
AOMB Intellectual property

Jakub Sielewiesiuk

President of the Board
Polish and european
patent attorney

j.sielewiesiuk@aomb.pl

AOMB Intellectual property

Blockchain

How to patent blockchain-related innovations?

Case studies

AOMB intellectual property

What is blockchain?

Blockchain is a database.

Data in a database is stored in „containers" - blocks.

„Container" is of specified size (e.g. 1 MB) and structure.

Each block comprises main data and additionally – among others, a timestamp and a so called „hash" of the preceding block.

„Hash" = cryptographic abbreviation of content. It is similar to checksum – but is more sophisticated.

0x945eb660aee95fb571272530d363409d5770ecc0cf5831a889dfafd8d9fb3d74

What is blockchain?

Checksum – simple way to check if data is correct

PESEL:

The last digit of PESEL number is a control digit, which depends on all the preceding digits.

The method of calculating that control digit is publicly known – e.g.

http://www.algorytm.org/numery-identyfikacyjne/pesel.html

25 25 24 012 3 X

If the numbers preceding X change (by replacement by different ones or by changing their order) – the newly obtained sequence will not fit to X, so the numer will not be a correct PESEL number.

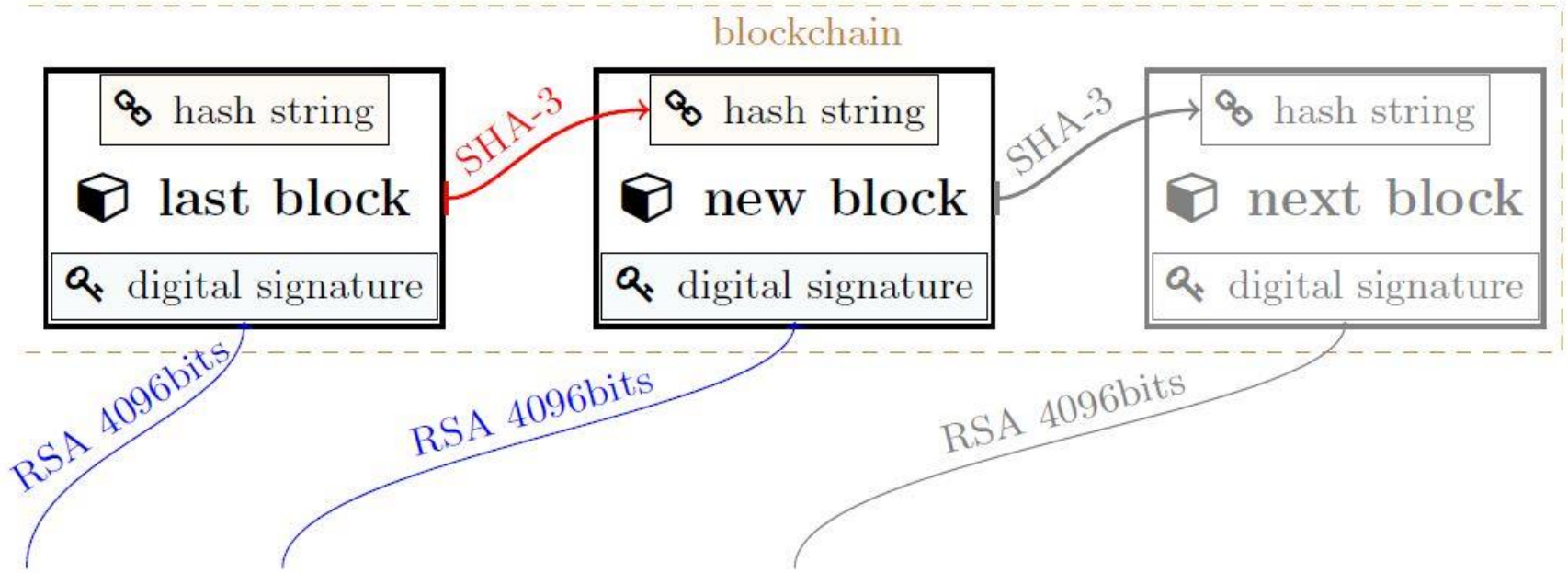
Bank account number (Poland): **72** 1140 1010 0000 4746 2300 1001

What is blockchain?

Blockchain is a database.

Each block comprises main data and additionally – among others, a timestamp and a so called „hash" of the **preceding** block.

