区块的概率为：

$$P_{fork\geq 1}=1-(1-P_b)^{\int_0^{\infty}(1-f(t))\mathrm{d}t} \quad (1)$$

为了方便后续描述，在 P_b 非常小的情况下，利用伯努利不等式把式（1）放大近似为：

$$P_{fork\geq 1}\approx P_b*\int_0^{\infty}(1-f(t))\mathrm{d}t \quad (2)$$

由定义可知，一定存在一正数 ε，使得 $t>\varepsilon$ 时 $f(t)$=1。所以，式（2）中的积分项大小大致取决于 ε 的大小。具体到比特币，全网节点的计算能力大小决定了 P_b 的大小，而网络延迟情况决定了 ε 的大小。所以，对于一个稳定的网络结构，式（2）中积分部分的值是相对稳定的。这表明分叉的产生和区块产生概率约成正比，也就是说区块产生速率越快，分叉越容易出现。虽然利用共识可以解决分叉问题，但其本身也是依赖于网络通信。如果区块产生的速率过快，将会导致系统中分叉的收敛速度变慢，区块链不同分叉尾部的一些区块变成孤块的可能性会大幅增加，从而严重影响系统的可用性和安全性。在区块产生的速率超过了共识交换信息所需要基本用时的极端情况下，区块链分叉甚至将无法收敛，共识机制不能起到任何作用，此时区块链就会崩塌。

Christian Decker 的模型假设中要求一个全节点的检测系统，这一点在真实环境中几乎不可能实现。一方面，技术上难以实现连接其所有的节点并向一个中心汇报数据；另一方面，系统中网络节点的规模本身也在不断变化，不可能做到实时更新检测。然而，区块速率必须被监测和控制。为了解决这一问题，比特币系统设计了一个难度算法共识，系统会在固定周期时间点不断根据当前系统状况调整挖矿的难度。区块链没有中心化系统，所以要实现这一难度调整工作必须通过共识来完成。比特币的挖矿速率控制目标是每隔 10 min 产生一个区块，在每 2 016 个区块产生后对系统的难度进行调整。其中，2 016 个区块刚好是理想速率下两周的时间所能挖得的区块数目。矿工在挖矿时会根据区块链中的区块数据自行计数来调整难度值。

比特币难度是通过计算一个 256 位的大整形数——目标值 Target 来控制挖矿的概率。前面提到每一个区块都有一个 nBits 字段，如图 2 所示 nBits 字段经过计算可以得到相对应的目标值，一个合法区块的哈希值应该小于目标值，这就意味着目标值越小，遍历随机数计算哈希时符合要求的期望就越低。比特币定义 nBits 在 0x1d00ffff 时对应最小难度，在 0x008000 时对应最大难度。每当 2 016 个区块产生后，系统中的节点会根据这些区块的产生时间 T 来调整计算目标值，改变后面区块的 nBits 字段，计算公式如下：

$$Target_{next}=\frac{T}{T_{2weeks}}*Target_{current} \quad (3)$$

其中 T_{2weeks} 是两周的时长。如果 $T<T_{2weeks}$，那么系统就会缩小当前的目标值，增大挖矿难度；反之，系统目标值将会变大，放宽挖矿的计算要求。通过难度值的调整，比特币大致保持了系统的区块产生速率稳定。截止到目前，根据 blockchain.info 网站的数据统计，比特币系统中孤块同时存在数未超过 5 个。可以说，在控制区块产生速率和分叉出现方面，比特币做得相当成功。

图 2　比特币目标值与 nBits 字段换算

虽然现阶段比特币较为稳定，但是由于控制分叉的要求，比特币中交易的确认速度十分缓慢。目前，比特币区块大小的上限是 1 MB，而每个区块所能包含的交易数目目前维持在 2 000 到 2 250。这意味着系统打包交易的速度大约是每秒3.5比交易，而确认交易的时间会更长。为此，比特币社区有人提出了增大区块链大小上限至 2 MB 的提案，以一次性包含更多的交易。事实上，区块的大小也会影响区块链的分叉。在不改变区块产生速率的前提下，区块增大会使得节点之间传播区块的传输时间线性增大，式（2）中 $f(t)$ 将会被横向拉伸，积分式的值也会线性增大。Christian Decker 通过实验也验证了这一结论，即在区块尺寸不是非常小的时候，区块大小和传输时间比基本为一个常数。因此，这样会使分叉产生的概率增大，给系统带来不稳定性。另一方面，大区块的哈希计算更加耗时，保持区块产生速率不变就意味着要降低区块难度，这会降低每一个区块的安全性。在交易保证安全性不变的要求下，交易确认需要等待的后续区块数目将会增加，这会反过来降低交易的确认速率。所以，不难看出，提升区块大小上限并不能正真解决交易确认慢的情况，且如果区块大小上限被过分放大，不排除有些矿工可能会故意构造小的区块来加快传播速度，从而使其在竞争中更有利，而这显然会严重影响挖矿秩序。鉴于种种原因，比特币的维护者们一直对于区块扩容持非常谨慎的态度，即使 2 MB 扩容提案已经确定会在未来实施，他们也非常清楚扩容并不是加快系统处理速度的根本方法。

