US010812274B2

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

(10) **Patent No.: US 10,812,274 B2**
(45) **Date of Patent: Oct. 20, 2020**

(54) **TRANSFERRING LEDGER ASSETS BETWEEN BLOCKCHAINS VIA PEGGED SIDECHAINS**

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

(72) Inventors: **Adam Back**, Valletta (MT); **Gregory Maxwell**, Mountain View, CA (US); **Matt Corallo**, New York City, NY (US); **Luke Dashjr**, Tampa bay, FL (US); **Mark Friedenbach**, San Jose, CA (US); **Andrew Poelstra**, Austin, TX (US); **Jorge Timon**, San Francisco, CA (US); **Pieter Wuille**, 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 829 days.

(21) Appl. No.: **15/150,032**

(22) Filed: **May 9, 2016**

(65) **Prior Publication Data**

US 2016/0330034 A1 Nov. 10, 2016

Related U.S. Application Data

(60) Provisional application No. 62/158,432, filed on May 7, 2015.

(51) **Int. Cl.**
G06Q 20/00 (2012.01)
H04L 9/32 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 9/3255*** (2013.01); ***G06Q 20/06*** (2013.01); ***G06Q 20/065*** (2013.01);
(Continued)

(58) **Field of Classification Search**
USPC 705/64
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2016/0098723 A1* 4/2016 Feeney G06Q 20/4016 705/75
2018/0359096 A1* 12/2018 Ford H04L 9/3236

OTHER PUBLICATIONS

Andresen, G., BIP16: Pay to script hash, Bitcoin Improvement Proposal, 2012, https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

(Continued)

Primary Examiner — Jacob C. Coppola
Assistant Examiner — John M Winter
(74) *Attorney, Agent, or Firm* — Dergosits & Noah LLP; Todd A. Noah

(57) **ABSTRACT**

Systems and methods are described for transferring an asset from a parent chain to a sidechain. A simplified payment verification (SPV) proof associated with the parent chain asset may be generated. The SPV proof may include a threshold level of work. The SPV proof associated with the parent chain asset may be validated, and a sidechain asset corresponding to the parent chain asset may be generated. If no reorganization proof is detected, the sidechain asset is released. To redeem the sidechain asset in the parent chain, a SPV proof associated with the sidechain asset may be generated. The parent chain may validate the SPV proof associated with the sidechain asset. The parent chain asset associated with the sidechain asset may be held for a second predetermined contest period. The parent chain asset may then be released if no reorganization proof associated with the sidechain asset is detected.

13 Claims, 4 Drawing Sheets