0x945eb660aee95fb571272530d363409d5770ecc0cf5831a889dfafd8d9fb3d74

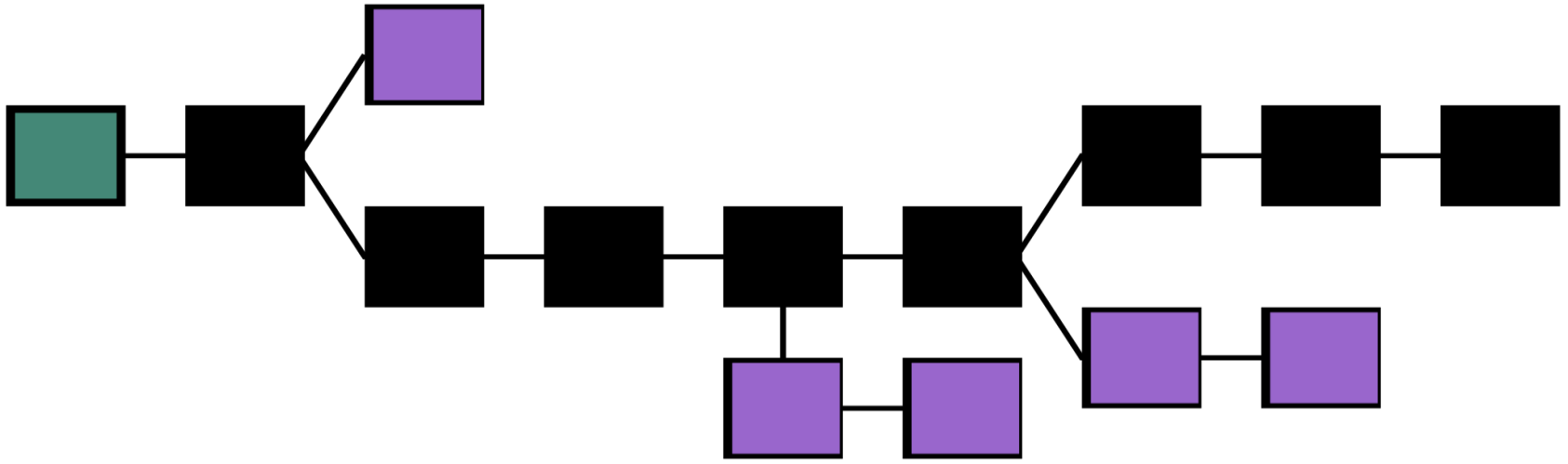


Source: EP 3 945 704 B1 „A method and a system for securing data, especially data of biotechnological laboratories"

What is blockchain?

Data change within Blockchain

Data change within Blockchain would either leave a trace (because the altered data would not correspond to the hash, so: it would be evident that data has been altered) or would require immense workload: it would be necessary to change the hash of the changed block, and in turns – necessary to change data in the next block, and then further for yet the next block etc. – for all subsequent blocks. And there are billions of blocks....



