US011062303B2

(12) **United States Patent**
Maxwell

(10) **Patent No.: US 11,062,303 B2**
(45) **Date of Patent: *Jul. 13, 2021**

(54) **CRYPTOGRAPHICALLY CONCEALING AMOUNTS TRANSACTED ON A LEDGER WHILE PRESERVING A NETWORK'S ABILITY TO VERIFY THE TRANSACTION**

(71) Applicant: **Blockstream Corporation**, Montreal (CA)

(72) Inventor: **Gregory Maxwell**, Mountain View, CA (US)

(73) Assignee: **Blockstream Corporation**, Montreal (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 822 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/176,833**

(22) Filed: **Jun. 8, 2016**

(65) **Prior Publication Data**

US 2016/0358165 A1 Dec. 8, 2016

Related U.S. Application Data

(60) Provisional application No. 62/172,684, filed on Jun. 8, 2015.

(51) **Int. Cl.**
G06Q 20/38 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/3829*** (2013.01); *G06Q 2220/00* (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/3829; G06Q 20/0655; G06Q 2220/00; H04L 9/3255; H04L 9/3239; H04L 2209/38
USPC 705/71
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2004/0123110 A1 6/2004 Zhang et al.
2004/0260926 A1 12/2004 Modiane et al.
2009/0193250 A1 7/2009 Yokota et al.
(Continued)

OTHER PUBLICATIONS

Rivest et al. (How to Leak a Secret, C. Boyd (Ed.): ASIACRYPT 2001, LNCS 2248, pp. 552-565, 2001, © Springer-Verlag Berlin Heidelberg 2001) (Year: 2001).*
(Continued)

Primary Examiner — James D Nigh
(74) *Attorney, Agent, or Firm* — Dergosits & Noah LLP; Todd A. Noah

(57) **ABSTRACT**

Systems and methods are described for encrypting an amount transacted on a blockchain ledger, while preserving the transaction's ability to be verified. A blinding amount is added to an input value, and an output value is generated and encrypted. Both the input value and the output value are within a value range, where a sum of any two values within the range does not exceed an overflow threshold. The sum of the encrypted input value and the encrypted output value may equal zero. Rangeproofs associated with each of the input value and the output value are generated. The rangeproofs prove that the input value and the output value fall within the value range, and each rangeproof may be associated with a different public key. Each public key may be signed with a ring signature based on a public key of a recipient in the transaction.

19 Claims, 5 Drawing Sheets