US010805090B1

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

(10) **Patent No.: US 10,805,090 B1**
(45) **Date of Patent: Oct. 13, 2020**

(54) **ADDRESS WHITELISTING USING PUBLIC/PRIVATE KEYS AND RING SIGNATURE**

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

(72) Inventors: **Andrew Poelstra**, Austin, TX (US); **Glenn Willen**, Mountain View, CA (US); **Gregory Maxwell**, Mountain View, CA (US); **Gregory Sanders**, Greenbelt, MD (US); **Jonas Nick**, Frankfurt (DE); **Matt Corollo**, New York City, NY (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 183 days.

(21) Appl. No.: **15/934,847**

(22) Filed: **Mar. 23, 2018**

Related U.S. Application Data

(60) Provisional application No. 62/476,168, filed on Mar. 24, 2017.

(51) **Int. Cl.**

H04L 9/32	(2006.01)
H04L 9/30	(2006.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3255*** (2013.01); ***H04L 9/3066*** (2013.01)

(58) **Field of Classification Search**
CPC . G06F 16/1805; G06F 21/64; H04L 2209/38; H04L 2209/56; H04L 9/3226;
(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.

(Continued)

Primary Examiner — Gary S Gracia
(74) *Attorney, Agent, or Firm* — Dergosits & Noah LLP; Todd A. Noah

(57) **ABSTRACT**

Systems and methods are described for transferring and verifying the transfer of an asset from a limited-participant side chain back to a main blockchain. A public difference, associated with a secret difference, is determined as a difference between a main blockchain address and the public offline key of a transferring participant. The public difference is used, along with each participant public online key, to generate a ring signature key for each participant. A ring signature is then generated over the ring signature keys, based on the public online keys and a set of uniform random scalars (each associated with a participant public online key). The main blockchain address, a first coefficient from the ring signature, and the uniform random scalars are then published. When verified, the published ring signature shows that the transferring participant has control of the main blockchain address and the private offline key.

13 Claims, 5 Drawing Sheets