Source: https://pl.wikipedia.org/wiki/Blockchain

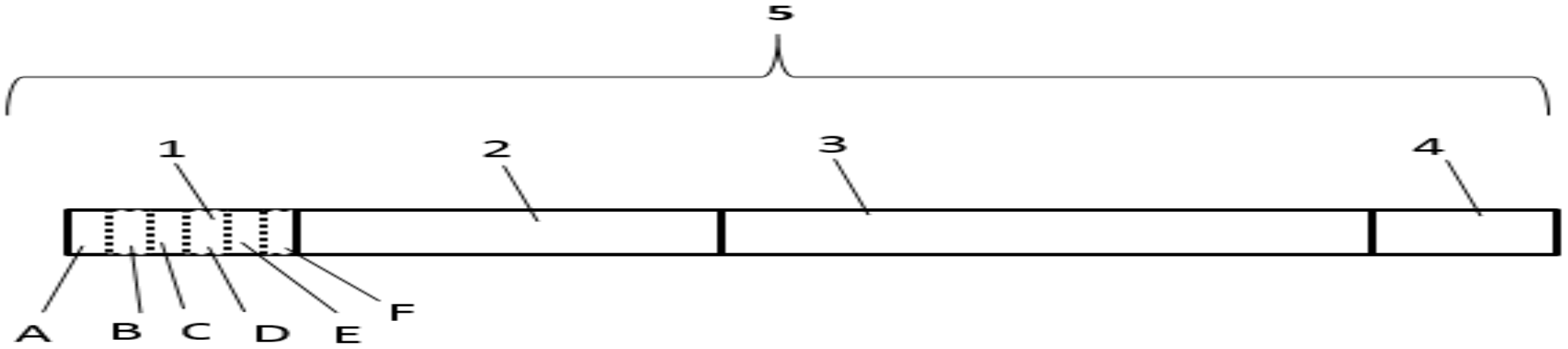
Example 1 – Trudatum

Example 1

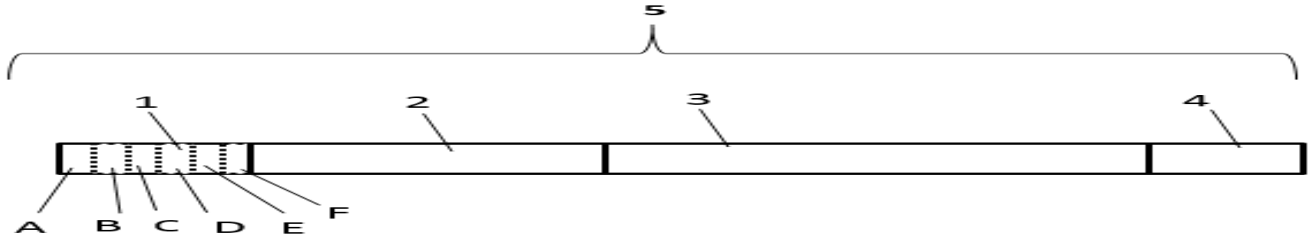
How to save any file („content") in blockchain, together with information of its source (proprietor) and a timestamp?

Answer: EP 3 579 496 B1 or US 10,944,548 B2 (or JP 7062838 B2)

„A method for registering of a data as digital file in a blockchain database"



Example 1 – Trudatum



Here is how to do it:

Make a data sequence comprising information about data (2), information about source (3), optionally a heading (1) and optionally a suffix (4), such that the length of the data sequence is a multiple of the size of the standard data container used in said blockchain database (e.g. 1 MB).

Divide the so obtained sequence into N parts of equal length.

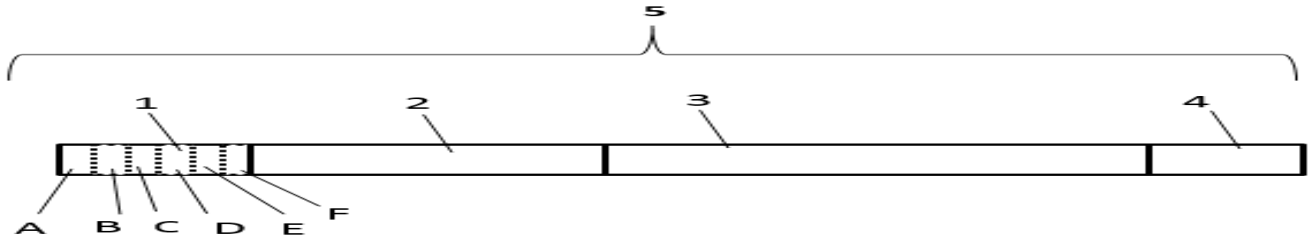
Generate N corresponding transactions, sign them electronically and save tchem in N containers in blockchain.

The heading (1) may include data concerning e.g. file version, file type, number of containers N, etc.

Information about data (2) – it may be the data itself or its hash.

Suffix (4) may include relevant or irrelevant data (like zero-digits only).

Example 1 – Trudatum



The heading (1) may include data concerning e.g. file version, file type, number of containers N, etc.

Information about data (2) – it may be the data itself or its hash.

Suffix (4) may include relevant or irrelevant data (like zero-digits only).

The data sequence in the frame may be different than 1-2-3-4.

