区块链技术和应用场景探究

赵龙飞(济宁市兖州区第一中学,山东省 济宁市 272199)

【摘 要】区块链技术是基于共识机制算法由中本聪提出并初步应用于虚拟货币发行中的计算机技术的新型应用模式。区块链本身并不神秘,其本质就是储存交易纪录的账本,但它所具有的不可篡改性,不可伪造性正成为其扩大应用范围而不仅仅局限于以比特币为代表的虚拟货币的优势特点。块链技术已经趋于成熟。中本聪通过区块链技术开发出比特币并风靡全球的成功案例确实极大地催发了区块链市场的活力,而区块链技术的内核也越来越多的被应用与电子账户,交易账本以及游戏开发中。电子货币在当下市场中以比特币,莱特币狗币等为主,虽然货币价格浮动较大但整体成良性发展趋势。区块链仅仅用于虚拟货币发行是对于其潜在价值的巨大浪费,所以我针对现今区块链技术中社会服务价值的缺失进行了研究。我通过查找资料,动手实践,尝试区块链技术服务等方式已经取得了一定的成果。区块链技术可用于交易公证,电子签到,成绩处理,诚信系统架构,金融等方面。在这些方面进行应用可以弥补信息诈骗,“老赖”横生却难以处理的不足对于社会稳定有着巨大意义。

【关键词】区块链;电子货币;区块链应用

【中图分类号】TP311.13 【文献标识码】A 【文章编号】1006-4222(2019)04-0298-02

1 导 论

当下的电子货币以比特币,莱特币为主,其他的诸如狗币(使用的是 scrypt 算法而不是 hash 算法)等小型货币百花齐放。但是从其监管和保值这两方面来看,还有待完善。虚拟货币的最大优势就是交易便捷且安全性极高,随着信息技术不断普及受众也在增多,但是它的价值却难以度量和保证,完全凭借市场认可和消费者的信赖。一旦出现资产大鳄抛售货币就会造成市场崩溃,价值得不到公证也就一文不值。

电子货币的技术基础——区块链,本身是一个分布式账本。通过把交易纪录与数据分散地存储在一个个区块中,实现了数据的分布式记录。

交易,在比特币等电子货币中主要依靠输入和输出数据来实现,当你支出一笔钱的时候,首先在交易单中就要描述清楚你要支出的钱的收入来源,然后在支出项中,指明要支出的金额,以及通过脚本的形式写明接收者的公钥,然后用自己的私钥签名认可该笔交易,最后将交易单广播到网络。

区块链技术的 hash 算法以及 scrypt 算法本身的性质赋予了区块链交易的不可篡改性。而区块链技术本身 P2P 公证机制保证了交易不可否认。智能合约机制也就是建立在这一基础上的一种代替传统合约新机制。智能合约是基于软件的,软件主要建立在比特位之上。公共的区块链往往是自动化的、全球的、无情的,这也就提高了合约的可信度以及公正性。

区块链的发展历程指明了它的发展方向,毫无疑问它会成为全新的金融工具以及信任体系中的关键一环。

目前国内研究最多的就是保值问题和核心算法的漏洞问题。

学术界已经做了大量的工作也取得了很大的成就,发现了 hashmap 的冲突问题,实现了 hash 函数的大量开发。

基于区块链技术的公司约 42%“区块链”公司是最近一年注册的,主要集中在深圳和广州市。据国家企业信用信息公示系统数据库显示,当前公司名字中含有“区块链”关键词的公司共有 1608 家其中具有代表性的又有趣链科技,星云 app,百度等以上研究都极具前瞻性,但是投入极大也难以盈利,泡沫终究会破灭,人们的热度也会消减。区块链需要换发新的活力才能长久的生存下去。

