

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2026/000869 A1

(43) 国际公布日
2026 年 1 月 2 日 (02.01.2026)

(51) 国际专利分类号:
H04L 9/00 (2022.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2024/139687

(22) 国际申请日: 2024 年 12 月 16 日 (16.12.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202410844017.9 2024年6月27日 (27.06.2024) CN

(71) 申请人: 杭州高新区(滨江)区块链与
数据安全研究院 (HANGZHOU HIGH-TECH
ZONE (BINJIANG) INSTITUTE OF BLOCKCHAIN
AND DATA SECURITY) [CN/CN]; 中国浙江省杭
州市滨江区物联网孵化器大楼2号楼
A楼4-7层 310051 (CN)。

(72) 发明人: 张帅(ZHANG, Shuai); 中国浙江省杭州市
滨江区物联网孵化器大楼2号楼A楼4-7
层 310051 (CN)。端豪(DUAN, Hao); 中国浙江省杭
州市滨江区物联网孵化器大楼2号楼A楼4-7
层 310051 (CN)。袁超(YUAN, Chao); 中国浙江
省杭州市滨江区物联网孵化器大楼2号楼A楼
4-7层 310051 (CN)。李晓静(LI, Xiaojing); 中国浙
江省杭州市滨江区物联网孵化器大楼2号楼
A楼4-7层 310051 (CN)。魏晓彤(WEI, Xiaotong);
中国浙江省杭州市滨江区物联网孵化器大
楼2号楼A楼4-7层 310051 (CN)。

(74) 代理人: 深圳中一联合知识产权代
理有限公司 (SHENZHEN ZHONGYI UNION
INTELLECTUAL PROPERTY AGENCY CO., LTD.);
中国广东省深圳市福田区莲花街道紫

(54) Title: CONSENSUS METHOD AND APPARATUS FOR BLOCKCHAIN SYSTEM

(54) 发明名称: 一种区块链系统的共识方法及装置

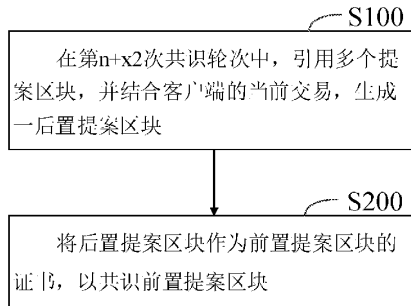


图 1

S100 IN AN (N+X2)TH CONSENSUS ROUND, REFERENCE A PLURALITY OF PROPOSAL BLOCKS, AND COMBINE SAME WITH THE CURRENT TRANSACTION OF A CLIENT, SO AS TO GENERATE A POST-PROPOSAL BLOCK
S200 USE THE POST-PROPOSAL BLOCK AS A CERTIFICATE FOR A PRE-PROPOSAL BLOCK, SO AS TO REACH A CONSENSUS ON THE PRE-PROPOSAL BLOCK

(57) Abstract: The present application is applicable to the technical field of blockchains. Provided are a consensus method and apparatus for a blockchain system. The consensus method comprises: in an (n+x2)th consensus round, referencing a plurality of proposal blocks, and combining same with the current transaction of a client, so as to generate a post-proposal block, wherein the plurality of proposal blocks are correspondingly generated by a plurality of validator nodes referencing a pre-proposal block in an nth consensus round, and the pre-proposal block is generated in an (n-x1)th consensus round; and using the post-proposal block as a certificate for the pre-proposal block, so as to reach a consensus on the pre-proposal block. By using the consensus method provided in the present application, it is unnecessary to transmit a large number of signature messages during a consensus process, instead, a reference relationship is established between blocks which are generated in different consensus rounds, so as to reach a consensus on a certain block. In this way, the overheads of transmitting and verifying signature messages during a consensus process are reduced.

[见续页]

荆社区深南大道6008号深圳特区报业大厦33层518034 (CN)。

- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。
- (84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请适用于区块链技术领域, 提供了一种区块链系统的共识方法及装置, 其中, 所述共识方法包括: 在第 $n+x$ 次共识轮次中, 引用多个提案区块, 并结合客户端的当前交易, 生成一后置提案区块; 其中, 多个提案区块是在第 n 次共识轮次中, 由多个验证节点引用一前置提案区块所对应产生的, 所述前置提案区块在第 $n-x$ 次共识轮次中产生; 将所述后置提案区块作为所述前置提案区块的证书, 以共识所述前置提案区块。利用本申请提供的共识方法, 在共识过程中不再需要传递大量的签名消息, 而是通过在不同共识轮次产生的区块之间建立引用关系, 以对某个区块进行共识。如此一来, 减少了共识过程中传输和验证签名消息的开销。