



国家知识产权局

510070

广州市先烈中路 100 号黄花岗科贸街 C 幢 305 室 广州市深研专利事
务所（普通合伙）
陈雅平(020-87685380)

发文日：

2020 年 11 月 26 日



申请号或专利号：201810634852.4

发文序号：2020111701576820

申请人或专利权人：中山大学

发明创造名称：一种基于区块链的多方公平 PDF 合同签署方法

授予发明专利权通知书

1. 根据专利法第 39 条及实施细则第 54 条的规定，上述发明专利申请经实质审查，没有发现驳回理由，现作出授予专利权的通知。

申请人收到本通知书后，还应当依照办理登记手续通知书的内容办理登记手续。

申请人按期办理登记手续后，国家知识产权局将作出授予专利权的决定，颁发发明专利证书，并予以登记和公告。

期满未办理登记手续的，视为放弃取得专利权的权利。

法律、行政法规规定相应技术的实施应当办理批准、登记等手续的，应依照其规定办理。

2. 授予专利权的上述发明专利申请是以下列申请文件为基础的：

原始申请文件。 分案申请递交日提交的文件。 下列申请文件：

申请日提交的说明书摘要、说明书第 1-111 段、说明书附图、摘要附图；

2020 年 11 月 10 日提交的权利要求第 1-2 项

3. 授予专利权的上述发明专利申请的名称：

未变更。

由__变更为上述名称。

4. 申请人于____年____月____日提交专利号为____的“放弃专利权声明”，经审查：

进入放弃专利权的程序。

未进入放弃专利权的程序。理由是：申请人声明放弃的专利与本发明专利申请不属于相同的发明创造。

5. 审查员依职权对申请文件修改如下：

注：在本通知书发出后收到的申请人主动修改的申请文件，不予考虑。

审查员：刘珍

审查部门：专利审查协作四川中心通信发明
审查部

联系电话：(028)62969354



210413
2020.3

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。



(12)发明专利申请

(10)申请公布号 CN 108833115 A
(43)申请公布日 2018.11.16

(21)申请号 201810634852.4

(22)申请日 2018.06.15

(71)申请人 中山大学

地址 510275 广东省广州市海珠区新港西路135号

(72)发明人 田海博 何杰杰 刘佳南

(74)专利代理机构 广州市深研专利事务所
44229

代理人 陈雅平

(51) Int. Cl.

H04L 9/32(2006.01)

H04L 9/08(2006.01)

H04L 9/06(2006.01)

G06Q 50/18(2012.01)

权利要求书3页 说明书9页 附图1页

(54)发明名称

一种基于区块链的多方公平PDF合同签署方法

(57)摘要

本发明涉及一种基于区块链的多方公平PDF合同签署方法,参与者包括多名合同签署方 P_1, \dots, P_n ,一个可信第三方TTP及区块链节点。首先 P_1 生成合同的可验证加密签名 VES_1 ,计算合同内容的哈希上下文 CTX_1 ,生成群组密钥协商协议GKA的元素 GE_1 ,把 VES_1 、 CTX_1 和 GE_1 封装为区块链交易,发送给区块链节点;然后 P_i 验证 P_{i-1} 的 $VES_{i-1}, 1 < i \leq n$,验证通过后 P_i 生成新的 VES_i 、 CTX_i 和 GE_i 并通过交易发给区块链节点; P_n 完成操作后, P_j 计算群组加密密钥 $GK, 1 \leq j \leq n$,加密PDF文档的数字签名形成密文 C_j ,把 C_j 封装为交易发给区块链节点; P_j 查询区块链数据,并用 GK 解密后合成完整的PDF合同; P_j 如果超时后未能获得区块链数据,与TTP通信处理异常。本发明对TTP的依赖较弱,效率更高。

