# 基于联盟链的分布式高效身份认证*

姚 影[1],颜 拥[1],郭少勇[2],熊 翱[2],张 旺[2]
(1.国网浙江省电力有限公司电力科学研究院,浙江 杭州 310014;2.北京邮电大学,北京 100876)

**摘 要**:为了解决传统身份认证中用户认证流程繁琐、身份信息不安全、认证系统易受攻击等问题,提出了一种基于联盟链的分布式身份认证方法,利用区块链的去中心化、不易篡改的特性和非对称加密等方法,提高用户身份认证系统的安全性和稳定性。在此基础上设计了分布式认证方案,包括身份注册和认证流程,并对其中的核心共识算法PBFT进行了优化,以提高认证效率。实验结果表明,基于区块链的认证机制和优化的PBFT算法提升了认证系统的可靠性并保证了其高效性。

**关键词**:联盟链;身份认证;非对称加密;PBFT
**中图分类号**:TN918.4;TP311.13 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.211816

**中文引用格式**:姚影,颜拥,郭少勇,等. 基于联盟链的分布式高效身份认证[J].电子技术应用,2022,48(3):104-108.
**英文引用格式**:Yao Ying,Yan Yong,Guo Shaoyong,et al. Distributed and efficient identity authentication based on consortium blockchain[J]. Application of Electronic Technique,2022,48(3):104-108.

## Distributed and efficient identity authentication based on consortium blockchain

Yao Ying[1],Yan Yong[1],Guo Shaoyong[2],Xiong Ao[2],Zhang Wang[2]
(1.State Grid Zhejiang Electric Power Company Electric Power Research Institute,Hangzhou 310014,China;
2.Beijing University of Posts and Telecommunications,Beijing 100876,China)

**Abstract**:In order to solve the problems of cumbersome user authentication process, insecure identity information, and vulnerability of authentication system in traditional identity authentication, a distributed identity authentication method based on alliance chain is proposed, which uses the decentralization of blockchain and is not easy to tamper with. Features and asymmetric encryption methods are used to improve the security and stability of the user identity authentication system. On this basis, a distributed authentication scheme was designed, including identity registration and authentication processes, and the core consensus algorithm PBFT was optimized to improve authentication efficiency. The experimental results show that the blockchain-based authentication mechanism and optimized PBFT algorithm improve the reliability of the authentication system and ensure its efficiency.

**Key words**:consortium blockchain;identity authentication;asymmetric encryption;PBFT

## 0 引言

传统互联网业务的身份认证技术主要以用户名密码为主[1],但随着互联网业务越来越多,不同的业务需要重复注册不同的账号,并且通常同一个用户不同账号之间的密码存在关联性,容易造成密码泄露的风险[2]。同时,传统认证系统是中心化[3]的,用户隐私信息存放在企业系统中。但是身份认证信息存储方式较为简单,相关系统易受攻击、用户隐私身份信息泄露的隐患较大。并且传统的中心化认证系统是业务系统的唯一认证接口,如果其遭受到有效攻击,那么系统存在极大的崩溃风险[4],因此为了解决用户隐私信息安全、维护业务系统的稳定性,构造分布式的身份认证系统是现在亟待解决的问题。

区块链技术[5]发展于比特币中,具有分布式去中心化、数据可追溯、不可篡改的优点。因为其分布式去中心化的特性,如果想要有效攻击区块链网络的话,需要同时攻克其不同节点[6],因此其比中心化网络更加稳定可靠;区块链的数据可追溯不可篡改[7]的特点,使得无人能够修改区块链上的数据,因此区块链网络下的不同节点之间能够相互信任彼此。区块链的高稳定性和信任传递的能力为身份认证技术提供了新的思路[8]。

联盟链作为区块链的一种是由多个机构共同参与管理的,与公有链访问权限全公开不同的是,只有这些机构拥有联盟链的写入与访问权限[9]。由于联盟链弱化了网络复杂性,可以使用更松散的共识机制,因此共识效率比公有链高很多同时具有去中心化的优势[10],具有很大的实用价值。