本文的工作将从区块链技术的简单实现和原理入手深入到其应用范畴,就是为了探究区块链技术更具意义的发展前景并为其注入新的活力。

2 区块链技术和简单实现

2.1 区块链的原理

加密算法:以 hash 算法为主其余的椭圆曲线等算法为辅主要应用于公钥私钥设置和电子签名。

签名算法:通过 hash 函数等方法定义一段不可复制,不可改动的电子信息密码,通过私钥解密后验证身份。

hash 函数:简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数,具有不可逆性的特点。

交易系统:交易系统由梅克尔树(merkletree),交易池,UTXO 池组成其中的梅克尔树是由 hash 函数组成的整个系统的框架它的树根就是创世区块,其中的各个函数的输出值都与上一个有关是交易在数值上的映射;易池是储存交易并管理交易的一个部分,所有的交易都在其中接受或等待处理;UTXO 池是储存输出的货币并保留等待处理的输入货币,所有交易都通过 UTXO 池发送货币,每个人名下所拥有的 UTXO 都储存在对应的账本也就是 UTXO 池中。一个用户的比特币余额,是钱包扫描区块链,并聚合所有属于该用户的 UTXO 来计算该用户的余额,本质上钱包里的比特币余额,是你名下所有 UTXO 的合集。

输入和输出是区块链运作交易的灵魂,输入就是将一笔 UTXO 放进一个交易中,输出就是将一个交易中的 UTXO 放进自己的账户也就是 UTXO 池中。

UTXO:比特币的基本单位是未经使用的一个交易输出,简称 UTXO 或未花费交易输出。说简单点,就是你能使用比特币的一个“账本”,有了 UTXO 这个“账本”,也可以说是使用权,你才能花费比特币。比特币的基本单位是未经使用的一个

能有机会通过实验获得数据,进一步调整计时电路,以在快速动作和准确动作之间取得更好的平衡。

参考文献

[1]朱亚薇.锂离子电池过充安全性的研究[D].厦门大学,2006.
[2]金 里.锂离子电池及其保护电路[J].电子产品世界,2000,5:14-15.
[3]田中俊.用于锂电池的保护芯片[J].电源技术,2009,33(10):887-888.
[4]邱关源,罗先觉.电路(第五版).高等教育出版社,2011,5.
[5]阎 石.数字电子技术基础(第五版).高等教育出版社,2006,10.

收稿日期:2019-3-15

交易输出,简称 UTXO 或未花费交易输出。说简单点,就是你能使用比特币的一个“账本”,有了 UTXO 这个“账本”,也可以说是使用权,你才能花费比特币。

区块链:由创世区块所带领的一条由区块组成的系统,其中的所有区块中的函数输出值息息相关。

主次链冲突:在区块链的生成中常常会出现两条链几乎同时被挖出的情况此时就需要通过对两条链进行长度比较来进行取舍。

2.2 区块链的实现

区块链程序主要由若干模组成,分别是区块模块、区块链模块、交易模块、加密模块、挖矿模块和同步模块,下边分别介绍这几个模块:

(1)区块模块:这个模块主要负责将交易组织在区块中,并记录相关的哈希信息,查找某一笔交易,验证交易和区块的合法性等。

(2)区块链模块:主要负责区块的链接、查找区块、验证区块链合法性,插入和删除区块以及主次链冲突解决等。

(3)交易模块:主要负责交易行为和验证。

(4)加密模块:主要负责相关信息的加密,基于公钥密码的签名机制以,用以验证区块链合法性的哈希算法等。

(5)挖矿模块:主要负责组合交易和改变 nonce 来产生新的区块,并负责调整挖矿难度。

(6)同步模块:负责在自己的网络邻居之间同步区块链的信息。

3 应用场景探究

3.1 金融方向

(1)应用于签订合同合约保证每一次交易的不可篡改和否认,把整个合约通过区块链的形式储存在区块中并输出一个 hash 值随后进行的任何改动都会反应在这一 hash 值上。

