US 20230231727A1

(19) United States
(12) Patent Application Publication (10) Pub. No.: US 2023/0231727 A1
FLETCHER et al. (43) Pub. Date: Jul. 20, 2023

(54) **COMPUTER IMPLEMENTED METHOD AND SYSTEM FOR TRANSFERRING ACCESS TO A DIGITAL ASSET**

(71) Applicant: **nChain Licensing AG**, Zug (CH)

(72) Inventors: **John FLETCHER**, Cambridge (GB); **Thomas TREVETHAN**, London (GB)

(21) Appl. No.: **18/126,467**

(22) Filed: **Mar. 26, 2023**

Related U.S. Application Data

(62) Division of application No. 17/045,425, filed as application No. PCT/IB2019/052428 on Mar. 26, 2019, now Pat. No. 11,641,283.

(30) **Foreign Application Priority Data**

Apr. 5, 2018 (GB) 1805633.3

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3255*** (2013.01); ***H04L 9/085*** (2013.01); ***H04L 9/3066*** (2013.01); ***H04L 9/3236*** (2013.01); *H04L 9/50* (2022.05); *H04L 2209/56* (2013.01)

(57) **ABSTRACT**

A method of digitally signing a message is disclosed. The method comprises distributing first shares of a first secret value among a plurality of participants, wherein the first secret value is a private key accessible by means of a first threshold number of the first shares, and is inaccessible to less than the first threshold number of the first shares; distributing second shares of a second secret value among the participants, wherein the second secret value is an ephemeral key, wherein said ephemeral key is inaccessible to less than said first threshold number of said second shares; and distributing third shares of a third secret value among the participants, wherein each third share is adapted to be applied to a message to generate a respective fourth share of a fourth secret value, wherein the fourth secret value is the message signed with the private key and using the ephemeral key.