Example 1 – Trudatum

1. A method for registering of a digital document as a digital file in a blockchain database, in which database transactions are constructed of standard data containers which may have a fixed size, in a system comprising one or more storage nodes for storing at least part of the blockchain database, one or more approval nodes for approving transactions in said blockchain database and a first computer for generating transactions in said blockchain database, said computer having access to said blockchain database and having access to a first private key, comprising the following steps:

a) providing a first set of data (2), relating to the contents of the digital file;

b) providing a second set of data (3), relating to the origin of the digital file;

c) generating a third set of data (5) by merging the first set of data (2), the second set of data (3), optionally a header (1) and optionally a suffix (4) into a data frame, wherein the header (1) may contain information about the structure of the third set of data, about the size of the first set of data (2), while the size of the suffix (4) is adjusted such that the size of the data frame is a multiple of the size of the standard data container used in said blockchain database;

Example 1 – Trudatum

… d) dividing the third set of data (5) into an integer number N≥1 of parts of equal size, said size corresponding to the size of the standard data container used in said blockchain database;

e) generating – by said first computer or an intermediary computer connected to the first computer and said one or more of the approval nodes – a single blockchain transaction for all the N parts obtained in the step d), signing the transaction by said first private key and sending the transaction and a first public key matching the said first private key to said one or more approval nodes for approval;

f) obtaining approval for the transaction from said one or more approval nodes;

g) registering the transaction approved in the step f) in a block of the blockchain database with a timestamp of registration by the one or more storage nodes,

wherein the second set of data (3) comprises a digital signature of a hash of the digital file and

wherein registering of the digital document as the digital file in the blockchain database is done by a first entity and the digital document is transmitted from the first entity to a second entity.

Example 1 – Trudatum

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) EP 3 579 496 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent: **07.10.2020 Bulletin 2020/41**

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

(21) Application number: **19159419.1**

(22) Date of filing: **26.02.2019**

(54) **A METHOD FOR REGISTERING OF A DATA AS DIGITAL FILE IN A BLOCKCHAIN DATABASE**

VERFAHREN ZUR REGISTRIERUNG VON DATEN ALS DIGITALE DATEI IN EINER BLOCKKETTENDATENBANK

PROCÉDÉ D'ENREGISTREMENT D'UNE DONNÉE SOUS FORME DE FICHIER NUMÉRIQUE DANS UNE BASE DE DONNÉES DE CHAÎNE DE BLOCS

(84) Designated Contracting States: **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**

(30) Priority: **07.06.2018 EP 18461565**
19.09.2018 EP 18195583

(43) Date of publication of application: **11.12.2019 Bulletin 2019/50**

(73) Proprietor: **Coinfirm Blockchain Lab Sp. z o.o.**
87-100 Torun (PL)

(72) Inventors:
- **ALEKSANDER, Pawel, Zygmunt**
  88-150 Kobylniki (PL)
- **KUSKOWSKI, Pawel**
  87-400 Golub-Dobrzyn (PL)
- **FIJOLEK, Jakub**
  85-034 Bydgoszcz (PL)

(74) Representative: **AOMB Polska Sp. z.o.o.**
Ul. Emilii Plater 53
21st Floor
00-113 Warsaw (PL)

(56) References cited:
US-A1- 2016 283 920 US-A1- 2018 139 056

- **ZHENG PEILIN ET AL: "A Detailed and Real-Time Performance Monitoring Framework for Blockchain Systems", 2018 IEEE/ACM 40TH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING: SOFTWARE ENGINEERING IN PRACTICE TRACK (ICSE-SEIP), ACM, 25 May 2018 (2018-05-25), pages 134-143, XP033396280,**
- **PASQUALE FORTE ET AL: "Beyond Bitcoin - Part I: A critical look at blockchain-based systems", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20151202:213043, 1 December 2015 (2015-12-01), pages 1-34, XP061019757,**
- **GIPP BELA ET AL: "CryptSubmit: Introducing Securely Timestamped Manuscript Submission and Peer Review Feedback Using the Blockchain", 2017 ACM/IEEE JOINT CONFERENCE ON DIGITAL LIBRARIES (JCDL), IEEE, 19 June 2017 (2017-06-19), pages 1-4, XP033131302, DOI: 10.1109/JCDL.2017.7991588**

Printed by Jouve, 75001 PARIS (FR)

EP 3 579 496 B1

US010944548B2

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

(10) **Patent No.: US 10,944,548 B2**
(45) **Date of Patent: *Mar. 9, 2021**

(54) **METHOD FOR REGISTRATION OF DATA IN A BLOCKCHAIN DATABASE AND A METHOD FOR VERIFYING DATA**

(71) Applicant: **Coinfirm Blockchain Lab Sp. Zo.o.**, Torun (PL)

