US011080665B1

(12) **United States Patent**
Poelstra et al.

(10) **Patent No.: US 11,080,665 B1**
(45) **Date of Patent: *Aug. 3, 2021**

(54) **CRYPTOGRAPHICALLY CONCEALING AMOUNTS AND ASSET TYPES FOR INDEPENDENTLY VERIFIABLE TRANSACTIONS**

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

(72) Inventors: **Andrew Poelstra**, Austin, TX (US); **Gregory Maxwell**, Mountain View, CA (US); **Adam Back**, San Francisco, CA (US); **Pieter Wuille**, Mountain View, CA (US); **Mark Friedenbach**, San Jose, 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 184 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/894,793**

(22) Filed: **Feb. 12, 2018**

Related U.S. Application Data

(63) Continuation-in-part of application No. 15/176,833, filed on Jun. 8, 2016.
(Continued)

(51) **Int. Cl.**
G06Q 20/06 (2012.01)
G06Q 20/38 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/0658*** (2013.01); ***G06Q 20/3829*** (2013.01); *G06Q 2220/00* (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/0658; G06Q 20/3829; G06Q 2220/00
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0089494 A1* 4/2012 Danezis G06Q 50/06 705/34
2012/0296829 A1* 11/2012 Camenisch G06Q 30/0603 705/67

(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 amounts and asset types of a verifiable transaction on a blockchain ledger. For each asset, an asset tag is blinded, multiplied by the amount of the asset, and the product is blinded again to create an encrypted amount of the asset. Both encrypted amount of the asset and a corresponding generated output value are within a value range, and the sum of the encrypted input value and the encrypted output value equals zero. Rangeproofs for each of the encrypted output values are associated with a different public key. Each public key is signed with a ring signature based on a public key of a recipient. A second ring signature is used to verify each asset tag, where the private key of the second ring signature for each asset is a difference between a first blinding value and an output coefficient.

15 Claims, 10 Drawing Sheets