时间戳在区块链技术中的运用研究

袁　亮（武汉商学院经济与金融学院讲师，湖北　武汉　430056）

摘　要：时间戳解决了“在什么时候存在什么数据的问题，并且不容篡改。”区块链时间戳的存在使得每一笔数据都具有时间标记，通过将每一笔交易、每一个生产的区块以时间先后排列，并且将前后区块首尾相连。每一个区块都会包含前一个区块中的 Hash 值，从而实现堆叠。在人们的经济生活中，时间是一个非常重要的概念，这一点在电子交易中表现得尤为明显和重要。时间戳是区块链技术中的最大创新点，然而也面临着诸多潜在的问题与风险。

关键词：时间戳；区块链；比特币

区块链和区块链技术是两个完全不同的概念。区块链是指利用数学和技术手段记录数据，并对数据进行打包、分区、链接从而形成数据链条。区块链技术则指一种通过自身分布式节点进行数据交互、验证、储存的一种技术方案。区块链技术的重大意义在于实现了在非安全的虚拟环境中数据的安全交互，其去中心化特点具有较高的创新意义。根据中心化移动的程度和偏离值的不同，区块链可以分为公共链、联盟链、私有链。区块链的去中心化是基于密码学算法建立的一个全球信用的基础协议。

“区块 + 链”的结构为我们提供了一个数据库的完整历史。时间戳的运用帮助数据库整理从第一个数据到最新的数据发生的先后顺序和提供数据的完整性与权威性，其为数据库提供了逐笔数据的查找功能。区块链上的每一笔交易数据都可以通过时间戳查找到，并一笔一笔得到验证。

1 时间戳是区块链技术的最大创新点

区块链的分布式功能，是通过构建分布式数据库系统和参与者公示协议，保护数据的完整性。这个完整性通过时间戳来完成。时间戳就是对区块链中的每一个区块上的信息生产加上时间验证，对每一个数据的输入追本溯源、根据时间顺序排列、验证、确保数据的真实性，不容数据被篡改，证明数据的原创性和所以权的归属。

在区块链技术中，数据以电子记录的形式被永久储存下来，存放这些电子记录的文件我们称之为区块。区块是按时间顺序一个一个先后生成的，每一个区块记录下它在被创建期间发生的数据变动，所有区块汇总起来形成一个记录合集。区块链数据库最大的创新点就是时间戳。区块链数据库让全网的记录者在每一个区块中都盖上一个时间戳，证明这个时间点上的数据输入，形成一个不可篡改，不可伪造的数据库。时间戳可以证明某一个活动、发明、创造是谁在第一时间进行的数据输入，其后的发表均为转载。

我国唯一权威法定时间服务机构就是中国科学院国家授时中心，其承担着我国的标准时间的产生、保持和发播任务。中国科学国家授时中心的唯一性代表着极高的权威，但这也给时间戳的安全隐患埋下伏笔。授时系统是国家不可缺少的基础设施，承担着重要的任务，负债标准时间、标准频率发播。

联合信任时间戳服务中心是国家授时中心和联合信任共同创建的我国唯一权威可信时间戳服务机构（TSA）。服务中心于 2005 年开始筹备建设，2007 年正式运营。作为解决可靠电子签名和保障数据电文原件形式的核心基础设施，联合信任时间戳服务中心签发的可信时间戳已经广泛应用在司法、行政执法、知识产权保护、档案、金融、证券保险、电子商务、医疗卫生、电信等各领域。以（TSA）的运营模式为背景，简单解释时间戳的技术原理为，任意格式的电子文件都可以算出一个 Hash 值。这个 Hash 值计算主要是通过单项散列函数的算法。这个 Hash 值相当于一个电子文件的特殊密码。然后这个特殊密码被上传到联合信任在国家授时中心的服务器中，特殊密码与此刻国家授时中心中的时间信息绑定在一起，生成时间戳文件。