(2)应用于资产证券化,把个人的资产统计出来通过区块链把它定义为 UTXO 保证产权以及防止资产转移。

(3)应用于跨境支付,不仅可以减少手续费,还可以避免一定的汇率计算实现公信的交易,还可以解决一般支付方式到账慢的问题。

区块链在金融方面已经应用在了虚拟货币发行这一方面,比特币就是一个很好的例子,央行也已经着手于跨境支付开发中了,总体上看在金融领域区块链技术得到了充分的肯定和利用。

3.2 社会方向

(1)应用于智能的运输服务,通过区块链和智能合约应用,发布到互联网,利用大量闲置的机器计算能力实现车辆和乘客的智能匹配,去掉平台商,将平台商的高额利润返还给乘客和司机。

(2)应用于诚信系统建设通过区块链建设将每个人的交易记录,借贷记录保存,个人信息记录后现时经常上新闻的遗产争夺,借钱不还,证明我爸是我爸这些问题都将不存在。

(3)造假和盗版问题,通过区块链技术可以把你所授权的技术很好的保护起来,而在想要剽窃就几乎不可能,但是进行更改的难度也很大。

(4)应用于人工智能管理通过区块链把每个机器人或只能设备变成区块,统一调控统一设置保证其稳定安全的运行。

区块链在社会方面的应用几乎是空白,平台商为保全利益不愿区块链技术介入,一旦诚信系统建立公证处就失去了意义,所以其应用还有待磋商。但是它的前景毋庸置疑,所能带来的便利也是显而易见的,未来必将大有作为。

3.3 生活细节

(1)应用于课堂签到工作打卡,保证迟到早退不复存在。

(2)应用于个人成绩的录入,学校可以通过系统直接在学生的档案中查询成绩,且成绩无法更改也就杜绝了徇私舞弊。

(3)应用于竞选计票,保证竞选公平公正,把每个人的票数都录入区块中保证其不可篡改和伪造,每个人的票数都是真实可信的。

(4)应用于大数据杀熟,互联网电商可以通过区块链技术收集用户信息,综合处理,挑选出利润最高的用户进行杀熟,获取最大利益。

在生活中还难以见到区块链的影子,区块链作为一种新兴技术,想要落地发挥效用还需要时间,其中带来的隐私问题也颇受人诟病。要想区块链真正造福人民还需要大众的认可和信赖。

4 结论

区块链技术经过一步步的演进已经相当的成熟了。它最开始由中本聪开发并率先应用于电子货币-比特币的发行中,如今越来越多的人认识并接受了它,区块链技术也有了更深层次的应用。本文主要通过动手实践和查询资料成功地探索了区块链技术的本质和技术内核,也达成了对其应用前景的探究。但是在区块链技术本身上理解还不够深刻,对于它的多层次架构跨链技术还不熟悉。针对以上不足我将进行深入的学习架构区块链的知识,并进行一定的跨链操作提高自己的技术水平。

参考文献

[1]袁 勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494.

[2]李 青,张 鑫.区块链:以技术推动教育的开放和公信[J].远程教育杂志,2017,35(01):36-44.

[3]刘瑜恒,周沙骑.证券区块链的应用探索、问题挑战与监管对策[J].金融监管研究,2017(04):89-109.

[4]张 偲.区块链技术原理、应用及建议[J].软件,2016,37(11):51-54.

[5]张 锐.基于区块链的传统金融变革与创新[J].国际金融,2016(09):24-31.

[6]黄冠华.区块链改进联网审计途径研究[J].财政科学,2016(10):84-91.

[7]张 健.区块链技术的核心、发展与未来[J].清华金融评论,2016(05):33-35.

[8]练小川,吴 孟,曹子郁,张良晗.比特币和区块链技术将改变一切[J].出版科学,2017,25(04):5-10

[9]章 宁,钟 珊.基于区块链的个人隐私保护机制[J].计算机应用,2017,37(10):2787-2793.

收稿日期:2019-3-15