(72) Inventors: **Pawel Zygmunt Aleksander**, Kobylniki (PL); **Pawel Kuskowski**, Golub-Dobrzyn (PL); **Jakub Fijolek**, Bydgoszcz (PL)

(73) Assignee: **COINFIRM BLOCKCHAIN LAB SP. Z O.O.**, Torun (PL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 229 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/231,367**

(22) Filed: **Dec. 21, 2018**

(65) **Prior Publication Data**

US 2019/0379531 A1 Dec. 12, 2019

(30) **Foreign Application Priority Data**

Jun. 7, 2018 (EP) 18461565
Sep. 19, 2018 (EP) 18195583

(51) **Int. Cl.**
H04L 9/06 (2006.01)
G06F 16/23 (2019.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 9/0637*** (2013.01); ***G06F 16/152*** (2019.01); ***G06F 16/2379*** (2019.01);
(Continued)

(58) **Field of Classification Search**
CPC .. G06F 16/2365; G06F 16/2379; G06F 9/466; G06F 16/152; H04L 9/0643;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,417,188 B2 * 9/2019 King G06F 16/1752
2008/0247470 A1 * 10/2008 Wang H04L 1/006 375/241

(Continued)

OTHER PUBLICATIONS

Pasquale Forte et al., "Beyond Bitcoin—Part I: A critical look at blockchain-based systems", International Association for Cryptologic Research, vol. 20151202:213043, Dec. 1, 2015, pp. 1-34.

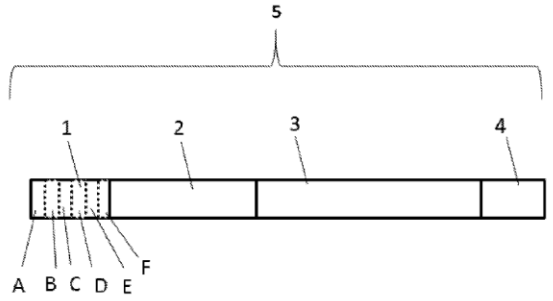
(Continued)

Primary Examiner — Hares Jami
(74) *Attorney, Agent, or Firm* — Masuvalley & Partners

(57) **ABSTRACT**

The invention comprises a method for registration of data in a blockchain database, in which database transactions are constructed of standard data containers which may have a fixed size, in a system comprising one or more storage nodes for storing at least part of the blockchain database, one or more approval nodes for approving transactions in said blockchain database and a first computer for generating transactions in said blockchain database, said computer having access to said blockchain database and having access to a first private key. The invention further comprises a method for verifying data based on the aforementioned method for registration and an application of these methods to handle a selected type of document. The invention also comprises a computer program product comprising program code stored on a computer readable medium, said program code comprising computer instructions for performing these methods.

18 Claims, 1 Drawing Sheet



JP 7062838 B2 2022.5.6

(19)日本国特許庁(JP)

(12)特 許 公 報(B2)

(11)特許番号
特許第7062838号
(P7062838)

(45)発行日 令和4年5月6日(2022.5.6)

(24)登録日 令和4年4月22日(2022.4.22)

(51)Int.Cl.
G06F 21/64 *(2013.01)*
G06Q 20/38 *(2012.01)*

F I
G06F 21/64
G06Q 20/38 310

請求項の数 19 (全 24 頁)

(21)出願番号 特願2021-515274(P2021-515274)
(86)(22)出願日 平成31年3月14日(2019.3.14)
(65)公表番号 特表2021-524978(P2021-524978A)
(43)公表日 令和3年9月16日(2021.9.16)
(86)国際出願番号 PCT/EP2019/056460
(87)国際公開番号 WO2019/233646
(87)国際公開日 令和1年12月12日(2019.12.12)
審査請求日 令和2年11月25日(2020.11.25)
(31)優先権主張番号 18461565.6
(32)優先日 平成30年6月7日(2018.6.7)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)
(31)優先権主張番号 18195583.2
(32)優先日 平成30年9月19日(2018.9.19)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者 520462089
コインファーム ブロックチェーン ラボ エスペー・ゾオ
COINFIRM BLOCKCHAIN LAB SP. Z. O. O.
ポーランド国 トルン 87-100 シ ョーザ チェルミンスカ 71
(74)代理人 100163991
弁理士 加藤 慎司
(72)発明者 アレクサンダー, パヴェル ジグムント
ポーランド国 コビルニキ 88-150 コビルニキ 32 エム5
(72)発明者 クスコウスキー, パヴェル
ポーランド国 ゴルゾードブジン 87-400 ドゥルヴェツカ 15