这样就会生产两个文件，一个是原始文件，一个是由联合信任服务中心加上时间戳后返回的文件，这两个文件是一组证据对。当原始文件遭到破坏时，或者文件原始性遭到质疑时，可以通过单项散列函数的算法再算一遍文件的 Hash 值，也就是得到文件的特殊密码，然后拿新的密码与之前由联合信任服务中心加上时间戳后返回的文件密码加以比对，如果密码吻合，则证明背后计算的 Hash 值一致，文件没有遭到破坏。

区块链时间戳的理论基础由来已久，可以追溯到哈勃和斯托尔内塔在 1991 年开始发表的一系列论文。他们提出一种可以安全对数据进行时间戳记录的方法。时间戳是为了记录文件创建的时间，更重要的是，可以准确反映文件创建的先后顺序：如果一个文件比另一个文件更早创建，可以从时间戳看出来。时间戳的安全性体现在文件的时间戳一旦生成，无法更改。

用户发送文件时，哈勃和斯托尔内塔设计的体系能够向客户提供时间戳服务。服务器收到文件时会用当时的时间，文件本身和文件生成的 Hash 值作为签名，来签名该文件并产生包含签名信息的认证。

区块链技术是使用随机散列并对生产的数据加上时间戳，其链式结构散列原理如下：

每个用户都有一个公钥和一个私钥。用户 2 使用用户 1 公钥验证，用户 1 通过用户 2 公钥发给用户 2 的使用用户 1 私钥签名及先前所有的交易信息，并确认用户 1 的身份，然后将交易信息进行重新组合或者分解，签署随机散列的数字签名，再链接用户 3。

区块链在进行随机散列时要加上时间戳，这样就可以通过时间戳有效证明每一个区块存在的合法性，每一个带有时间戳的数据会将上一个带有时间戳的数据纳入其随机

散列值中，用以检验和加强上一时间戳信息。

类似于我在发出的每份纸条上印上一串独特的序列号。当被人把纸条给你时，你检查一下我的签名，然后打电话给我，告诉我相应的序列号，询问印有这个序列号的纸条是否已被使用过。如果我告诉你没有，那你就可以放心地收下这个纸条。我会在账本上记录该纸条已被使用。

时间戳技术具有的另一大优势特点：在这个讲究信息安全的年代，“零知识证明”是时间戳的亮点，也就是说在不知道原始数据的实际内容的情况下证明其是否被篡改，极大地解决了信息安全问题。

2 时间戳面临的问题

在千禧年危机中，因为担心电脑系统无法识别 1900 和 2000 之间的区别，人类第一次面临了由于系统时间记录错乱而引发巨大灾难的潜在威胁。 在时间戳的运用当中，一个时间戳的信任程度直接取决于对于时间戳权威的信任程度，这涉及一系列问题，如：他们是如何得到时间的？时间源是否稳定？可以防止篡改吗？它是一台依赖于内部时钟的常规 PC 电脑，还是与权威授时部门保持同步的专用硬件设备？即使时间源本身是可信的，但是加盖时间戳所使用的密钥的安全性有多大程度的可信度呢？如果密钥受到威胁了，那么它所产生的所有时间戳也都受到威胁。

2016 年 6 月 25 日，中国互联网金融（青岛）高峰论坛在青岛举行。安存科技旗下公司北京安金网络科技有限公司副总裁马成龙在论坛上发言中称：“互联网金融领域之所以有这么多乱象发生，根源在于互联网这个虚拟空间里，记录主体行为的载体变成了电子数据，很难追溯。”

作为一种永久存储，信息不可篡改的分布式数据库，区块链由数以亿计的大量计算节点共同维护。复杂的校验机制和时间戳技术使得保存在区块链上的数据具有连续性和一致性。这也是区块链技术在互联网金融领域中被极度看好的主要原因。但是整个校验机制中过分依赖时间戳，如果时间戳一旦遭到威胁，整个区块链技术数据被记录的先后顺序将发生混乱，数据的连续性将遭到破坏。

时间戳的运用存在数据确认时间较长的问题，这一问题在金融区块链系统中尤为严重。以比特币区块链为例，当前比特币交易的一次确认时间大约 10 分钟，6 次确认的情况下，需要等待约 1 小时。当然对于信用卡动则 2–3 天的确认时间来说，比特币已经有了很大的进步，但是距离理想状态还有很大的距离。