本文针对传统身份认证所存在的重复认证、身份隐

*基金项目:国网浙江省电力有限公司科技项目(5211DS200002)

私不安全、单一系统易受攻击等痛点，结合联盟链的优势，构建出一套基于联盟链的身份认证方法。并为了提高系统的认证效率，改进了分布式身份认证方法中联盟链的共识算法[11]。

## 1 方案设计

### 1.1 系统架构设计

为了解决传统身份认证中存在的不同问题，本文利用区块链技术构建分布式身份认证方案[12]。基于区块链的分布式身份认证架构包括四个部分：可信授权中心、联盟链网络、业务系统和用户，其结构如图 1 所示。在本系统中，用户通过提交自身身份信息至业务的身份认证系统，由业务系统将用户的身份信息加密上链，完成用户身份的注册；当用户访问业务系统时，业务系统从区块链节点上获取相应用户注册信息，与用户认证信息进行对比验证，完成用户认证功能。

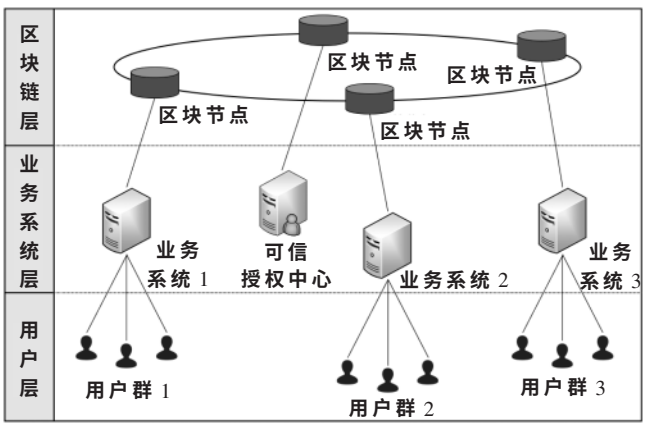



图 1 基于联盟链的分布式身份认证架构

分布式身份认证架构各个部分的功能如下：

(1)可信授权中心：负责为各业务系统和用户颁发数字证书。

(2)区块链网络：每个区块链节点由区块链中的一个企业维护，提供用户实体身份信息上链和查询等功能。

(3)业务系统：提供各类业务服务的不同应用系统，并且对访问系统的用户进行注册和认证功能。

(4)用户：访问业务系统的人，身份认证系统的使用者。

### 1.2 流程设计

在本方案设计的认证系统中，用户的注册信息通过可信信道送到区块链网络中，并广播共识到所有区块链结点中，区块链网络中的任意服务节点均可获取用户的注册身份，从而能够实现对用户单点注册多点认证的功能，省去了重复注册用户账号密码的麻烦。用户认证信息包含以下几种数据，具体见表 1。

#### 1.2.1 注册身份流程

用户注册流程如下：

(1)用户 U 在本地根据 ECC 秘钥生成算法生成自己的公私钥对(UPK，USK)，其中公钥为 UPK，私钥为 USK。

表 1 身份信息数据说明

| 标识 | 说明 |
|---|---|
| UID | 用户身份信息，由用户注册时用户自己设定 |
| UAI | 用户验证信息，可为密码、指纹、面容 ID 等 |
| UPK | 用户公钥，由用户自己生成，采用 ECC 算法 |
| USK | 用户私钥，由用户自己生成，采用 ECC 算法 |
| IS | 用户身份信息摘要 |
| DS | 用户身份信息数字签名 |
| DC | 用户数字证书 |

(2)用户 U 在业务系统的注册接口输入自己的用户身份 UID、用户认证信息 UAI、公钥 UPK。

(3)业务系统 BS 接收到用户发来的注册信息(UID，UAI，UPK)，核查 UID 与 UPK 是否和已有注册用户的身份或公钥冲突，如果至少有其中一项冲突，则向用户反馈注册失败信息，并返回第(1)步重新开始；若都不冲突，则向下进行。

