US 20230231711A1

(19) **United States**

(12) **Patent Application Publication**

Allen

(10) **Pub. No.: US 2023/0231711 A1**

(43) **Pub. Date: Jul. 20, 2023**

(54) **BLOCKCHAIN-IMPLEMENTED METHOD AND SYSTEM**

(71) Applicant: **nChain Licensing AG**, Zug (CH)

(72) Inventor: **Gavin Allen**, London (GB)

(21) Appl. No.: **18/099,145**

(22) Filed: **Jan. 19, 2023**

Related U.S. Application Data

(63) Continuation of application No. 16/320,083, filed as application No. PCT/IB2017/054423 on Jul. 21, 2017, now Pat. No. 11,563,574.

(30) **Foreign Application Priority Data**

Jul. 29, 2016	(GB)	1613148.4
Jul. 29, 2016	(GB)	1613177.3
Jul. 29, 2016	(GB)	1613188.0

Publication Classification

(51) **Int. Cl.**

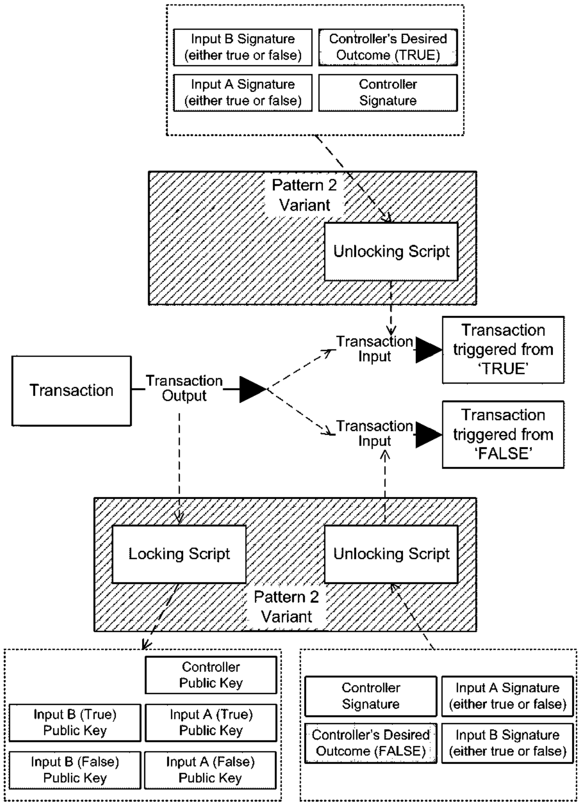
H04L 9/14	(2006.01)
G06Q 20/38	(2006.01)
G06Q 20/36	(2006.01)
G06F 21/64	(2006.01)
G06F 21/30	(2006.01)
H04W 4/70	(2006.01)
G06Q 20/06	(2006.01)
H04L 9/06	(2006.01)
H04L 9/32	(2006.01)
H04L 9/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/14*** (2013.01); ***G06F 21/305*** (2013.01); ***G06F 21/645*** (2013.01); ***G06Q 20/36*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/389*** (2013.01); ***G06Q 20/0658*** (2013.01); ***G06Q 20/3829*** (2013.01); ***H04L 9/0637*** (2013.01); ***H04L 9/0643*** (2013.01); ***H04L 9/0861*** (2013.01); ***H04L 9/3263*** (2013.01); ***H04W 4/70*** (2018.02); *H04L 9/50* (2022.05)

(57) **ABSTRACT**

This invention relates generally to distributed ledger technology (including blockchain related technologies), particularly a method and corresponding system for providing a blockchain transaction comprising a redeem script for an output that comprises: i) a plurality of public keys, each associated with a corresponding private key, wherein each public key is uniquely associated with a potential state of at least one data source; and ii) logic arranged to provide a result based on: A) a determination of which of the plurality of associated private key(s) is/are used to sign the unlocking script, so as to provide an interim result: and B) a comparison of a parameter supplied via the unlocking script against the interim result, and further attempting to spend the transaction output more than once, each attempt supplying a different parameter.


Input B Signature (either true or false)
Controller's Desired Outcome (TRUE)
Input A Signature (either true or false)
Controller Signature
Pattern 2 Variant
Unlocking Script
Transaction Input
Transaction triggered from 'TRUE'
Transaction
Transaction Output
Transaction Input
Transaction triggered from 'FALSE'
Locking Script
Unlocking Script
Pattern 2 Variant
Controller Public Key
Input B (True) Public Key
Input A (True) Public Key
Input B (False) Public Key
Input A (False) Public Key
Controller Signature
Input A Signature (either true or false)
Controller's Desired Outcome (FALSE)
Input B Signature (either true or false)