1. WO2019049022 - IMPROVED TIME LOCK TECHNIQUE FOR SECURING A RESOURCE ON A BLOCKCHAIN

Publication Number
WO/2019/049022

Publication Date
14.03.2019

International Application No.
PCT/IB2018/056734

International Filing Date
04.09.2018

IPC
H04L 9/32 2006.1

CPC
G06Q 20/3829 | G06Q 20/40155 | G06Q 2220/00 | H04L 9/0643 | H04L 9/3236 | H04L 9/3297
View more classifications

Applicants
NCHAIN HOLDINGS LIMITED [AG]/[AG]
Fitzgerald House
44 Church Street
St. John's
Antigua and Barbuda

Inventors
WRIGHT, Craig Steven

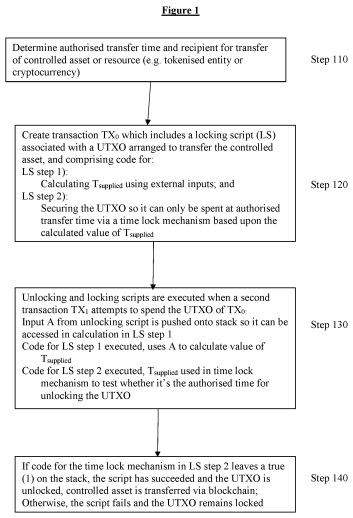
Priority Data
1714517.8 08.09.2017 GB
PCT/IB2017/055430 08.09.2017 IB

Publication Language
English (en)

Filing Language
English (en)

Designated States
View all

Title
[EN] IMPROVED TIME LOCK TECHNIQUE FOR SECURING A RESOURCE ON A BLOCKCHAIN
[FR] TECHNIQUE DE VERROUILLAGE TEMPOREL AMÉLIORÉE POUR SÉCURISER UNE RESSOURCE SUR UNE CHAÎNE DE BLOCS



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 $T_{supplied}$) using the external data provided; and 2) use of the calculated $T_{supplied}$ 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).
[FR] L'invention porte sur une solution pour sécuriser une sortie (UTXO) dans une transaction (TX) de chaîne de blocs (par exemple, Bitcoin) unique de manière qu'elle ne puisse être déverrouillée que par une partie autorisée à un moment autorisé, et conformément à des données externes fournies au script de verrouillage de la transaction. L'invention peut comprendre deux étapes qui sont mises en œuvre dans un script de rachat fourni à l'intérieur du script de verrouillage de l'UTXO : 1) calcul d'une valeur relative au temps (que nous appellerons $T_{supplied}$) à l'aide des données externes fournies; et 2) utilisation de la valeur $T_{supplied}$ calculée dans une technique de verrouillage temporel pour garantir que le déverrouillage se produit à un moment prédéterminé. L'invention permet d'introduire des données externes dans la commande de verrouillage temporel d'une transaction sur la chaîne de blocs. Elle comprend également une technique permettant de combiner de temps de verrouillage absolu et relatif (par exemple CLTV et CSV tels qu'on les connaît dans le protocole Bitcoin).

Related patent documents

CN111095861 EP3679685 US20200279256 JP2020533671 JP2023089153 US20240338690

Latest bibliographic data on file with the International Bureau