(4)业务系统 BS 将用户身份 UID、用户认证信息 UAI 进行 hash 运算得到用户的身份信息摘要 IS，返回给用户，并通知用户注册身份信息正确。

(5)用户 U 收到身份信息摘要 IS 后，用自己的私钥 USK 对身份信息摘要进行加密，生成数字签名 DS，发送给业务系统。

(6)业务系统 BS 收到用户数字签名 DS 后，将其与用户身份 UID、用户公钥 UPK 发送给区块链节点 s。

(7)区块链结点 s 接收到业务系统发来的相关信息后，将信息打包共识到区块链网络，并由可信授权中心为用户发布数字证书 DC。

(8)当区块链网络将注册信息共识成功后，由业务系统 BS 通知用户 U 注册成功，并将数字证书 DC 返回给用户，由用户保存。

#### 1.2.2 认证身份流程

用户认证流程如下：

(1)用户 U 在业务系统认证接口输入用户身份 UID、用户认证信息 UAI 与数字证书 DC。

(2)业务系统 BS 接收到用户发来的认证信息(UID，UAI，DC)后，将其广播到联盟链上的所有业务系统中，一起对其进行验证。并由各系统对认证信息进行共识投票。

(3)业务系统 BS 根据用户身份 UID 到区块链节点 s 上查找注册时 UID 对应的公钥 UPK′。并判断链上用户公钥 UPK′与数字证书 DC 内的用户公钥 UPK 是否一致。若 UPK≠UPK′，则说明用户身份信息与注册时绑定的用户公钥不一致，在认证共识中投反对票；若 UPK=UPK′，则说明用户身份信息与注册时绑定的用户公钥一致，进行下一步验证。

(4)业务系统 BS 根据用户身份 UID 进一步到区块链节点处获取注册时 UID 对应的用户数字签名 DS。并用用户数字证书 DC 内的用户公钥 UPK 对数字签名 DS 进

行解密，得到用户身份对比身份信息摘要 IS′。

(5)业务系统 BS 对用户身份 UID 与用户认证信息UAI 进行 hash 计算，得到用户认证身份信息摘要 UIS。若 IS≠IS′，则说明用户输入的认证信息 UAI 不正确，认证失败；若 IS=IS′，则说明用户输入的身份信息与注册时无误，验证成功，在认证共识中投通过票。

(6)联盟链网络根据最终的认证共识投票情况给出认证结果，业务系统 BS 根据认证结果判断是否为用户提供服务。

## 2 共识算法优化

为了使身份认证系统工作更加高效，提高其注册、认证的吞吐量，本节对 PBFT 算法[13]进行优化，以满足分布式身份认证对共识效率的要求。

### 2.1 PBFT 算法改进思路

节点数为 $N$ 的传统 PBFT 算法网络，可以容错 $f$ 个拜占庭节点，其中 $f=(N-1)/3$。但是为了这个容错能力，产生了很多无效的通信[14]。因为节点在收到 $2f+1$ 个正确的消息之后就可以进入下一阶段，但是每个节点要向网络中广播大于 $3f$ 个消息[15]。无效的通信主要发生在准备阶段的全网广播。因此，改进的 PBFT 算法引入动态权重机制，称其为“动态实用拜占庭容错算法(Dynamic Practical Byzantine Fault Tolerance，DPBFT)”，根据节点在共识过程中的表现情况来动态调整不同节点之间的权重值。每个共识节点维护一个权重向量表 $W_T=\{w_1,w_2,\cdots,w_i,\cdots,w_N\}$，其中权重 $p=n/N$ 反映出 $i$ 节点的动态通信性能和可信度。$W_T$ 会随着共识的进行而不断更新，在每轮共识结束之后，每个共识节点会根据此次共识的投票和通信情况对自己维护的 $W_T$ 进行更新。共识期间选择权重最大的那几个节点来进行选择性广播。之后在共识流程的广播阶段，节点将在各自的广播域内进行投票消息广播，并且广播域将随着 $W_T$ 的更新而更新。引入一个动态参数 $p$ 来表示选择性广播域的大小，其中 $p=n/N$。$n$ 为选择性广播域中节点的个数。