最終頁に続く

(54)【発明の名称】ブロックチェーンデータベースにデータをデジタルファイルとして登録する方法

(57)【特許請求の範囲】

【請求項１】

ブロックチェーンデータベースにデジタルドキュメントをデジタルファイルとして登録する方法であって、データベーストランザクションは固定サイズを有し得る標準データコンテナで構成され、前記ブロックチェーンデータベースの少なくとも一部を格納するための１つ又は複数の格納ノードと、前記ブロックチェーンデータベース内のトランザクションを承認するための１つ又は複数の承認ノードと、前記ブロックチェーンデータベース内のトランザクションを生成するための第１のコンピュータとを含んだシステムにおいて、前記第１のコンピュータは前記ブロックチェーンデータベースへのアクセスを有し、且つ、第１の秘密鍵へのアクセスを有しており、

ａ）前記デジタルファイルの内容に関する第１のデータセット（２）を提供する工程と；

ｂ）前記デジタルファイルの出所に関連する第２のデータセット（３）を提供する工程と；

ｃ）第１のデータセット（２）、第２のデータセット（３）、ヘッダ（１）、及びサフィックス（４）をデータフレームに統合することによって第３のデータセット（５）を生成する工程であって、前記ヘッダ（１）は、前記第３のデータセットの構造に関する及び前記第１のデータセットのサイズに関する情報を含んでいてもよく、一方、前記サフィックス（４）のサイズは、前記データフレームのサイズが前記ブロックチェーンデータベースで使用される前記標準データコンテナのサイズの倍数になるように調整される工程と；

ｄ）前記第３のデータセット（５）を整数Ｎ≧１個の同一サイズの部分に分割する工程で

https://worldwide.espacenet.com/patent/search/family/065598536/publication/EP3579496B1?q=EP3579496B

Example 1 – Trudatum

Technologia blockchain ułatwi weryfikację dokumentów bankowych

2018.03.27

PKO Bank Polski oraz start-up Coinfirm podpisały umowę o współpracy. Jest to kolejny etap realizacji cyfrowej strategii banku. Platforma blockchain Trudatum została stworzona, by dostarczyć instytucjom finansowym nowe rozwiązania weryfikujące autentyczność danych. Dotychczasowe testy potwierdziły możliwości integracji tej technologii z istniejącą infrastrukturą banku w wielu ważnych obszarach biznesowych. Nad rozwojem technologii pracować będzie nowo powołane Centrum Kompetencyjne Blockchain PKO Banku Polskiego.

- **PKO Bank Polski oraz start-up Coinfirm podpisały umowę o współpracy. Bank jako pierwsza polska instytucja finansowa rozpoczęła wdrożenie rozwiązań w technologii blockchain.**

https://media.pkobp.pl/70784-technologia-blockchain-ulatwi-weryfikacje-dokumentow-bankowych