4　区块链分叉的应用

由于网络异步性和节点的竞争，分叉在区块链中几乎不可避免，这让许多人开始研究如何利用分叉进行攻击或者是加以应用。下面将介绍常见的基于分叉的攻击手段、新的分叉处理机制 GHOST 以及比特币的软分叉和硬分叉。

4.1　区块链分叉攻击

很长一段时间，人们认为如果比特币中没有一个节点的计算能力超过 50%，那么系统就是安全的。因为只有超过全网一半的计算能力，攻击者才可以比其他所有节点更快地产生区块，从而做到利用分叉覆盖交易记录进行双重支付、阻止区块确认特定交易以及阻止其他矿工开采到有效的区块。这种攻击被称为“51% 攻击”。在这种攻击下，比特币的去中心化特性将名存实亡。

但是，比特币实际上更加脆弱。Ittay Eyal 和 Emin G ü n Sirer 在比特币研究中 [4] 提出了一种自私挖矿策略。这一策略使得攻击者只需要获得系统大约 25% 的计算能力，就可以获得超过这一比值的收益。自私挖矿策略是指矿工隐藏自己挖到的区块，在拥有一定计算优势的情况下，攻击者总能得到比系统中区块链更长的私有链。一旦攻击者持有的私有链长度超过系统中的区块链，矿工会将自己的私有链广播，人为制造分叉产生，而这条私有链最终会因为长度优势成为主链，导致大量诚实节点的计算工作就此浪费。Ayelet Sapirshtein 等人进一步研究了这一攻击策略 [5]，并指出即使在计算能力不到全网 25% 的情况下，攻击者仍然可以寻找最优的自私挖矿策略来获得不成正比的收益。

自私挖矿中单节点达到 25% 左右的计算能力比较困难，但是攻击者可以结合网络攻击降低这一要求。攻击者可以通过控制系统的大部分节点来发布自己的区块数据，从而削弱其他节点的区块链数据在全网的比重，这种攻击称为“女巫攻击”。它使得攻击者能够轻易获得系统中节点对其私有区块链的认可，从而改变区块链的数据。攻击者还可以控制其他节点的连接，割裂网络通信，使网络中计算能力的优势被放大，从而使得自私挖矿更加容易。这种攻击被称为“日蚀攻击”。Ethan Heilman 等人首先提出了具体方案 [6]，并给出了具体控制的规模和数目要求。

目前，比特币还未出现过明显的上述这些攻击，但为了防患于未然，比特币官方也在比特币挖矿程序中硬编码了“检查点” [7] 来禁止某一个区块前的任何分叉被认可。事实上，一旦这几种攻击被发现，系统将很容易定位到攻击者。比特币的维护者们不会坐视不管，他们会采取硬分叉来强制撤销攻击链，使用 IP 黑名单等手段来排除网络异常。此外，这种大范围的攻击会导致舆论发表对于比特币的负面言论，造成比特币的信誉降低和价缩水值，但这对于攻击者来说得不偿失。

4.2 GHOST 分叉协议

虽然会增大分叉产生的可能性，但是许多以区块链作为底层技术的应用还是迫切希望能够加快区块产生速率，从而提升系统的吞吐量。针这一问题，Sompolinsky 和 Zohar 提出了 GHOST（Greedy Heaviest-Observed Sub-Tree）协议[8]。GHOST 是一种新的分叉选择策略，不同于比特币中选取最大高度的支链作为主链，GHOST 选择最大子树作为主链区块选择依据。如图 3 所示，GHOST 在决定分叉区块的哪一个子区块作为主链上的区块时，会计算子树所包含的区块数目，选择其中最大值作为主链上的区块。依照这一策略，0 → 4G 构成了 GHOST 共识下的主链，而不是最长的 0 → 6B。GHOST 对于自私挖矿有着很好的限制。在高区块产生速度的情况下，诚实挖矿节点的工作不会被浪费，而是作为权重来抵抗自私挖矿。图 3 中的最长链 0 → 6B 就很有可能是来自某个自私挖矿的攻击，然而它不是主链，其区块也不会被认可。

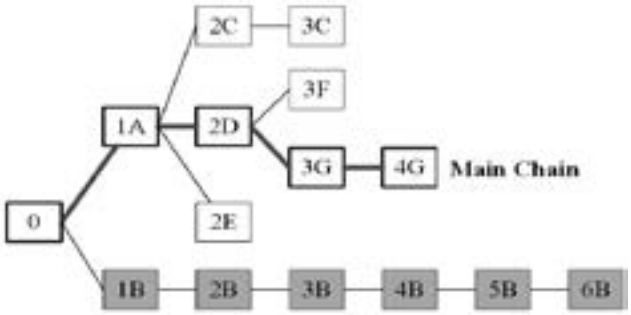

图 3 GHOST 主链选择策略

GHOST 在尽可能不影响安全性的情况下，提升了区块产生速率，从而增强了系统的处理能力。这一特性在区块链实际应用中颇具价值，著名的以太坊项目（Ethereum）就已经使用经过微小修改的 GHOST 协议作为其区块链实现的标准之一。