### 2.2 算法设计

算法流程如图 2 所示。首先初始化共识节点的投票权重，开始进行一次正常的 PBFT 投票流程。然后根据每次投票的结果，动态调整权重，构建选择性广播域。改进的 PBFT 算法与传统的 PBFT 算法流程大体相似，只是在一致性协议的广播阶段进行相应改进。这里对改进后的算法一致性协议阶段进行主要功能描述：

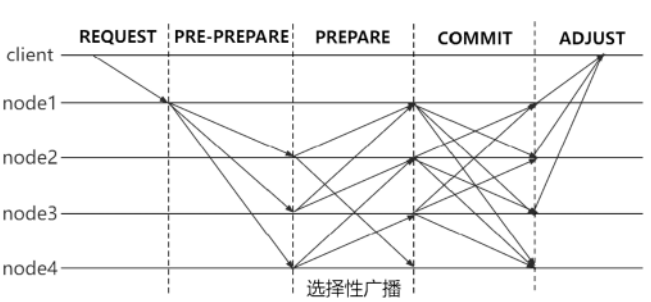



图 2 改进的 PBFT 算法流程图

(1)PRE-PREPARE 阶段：主节点接收客户端发送的 PRE-PREPARE 消息，并将消息广播给参与共识的所有节点。

(2)PREPARE 阶段：从节点收到主节点发送的 PRE-PREPARE 消息后生成 PREPARE 消息，根据 $W_T$ 和 $p$ 值去定一个选择性广播域，将 PREPARE 消息选择性广播给自己的共识域内的节点。如果接收到超过 $2f+1$ 个正确的准备消息，则会进入 COMMIT 阶段。

(3)COMMIT 阶段：节点生成 COMMIT 消息并广播到共识域内节点，其他节点验证 COMMIT 消息，验证通过后，进行 ADJUST 阶段。

(4)ADJUST 阶段：根据共识结果给每个参与共识节点的情况进行打分。根据各个节点提交 commit 的时间，为每个节点离散化 0~100 分数。根据式(1)：

$$Q_i=100(T-t_i)/T \tag{1}$$

式中 $Q_i$ 为 $i$ 节点本轮共识的得分，$t_i$ 为 $i$ 节点提交 commit 的时间，$T$ 为第一个 commit 发生到共识结束总耗时。第一个提交 commit 的节点得分 100 分，未参加 commit 的节点得分为 0。并根据式(2)动态调整每个节点权重。

$$W_i=(1-q)\cdot w_i+q\cdot Q_i \tag{2}$$

式中 $q$ 为上一状态权重在新权重中所占比例，$w_i$ 为上一状态中 $i$ 节点权重值。

## 3 安全性分析

### 3.1 用户身份信息安全性分析

区块链节点上只保存用户认证信息的摘要，不保存用户认证信息 UAI 的明文信息，攻击者即使攻破联盟链网络中的节点也无法获取用户对应的认证信息 UAI。并且用户公钥由可信授权中心颁发数字证书，只有合法注册的公钥才能在业务系统上验证。攻击者很难同时获取用户的数字证书 DC 和认证信息 UAI 来伪造用户身份。因此本系统可以有效保证用户的身份信息安全。

### 3.2 系统稳定性分析

用户身份信息加密保存在区块链节点，每个业务系统都可以通过访问联盟链网络获取用户加密身份信息进行验证。当某个业务认证系统瘫痪后，用户可以选择就近业务系统进行验证。因此本系统可以实现单点注册，多点认证，提升可用性的同时有效防止中心化业务认证系统的易崩溃，不稳定的风险。

## 4 性能分析

基于 GO 编程语言实现了一个多节点联盟链实验系统，用以模拟在本设计方案中用户注册以及用户行为上链共识过程。在该系统中对原 PBFT 算法和本文提出的 DPBFT 算法进行了性能测试。主要分析 PBFT 与 DPBFT 在不同的 $p$、$q$ 值的选取上存在的性能差异。

