Title (en)

A METHOD FOR GENERATING RANDOM NUMBERS IN BLOCKCHAIN SMART CONTRACTS

Title (de)

VERFAHREN ZUR ERZEUGUNG VON ZUFALLSZAHLEN IN INTELLIGENTEN BLOCKCHAIN-VERTRÄGEN

Title (fr)

PROCÉDÉ DE GÉNÉRATION DE NOMBRES ALÉATOIRES DANS DES CONTRATS INTELLIGENTS À CHAÎNE DE BLOCS

Publication

EP 3912023 A4 20221012 (EN)

Application

EP 20741818 A 20200120

Priority

- US 201962794336 P 20190118
- CA 2020050056 W 20200120

Abstract (en)

[origin: WO2020146955A1] A method for generating fair and effective random numbers for smart contracts, which effectively mitigates certain problems associated with conventional methods while achieving verifiable and non-tamperable random number generation is disclosed. The concept behind the disclosed method treats miners as being not trustworthy, and presumes that the number of miners in the blockchain is limited. With sufficient motivation, miners can reach a consensus to manipulate the block. The goal is thus to create a verifiable fair Random Number Generator. Under this condition, as long as at least one of the parties to the smart contract is credible and does not misuse the confidential information, a trusted blockchain random number can be generated. After the last disclosure of the random number, the verification signature submitted by parties to the contract can be used to confirm that the random number calculation process is credible.

IPC 8 full level

G06F 7/58 (2006.01); **G06F 16/27** (2019.01); **G06F 21/64** (2013.01)

CPC (source: EP IL KR)

G06F 7/58 (2013.01 - EP IL KR); **G06F 16/9024** (2018.12 - EP IL KR); **G06F 21/64** (2013.01 - EP IL KR); **H04L 9/0662** (2013.01 - EP IL KR); **H04L 9/3239** (2013.01 - EP IL KR); **H04L 9/3247** (2013.01 - EP IL KR); **H04L 9/50** (2022.05 - EP KR); H04L 9/50 (2022.05 - IL)

Citation (search report)

- [I] WO 2018104728 A1 20180614 - QUANTA TECH LTD [GB]
- [I] RANDAO.ORG: "Randao: Verifiable Random Number Generation", 11 September 2017 (2017-09-11), pages 1 - 24, XP055590669, Retrieved from the Internet <URL:https://randao.org/whitepaper/Randao_v0.85_en.pdf> [retrieved on 20190521]
- [IP] CHATTERJEE KRISHNENDU ET AL: "Probabilistic Smart Contracts: Secure Randomness on the Blockchain", 2019 IEEE INTERNATIONAL CONFERENCE ON BLOCKCHAIN AND CRYPTOCURRENCY (ICBC), IEEE, 14 May 2019 (2019-05-14), pages 403 - 412, XP033572005, DOI: 10.1109/BLOC.2019.8751326
- See references of WO 2020146955A1

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

DOCDB simple family (publication)

WO 2020146955 A1 20200723; CA 3126956 A1 20200723; CN 113853578 A 20211228; EP 3912023 A1 20211124; EP 3912023 A4 20221012; IL 284876 A 20210831; JP 2022523643 A 20220426; KR 20210135495 A 20211115

DOCDB simple family (application)

CA 2020050056 W 20200120; CA 3126956 A 20200120; CN 202080014780 A 20200120; EP 20741818 A 20200120; IL 28487621 A 20210715; JP 2021541494 A 20200120; KR 20217025655 A 20200120