4.3 比特币的硬分叉与软分叉

比特币的设计决定了其升级或者修改规范是非常难以实现的。因为去中心化的特性，任何对区块结构或者是计算规范的改变，都会影响每一个节点的挖矿、验证以及历史数据的合法性。但是，分叉可以用来巧妙地实现协议或者规范升级。比特币有两种分叉升级策略：硬分叉和软分叉。

硬分叉升级有一个特点，即旧的区块按照新规范仍然能被验证通过，但新的区块不能被旧的规范所认可。所以，硬分叉在实施前会事先调查新规范的接受程度，当多数节点同意升级规范后，新规范就被正式实施。硬分叉初期，系统将会产生大量按照新规范产生的区块，而未升级的节点无法验证通过这些区块而舍弃它们。由于不同的共识，硬分叉会使未升级节点与升级节点分别在旧区块链上和新的分支上继续挖矿。但是，由于升级节点占多数，未升级矿工也会逐渐升级，新的分支最终将会替代旧链，升级过程得以实现。硬分叉的实施关键取决于大部分计算能力是否支持升级方案。截止到目前，比特币还未进行过任何的正式硬分叉升级，而正在准备进行的 SegWit2x 将会是比特币第一次正式硬分叉（SegWit2x 是将区块大小上限扩大为 2 MB 的方案）。

软分叉不是真正意义上的分叉，而是一种双向兼容的规范设计。软分叉要求新规范下的区块能够被未升级节点认可，而升级节点同样也能够认可按照旧规范产生的区块。这种升级不会造成实际分叉，是一种非常平稳的方法，适用于细微的规范和协议修改。2012 年，比特币通过软分叉实现了 BIP（Bitcoin Improvement Proposal）16[9] 中添加 P2SH 锁定脚本签名方案的升级。软分叉对设计有着相当高的要求，在对协议或者规范进行破坏性修改时，软分叉的实现会非常困难，甚至不能胜任。而一旦软分叉的实现过于复杂，其实现过程中出现漏洞的可能性也会增大。

综上所述，比特币的这两种分叉升级策略各有优缺点，所以升级时需要按照实际情况选择使用。

5 结 语

本文主要综述比特币中区块链的分叉现象，分析分叉的成因和影响因素，介绍相关的攻击手段、改良方案和应用场景。可以看到，区块链的分叉是非常复杂的现象，它的产生特性是由区块链的许多特性决定的，而理解分叉对于设计和应用区块链技术有着非常重要的作用。本文的许多概念和思想仍然适用与其他基于区块链的系统，对于区块链技术的理论研究有着一定的借鉴和参考意义。

参考文献：

[1] Nakamoto S.Bitcoin:A Peer-to-peer Electronic Cash System[EB/OL].(2008-10-31)[2017-08-25].https://bitcoin.org/bitcoin.pdf.

[2] SEC S.2:Recommended Elliptic Curve Domain Parameters[S].Standards for Efficient Cryptography Group,Certicom Corp,2000.

[3] Decker C,Wattenhofer R.Information Propagation in the

Bitcoin Network[C].Peer-to-Peer Computing(P2P),2013 IEEE Thirteenth International Conference on,2013:1-10.
[4] Eyal,Ittay,Emin G S.Majority is not Enough:Bitcoin Mining is Vulnerable[C].International Conference on Financial Cryptography and Data Security,2014.
[5] Sapirshtein,Ayelet,Yonatan S,et al.Optimal Selfish Mining Strategies in Bitcoin[C].International Conference on Financial Cryptography and Data Security,2016.
[6] Heilman E,Kendler A,Zohar A,et al.Eclipse Attacks on Bitcoin's Peer-to-Peer Network[C].USENIX Security Symposium,2015:129-144.
[7] Bitcoin Wiki Contributors.Checkpoint Lockin [G/OL].(2014-07-08)[2017-08-25].https://en.bitcoin.it/w/index.php?title=Checkpoint_Lockin&oldid=47965.
[8] Sompolinsky Y,Zohar A.Secure High-rate Transaction Processing in Bitcoin[C].International Conference on Financial Cryptography and Data Security,2015:507-527.
[9] Bitcoin Wiki Contributors.BIP 0016[G/OL].(2015-12-29)[2017-08-25].https://en.bitcoin.it/w/index.php?title=BIP_0016&oldid=59730.

作者简介：

王　健（1993—），男，硕士，主要研究方向为网络安全；

陈恭亮（1961—），男，博士，教授，主要研究方向为应用密码学、信息安全。