### 4.1 认证时延

认证时延是指企业或授权中心向区块链网络发送上链信息到区块链网络完成共识的时间间隔。在不同节点数量的情况下，比较了 PBFT 和 DPBFT 算法的认证时延，同时引入影响广播域大小的因子 $p$ 和分数调整的衰减因子 $q$ 来观察其对认证时延的影响。每个数据都是重复测试 20 次后取的平均值。实验结果如图 3 所示，DPBFT 算法比 PBFT 算法所产生的认证时延要小。当区块链网络节点数量和衰减因子 $q$ 确定时，$p$ 的大小决定了节点选择性广播域的大小。从图中可以看出，$p$ 越小，交易时延越小，共识效率越高。但不可为了追求共识效率设置很小的 $p$ 值，因为当 $p$ 值小于 2/3 时，节点不能接收到足够的信息进入确认状态，导致全网不能共识。

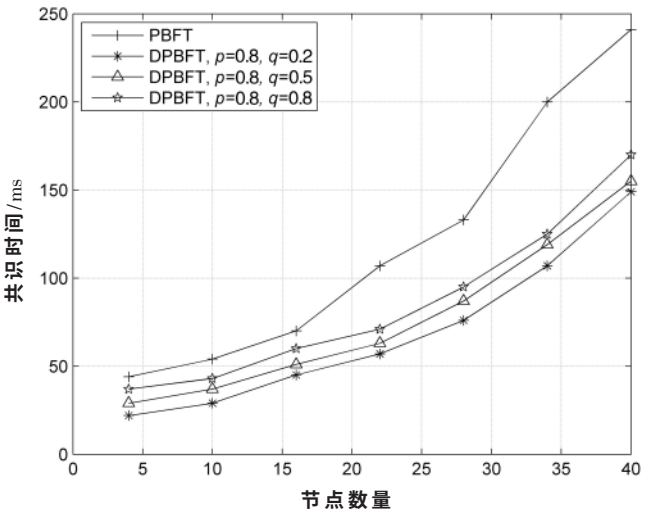
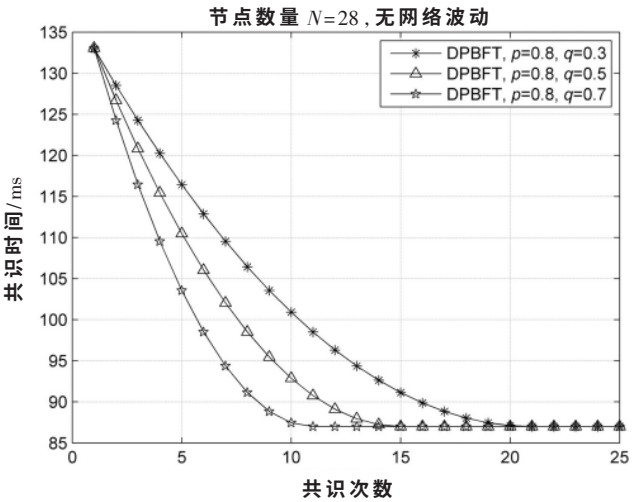



图 3　相同 $q$ 值不同 $p$ 值的 DPBFT 算法与 PBFT 算法的交易时延

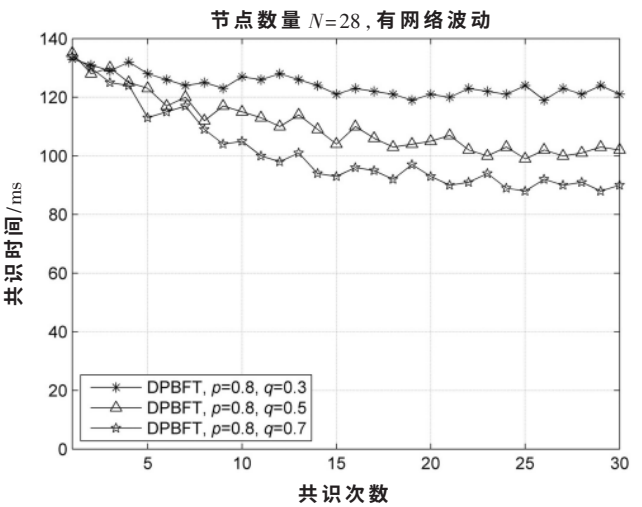
衰减因子 $q$ 对选择性广播域的大小没有影响，因此其对共识效率也没有影响。在无网络波动的情况下，观察了区块链网络节点数量和影响广播域因子 $p$ 确定时，不同的衰减因子 $q$ 对网络共识时间的影响，结果如图 4(a) 所示。衰减因子 $q$ 越大，最近一次共识得分对整体分数的影响效果越大。因此，$q$ 越大，网络收敛到最佳广播域的速度越快。但当存在网络波动时，如图 4(b)所示，最近一次共识结果的得分不能象征整体网络中节点的可依靠程度。因此，$q$ 越大，节点得分调整幅度过大，导致一直没法收敛到最佳状态，共识效率提升不高。所以，为了使共识效率达到最理想状态，应该根据网络波动情况，选择合适的 $q$ 值。