wprost BIZNES OPINIE TWÓJ PORTFEL GOSPODARKA FINANSE FIRMY TECHNOLOGIE NAJBOGATSI SUBSKRYBUJ

Wprost / Biznes / Finanse i inwestycje / Waluty

PKO BP i Coinfirm tworzą historię finansów

Dodano: 21 lipca 2017 18:23

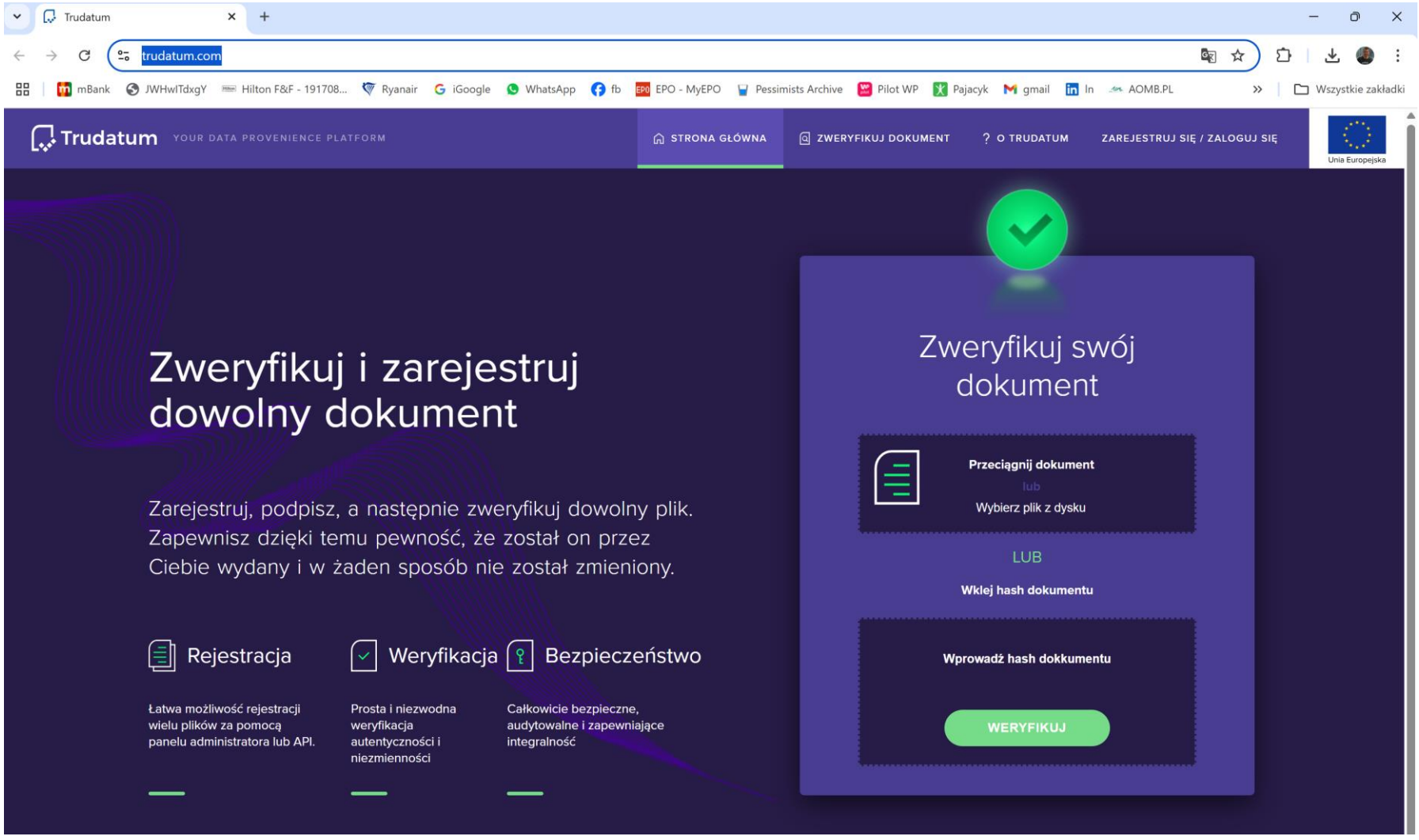
trudatum - pierwsze zastosowanie blockchain w polskim banku

Reklamy Google
Prześlij opinię
Dlaczego ta reklama?

Bank właśnie rozpoczął testowanie trudatum, platformy stworzonej przez polsko-brytyjską firmę Coinfirm, tworząc tym samym nowy standard w bezpieczeństwie i weryfikacji dokumentów. To kolejny przełom w drodze nowej technologii do centrum świata finansów. PKO jest jedną z pierwszych instytucji finansowych na świecie,

https://biznes.wprost.pl/finanse-i-inwestycje/waluty/10066438/pko-bp-i-coinfirm-tworza-historie-finansow.html

Example 1 – Trudatum



https://www.trudatum.com/

Example 2 – Travel Rule

Example 2

How to provide secure transfer of data to an addressee, through a distrusted environment, with no reliable third-party? And in line with Finacial Action Task Force (FATF) rules regarding prevention of money laundering and financing of terrorism.

Answer: EP 3 799 352 A1 or US 11,405,188 B2

„A method for secure transferring of information through a network between an origin Virtual Asset Service Provider and a destination Virtual Asset Service Provider"

The addressee is able to cryptographically prove entitlement to the transferred data.

