

Title (en)

DEVICE FOR STORING DIGITAL KEYS FOR SIGNING TRANSACTIONS ON A BLOCKCHAIN

Title (de)

VORRICHTUNG ZUM SPEICHERN VON DIGITALEN SCHLÜSSELN ZUM SIGNIEREN VON TRANSAKTIONEN AUF EINER BLOCKCHAIN

Title (fr)

DISPOSITIF DE STOCKAGE DE CLÉS NUMÉRIQUES POUR SIGNER DES TRANSACTIONS SUR UNE CHAÎNE DE BLOCS

Publication

EP 3707857 A1 20200916 (FR)

Application

EP 18833920 A 20181212

Priority

- FR 1762129 A 20171214
- FR 2018053211 W 20181212

Abstract (en)

[origin: WO2019115936A1] The invention relates to a physical device designed to store digital keys for carrying out transactions on a blockchain. The physical device (200) comprises a microphone (213), a loudspeaker (215), and a DSP processor (219) comprising a secured element in which the pairs of secret keys and public keys are stored, the DSP also comprising an acoustic codec using a dictionary S containing words that represent random or pseudo-random ultrasonic signals stored in the memory of the DSP. The DSP (219) is designed to decode a message consisting of words from S, received from an acoustic channel via the microphone (213), to sign the thus decoded message by means of a private key and to transmit the signature obtained in this way in the form of a response consisting of successive words from S, over said acoustic channel (250), via the loudspeaker (217).

IPC 8 full level

H04B 11/00 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP KR US)

G06Q 20/363 (2013.01 - US); **G06Q 20/3674** (2013.01 - US); **H04B 11/00** (2013.01 - EP US); **H04L 9/0643** (2013.01 - KR US); **H04L 9/0825** (2013.01 - US); **H04L 9/0869** (2013.01 - KR); **H04L 9/0894** (2013.01 - KR); **H04L 9/0897** (2013.01 - US); **H04L 9/3066** (2013.01 - KR US); **H04L 9/3215** (2013.01 - US); **H04L 9/3234** (2013.01 - EP KR US); **H04L 9/50** (2022.05 - KR); **H04L 9/50** (2022.05 - US)

Citation (search report)

See references of WO 2019115936A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

WO 2019115936 A1 20190620; AU 2018382778 A1 20200723; CN 111656732 A 20200911; EP 3707857 A1 20200916; FR 3075534 A1 20190621; FR 3075534 B1 20200110; JP 2021507586 A 20210222; KR 20200116455 A 20201012; US 2021073795 A1 20210311

DOCDB simple family (application)

FR 2018053211 W 20181212; AU 2018382778 A 20181212; CN 201880087464 A 20181212; EP 18833920 A 20181212; FR 1762129 A 20171214; JP 2020532556 A 20181212; KR 20207020393 A 20181212; US 201816771754 A 20181212