### 4.2 认证吞吐量

“吞吐量(Transaction Per Second，TPS)”指的是在单位时间内完成的认证的数量。实验中每秒向区块链网络发送 100 条认证请求，记录每秒能够完成认证的数量，并在不同节点个数的情况下进行测试。图 5 所示为改进前后的 PBFT 的吞吐量对比图。可以看出，在相同节点数量和相同衰减因子 $q$ 的情况下，改进的 PBFT 算法比 PBFT 算法吞吐量高，随着网络节点数量的增加，每种算




(a)无网络波动




(b)有网络波动

图 4　相同 $p$ 值不同 $q$ 值的 DPBFT 算法与 PBFT 算法的共识时间

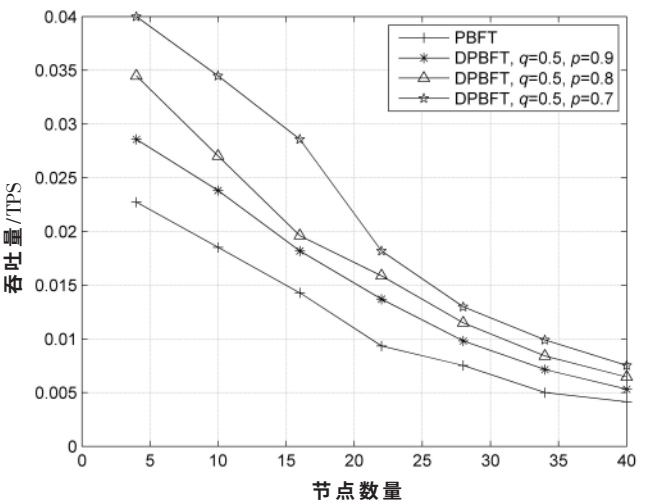



图 5　DPBFT 算法与 PBFT 算法的吞吐量比较

法的吞吐量都会下降，因为共识阶段需要广播的消息变多了。同时，在相同节点数量的情况下，$p$ 越小，选择性广播域越小，每一条消息的共识时间越短，因此吞吐量越高。

## 5 结论

针对传统身份认证技术的弊端，提出了一种基于联盟链的分布式身份认证方法。用户在业务系统注册身份之后，身份信息加密广播共识到所有联盟链节点，每个节点都可以对注册的用户进行认证，达成用户单点注册多点登录的功能并有效防止了用户身份隐私泄露的风险。用户认证过程由全网共识投票，即使服务节点故障，也可依靠整个系统的分布式鲁棒性来保证认证系统的正常工作，提高系统的抗攻击能力。最后通过实验表明，本方法比传统联盟链共识效率更快，吞吐量更高。可根据网络情况调整 $p$、$q$ 值，达到效率最大化。