随着区块链的发展，带有时间戳的区块数据体积会越来越大，存储和计算负担将越来越重。以比特币区块链为例，其完整数据的大小当前已达 63.61G，用户如果使用比特币核心客户端进行数据同步的话，可能三天三夜都无法同步完成，并且，区块链的数据量还在不断地增加。这给比特币核心客户端的运行带来了很大的困难。

参考文献：

[1] 阿尔文德·纳拉亚南，约什·贝努，爱德华·费尔顿，安德鲁·米勒 . 区块链技术驱动金融 [M]. 北京：中信出版社 ,2016.

[2] 长铁，韩锋 . 区块链从数字货币到信用社会 [M]. 北京：中信出版社 ,2016.

[3] 韩布伟 . 区块链重塑经济的力量 [M]. 北京：中国铁道出版社 ,2016.

[4] 朱建明，付永贵 . 基于区块链的供应链动态多中心协同认证模型 [J]. 网络与信息安全学报 ,2016,(1).

[5] 冯珊珊 . 时间戳：给电子合同“按指纹”[J]. 首席财务官 ,2016,(6).

[6] 骆慧勇 . 区块链技术原理与应用价值 [J]. 金融纵横 ,2016,(7).

[7] 方燕儿，何德旭 . 区块链技术在商业银行产业链金融中的发展探索 [J]. 新金融 ,2017,(4).

[8] 伍旭川 . 区块链技术的特点、应用和监管 [J]. 金融纵横 ,2017,(4).

[9] 俞学劢 . 区块链的 4 大核心技术 [J]. 金卡工程 ,2016.(10).

[10] 林小驰，胡叶倩雯 . 关于区块链技术的研究综述 [J]. 金融市场研究 ,2016,(2).

[11] 郭伟，漆溢，荣川 . 数字时间戳服务系统的设计 [J]. 时间频率学报 ,2006,(6).

作者简介：

袁亮（1980- ），男，毕业于美国大河谷州立大学，金融专业，研究方向：网络化教学与价值投资。

基金项目：2016 武汉商学院校级科学研究项目“基于区块链技术的 p2p 平台的开发与应用”（项目编号：2016kc07）

（上接第 108 页）

4 强制放顶爆破效果

本次深孔爆破强制放顶工作取得的效果较好。爆破后顶板未出现大量涌水及工作面设备、设施损坏现象。爆破后采空区基本顶有效预裂，且充填率达到了预期目的。工作面推进了12.6m左右时顶板从工作面中部开始逐渐垮落，工作面推进到 20m 时采空区已基本垮落严实，此后，当工作面推进到 38m 时工作面开始初次来压，来压步距平均为 41.4m，来压强度不大。

由葫芦素煤矿 21102 工作面切眼深孔预裂爆破强制放顶成功经验，在本矿的 21204 工作面切眼也采取了同样参数的深孔爆破强制放顶，同样取得了良好的效果，由以上两个工作面的实际情况来综合确定，对于榆神矿区葫芦素煤矿 2–1 煤面长为 320m 的综采工作面，在进行深孔爆破强制放顶后，其初次来压步距与周期来压步距相当接近。

5 结论

葫芦素矿 21102 工作面依据煤层直接顶、老顶厚度、现场观测、理论分析和实验分析的方法，提出采用深孔预裂爆破，强制放顶技术。通过设置孔深和间距以及爆破方式，缩短了初次来压步距，取得良好效果。爆破后顶板未出现大量涌水及工作面设备、设施损坏现象。爆破及施工过程也未发生任何安全事故。爆破后采空区基本顶有效预裂，且充填率达到了预期目的。

参考文献：

[1] 张亮，解兴智 . 浅埋煤层坚硬顶板初采爆破放顶研究 [J]. 煤矿开采 ,2014(1):83-86.

[2] 钱鸣高 . 岩层控制中的关键层理论 [J], 煤炭学报 ,1996(3):225-230.

[3] 曹胜根，缪协兴 . 超长综放工作面采场矿山压力控制 [J]. 煤炭学报 ,2001(6):621-625.