(12) UK Patent Application (19) GB (11) 2571801 (13) A

(43) Date of Reproduction by UK Office 11.09.2019

(21) Application No: 1806524.3

(22) Date of Filing: 21.02.2017

Date Lodged: 23.04.2018

(30) Priority Data:
(31) 1603117 (32) 23.02.2016 (33) GB
(31) 1604498 (32) 16.03.2016 (33) GB
(31) 1619301 (32) 15.11.2016 (33) GB

(86) International Application Data:
PCT/IB2017/050980 En 21.02.2017

(87) International Publication Data:
WO2017/145049 En 31.08.2017

(71) Applicant(s):
nChain Holdings Limited
Fitzgerald House, 44 Church Street, St. John's, Antigua and Barbuda

(72) Inventor(s):
Craig Steven Wright
Stephane Savanah

(continued on next page)

(51) INT CL:
G06Q 40/00 (2012.01) *G06Q 10/10* (2012.01)

(56) Documents Cited:
US 20150244690 A1 US 20150120567 A1
[XAY] - Gus Gutoski ET AL, "Hierarchical deterministic Bitcoin wallets that tolerate key leakage (Short paper)", (20120201), URL: https://eprint.iacr.org/2014/998.pdf, (20170505), XP055369870
- Andreas M. Antonopoulos, "Mastering Bitcoin - Unlocking Digital Cryptocurrencies", Mastering bitcoin : [unlocking digital cryptocurrencies], Beijing Cambridge Farnham KÃ¶ln Sebastopol Tokyo, O'Reilly Media, (20141220), ISBN 978-1-4493-7404-4, XP055306939

(58) Field of Search:
INT CL **G06Q, H04L**
Other: **EPO-Internal, WPI Data**

(54) Title of the Invention: **Consolidated blockchain-based data transfer control method and system**
Abstract Title: **Consolidated blockchain-based data transfer control method and system**

(57) The invention relates to blockchain technologies such as, for example, the Bitcoin blockchain. It provides a method (and corresponding system) of generating public keys for a linked structure of entities, wherein a function is applied to a deterministic key to generate the public key, the deterministic key being generated by applying a hash function to either a parent entity identifier to generate a parent deterministic key, or to a sum of the parent deterministic key and a child entity identifier to generate a child deterministic key. There is also provided a computer-implemented method for accounting on transactions with entities, the transaction being recorded in a peer-to- peer distributed ledger (blockchain), the method comprising: associating public addresses of the entities with one or more identifiers of a first classification type to classify the public addresses based on the first classification type; receiving, from a communication network, a first identifier of the one or more identifiers of the first classification type; determining a first set of public addresses associated with the first identifier, wherein the first set of public address is a subset of the public addresses; and determining a first set of transactions in the peer-to-peer distributed ledger based on the first set of public addresses associated with the first identifier, wherein the first set of transactions is a subset of the transactions.

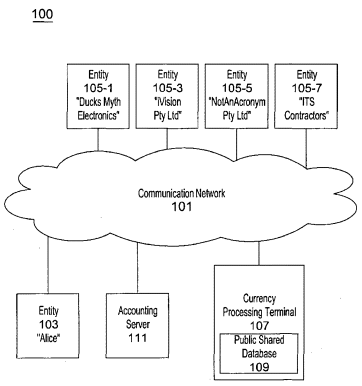

FIG. 1

GB 2571801 A

(74) Agent and/or Address for Service:
Urquhart-Dykes & Lord LLP
UDL Intellectual Property, 7th Floor, Churchill House,
17 Churchill Way, Cardiff, CF10 2HH, United Kingdom