## 参考文献

[1] 宋芹芹，袁泉.PKI/CA 系统异地统一身份认证研究与实现[J].网络安全技术与应用，2017(6)：54-55.
[2] 丁子康，黄锐，杨鸿靖宇.密码学技术的发展与网络安全研究[J].无线互联科技，2019，16(7)：38-39.
[3] 李强，舒展翔，余祥，等.区块链系统的认证机制研究[J].指挥与控制学报，2019，5(1)：1-17.
[4] 姚伟.无口令身份认证技术的研究与实现[D].绵阳：西南科技大学，2020.
[5] 申屠青春.区块链底层技术平台[A].中国人民大学国际货币研究所.《IMI 研究动态》2016 年合辑[C].中国人民大学国际货币研究所，2016：6.
[6] 单康康，袁书宏，张紫徽，等.区块链技术及应用研究综述[J].电信快报，2020(11)：17-20.
[7] 苗清岚.区块链存证的应用问题研究[J].营销界，2020(38)：107-109.
[8] 吴乾隆.基于区块链的物联网身份认证技术研究[D].重庆：重庆邮电大学，2020.
[9] 郭上铜，王瑞锦，张凤荔.区块链技术原理与应用综述[J].计算机科学，2021，48(2)：271-281.
[10] 冷基栋，吕学强，姜阳，等.联盟链共识机制研究综述[J].数据分析与知识发现，2021，5(1)：56-65.
[11] 李福涛.区块链中的共识机制[J].中国新通信，2019，21(21)：12.
[12] 王乃洲，金连文，高兵，等.基于区块链技术的身份认证与存储方法研究[J].现代信息科技，2020，4(8)：164-167.
[13] 王冠，张文月.基于可信性评估的区块链共识机制的研究[J].郑州大学学报(理学版)，2020，52(3)：27-33.
[14] 黄秋波，安庆文，苏厚勤.一种改进 PBFT 算法作为以太坊共识机制的研究与实现[J].计算机应用与软件，2017，34(10)：288-293，297.
[15] 张良嵩.基于拜占庭容错的区块链共识算法研究[D].成都：电子科技大学，2020.

(收稿日期：2021-05-30)

作者简介：

姚影(1989-)，男，工程师，主要研究方向：能源区块链。

颜拥(1986-)，男，高级工程师，主要研究方向：能源区块链。

郭少勇(1985-)，男，博士，副教授，主要研究方向：区块链、物联网、泛在网络和智能电网。

扫码下载电子文档

(上接第 103 页)

IEEE Transactions on Power Electronics，2001，16(1)：26-33.
[6] PANOV Y，JOVANOVIC M M.Design considerations for 12-V/1.5-V，50-A voltage regulator modules[J].IEEE Transactions on Power Electronics，2001，16(6)：776-783.
[7] AHMED M H，CHAO F，LEE F C，et al.48-V voltage regulator module with PCB winding matrix transformer for future data centers[J].IEEE Transactions on Industrial Electronics，2017，64(12)：9302-9310.
[8] 郭冠亚.1V/30A 输出应用新型同步整流驱动方案的正反激电路的研究[D].杭州：浙江大学，2008.
[9] 高双，赵世伟，张龙威，等.一种基于 Sepic 的新型高增益 DC/DC 变换器[J].电子技术应用，2021，47(5)：108-111，116.
[10] 卢诚，邵剑龙，谢实，等.离散数字恒能量斩波变流母技术：CN1547317A[P].2004-11-17.
[11] 谢鹤龄，金建辉，谢佳明，等.一种高性能脉冲信号处理电路模块[J].电子技术应用，2020，46(1)：39-43.
[12] 朱俊颖.开关电源 PCB 电磁干扰的仿真与实验分析[D].成都：电子科技大学，2020.
[13] 骆嘉迪.系统级封装与 PCB 板级电磁兼容性研究[D].西安：西安电子科技大学，2019.
[14] 王天凤.基于 SG3525 的推挽式逆变电路设计与实现[J].仪表技术，2020(6)：4-6.
[15] 刘中锋，刘春，倪文斌.基于 SG3525 芯片的大功率恒压/恒流 LED 电源研制[J].电源技术，2016，40(2)：404-407.

(收稿日期：2021-04-24)

作者简介：

余世科(1976-)，男，本科，高级工程师，主要研究方向：电力电子技术以及电动力技术。

叶明刚(1978-)，男，硕士，高级工程师，主要研究方向：水中兵器工程研究。

谢鹤龄(1995-)，男，硕士研究生，主要研究方向：电力电子与电磁兼容、控制工程。

扫码下载电子文档

# 版权声明