

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

(10) **Patent No.:** **US 10,572,684 B2**
(45) **Date of Patent:** ***Feb. 25, 2020**

(54) **SYSTEMS AND METHODS FOR ENFORCING CENTRALIZED PRIVACY CONTROLS IN DE-CENTRALIZED SYSTEMS**

(71) Applicant: **Anonos Inc.**, New York, NY (US)
(72) Inventors: **Malcolm Gary LaFever**, Lyons, CO (US); **Ted N. Myerson**, New York, NY (US); **Steven Mason**, Las Vegas, NV (US)
(73) Assignee: **Anonos Inc.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.
This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/963,609**
(22) Filed: **Apr. 26, 2018**

(65) **Prior Publication Data**
US 2018/0307859 A1 Oct. 25, 2018

Related U.S. Application Data
(63) Continuation-in-part of application No. 15/483,997, filed on Apr. 10, 2017, now Pat. No. 10,043,035, (Continued)

(51) **Int. Cl.**
H04L 9/00 (2006.01)
G06F 21/62 (2013.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC **G06F 21/6254** (2013.01); **H04L 63/0407** (2013.01); **G06F 2221/2115** (2013.01); **H04L 63/068** (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/6254
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS

7,430,755 B1 9/2008 Hughes
7,454,356 B2 11/2008 Fields
(Continued)

FOREIGN PATENT DOCUMENTS

DE 19638072 A1 3/1998
EP 1154624 A2 11/2001
(Continued)

OTHER PUBLICATIONS

“We’ll see you, anon: Can big databases be kept both anonymous and useful?” The Economist, Apr. 15, 2015, available at <http://www.economist.com/news/science-and-technology/21660966-can-big-databases-be-kept-both-anonymous-and-useful-well-see-you-anon?fsrc=scn/tw/te/pe/ed/Wellseeyouanon>.
(Continued)

Primary Examiner — Josnel Jeudy
(74) *Attorney, Agent, or Firm* — Blank Rome LLP

(57) **ABSTRACT**
Systems, computer-readable media, and methods for improving both data privacy/anonymity and data value, wherein data related to a data subject can be used and stored, e.g., in a distributed ledger data structure, such as a blockchain, while minimizing re-identification risk by unauthorized parties and enabling data, including quasi-identifiers, related to the data subject to be disclosed to any authorized party by granting access only to the data relevant to that authorized party’s purpose, time period, place and/or other criterion via the obfuscation of specific data values, e.g., pursuant to the European Union’s General Data Protection Regulation (GDPR) or other similar regulatory schemes. The techniques described herein maintain this level of privacy/anonymity while still satisfying the immutability, auditability, and verification mandated by blockchain and other distributed ledger technologies (DLTs) for the decentralized storage of transactional data. Such systems, media,
(Continued)

