1. CN111095861 - IMPROVED TIME LOCK TECHNIQUE FOR SECURING RESOURCE ON BLOCKCHAIN

National Biblio. Data | Description | Claims | Drawings | Patent Family | Documents

PermaLink   Machine translation

Note: *The English version of this data is provided for search and reference purposes only. It is not an official translation. The original Chinese version remains the authoritative legal document. Please refer to the Chinese data for any legal or official use.*

Office
China

Application Number
201880058255.X

Application Date
04.09.2018

Publication Number
111095861

Publication Date
01.05.2020

Publication Kind
A

IPC
H04L 9/32

CPC
H04L 9/3236   H04L 9/3297   H04L 9/50
G06Q 20/40155   G06Q 20/3829
G06Q 2220/00
View more classifications

Applicants
NCHAIN HOLDINGS LIMITED
区块链控股有限公司

Inventors
WRIGHT CRAIG STEVEN
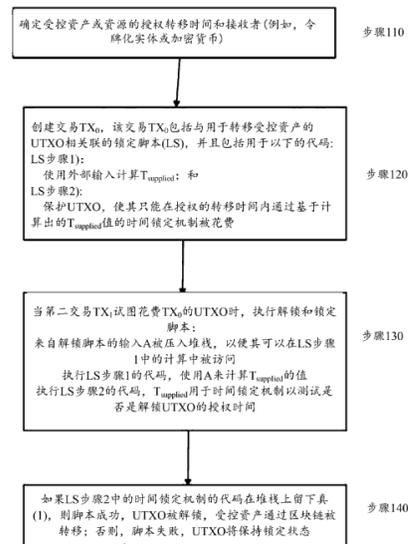克雷格·史蒂文·赖特

Agents
上海晨皓知识产权代理事务所(普通合伙) 31260

Priority Data
1714517.8 08.09.2017 GB
PCT/IB2017/055430 08.09.2017 IB

Title
[EN] Improved time lock technique for securing resource on blockchain
[ZH] 用于保护区块链上资源的改进时间锁技术

Abstract

[EN] The invention comprises a solution for securing an output (UTXO) in a single blockchain (e.g. Bitcoin) transaction (TX) so that it can only be unlocked by an authorised party at an allowed time, and in accordance with external data supplied to the transaction's locking script. The invention may comprise two steps which are implemented within a redeem script provided within the UTXO's locking script: 1) Calculation of a time-related value (which we will call Tsupplied) using the external data provided; and 2) use of the calculated Tsupplied value in a time lock technique to ensure that unlocking occurs at a time pre-determined time. The invention allows external data to be introduced into the time lock control of a transaction on the blockchain. It also includes a technique for combining absolute and relative time locks (e.g. CLTV and CSV as known in the Bitcoin protocol).
[ZH] 本发明包括了用于在单个区块链(例如，比特币)交易(TX)中保护输出(UTXO)的解决方案，使得其只能由授权方在允许的时间内根据提供给交易的锁定脚本的外部数据来解锁。本发明可包括两个步骤，所述两个步骤在UTXO的锁定脚本内提供的赎回脚本中实现：1)使用提供的外部数据计算时间相关值(我们将其称为Tsupplied)；以及2)在时间锁技术中使用计算出的Tsupplied值，以确保在预先确定的时间发生解锁。本发明允许将外部数据引入区块链上的交易的时间锁控制中。本发明还包括一种用于组合绝对时间锁和相对时间锁(如比特币协议中已知的CLTV和CSV)的技术。

Related patent documents
EP3679685   WO/2019/049022   US20200279256   JP2020533671   JP2023089153   US20240338690