Example 2 – Travel Rule

…. 0a) Registering an asset owner, having an owner cryptocurrency private key and an owner cryptocurrency public key, with the destination VASP (VASP Z, RV),

0b) Creating an owner cryptocurrency address as a function of the owner cryptocurrency public key, preferably base58 hash160 with metadata and checksum, and depositing the owner cryptocurrency address in a database accessible to the destination VASP (VASP Z, RV),

0c) Creating a proof of ownership (POO) comprising as the first contents: the owner cryptocurrency address and the destination VASP network public key and **comprising a first signature of said first contents generated as a function of the owner cryptocurrency private key**, preferably generated using the Elliptic Curve Digital Signature Algorithm, ECDSA,

0d) Storing the proof of ownership (POO) in a database accessible to the destination VASP (VASP Z, RV)

… followed by the sequence of querries and responses + challenge-response leading to determination of the proper addressee (receiver)….

Example 2 – Travel Rule

MSG 2

POO

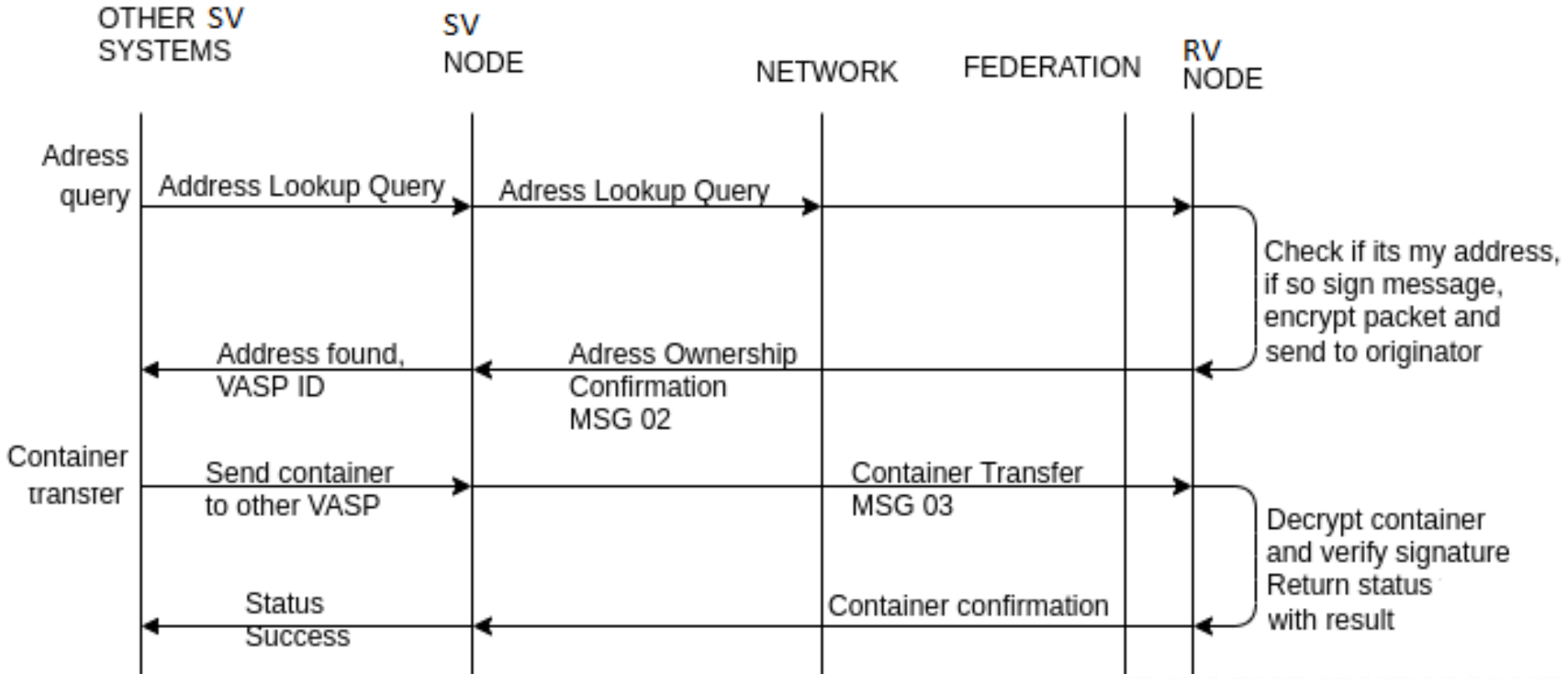
Crytpocurrency Address

VASP Z Network Public Key

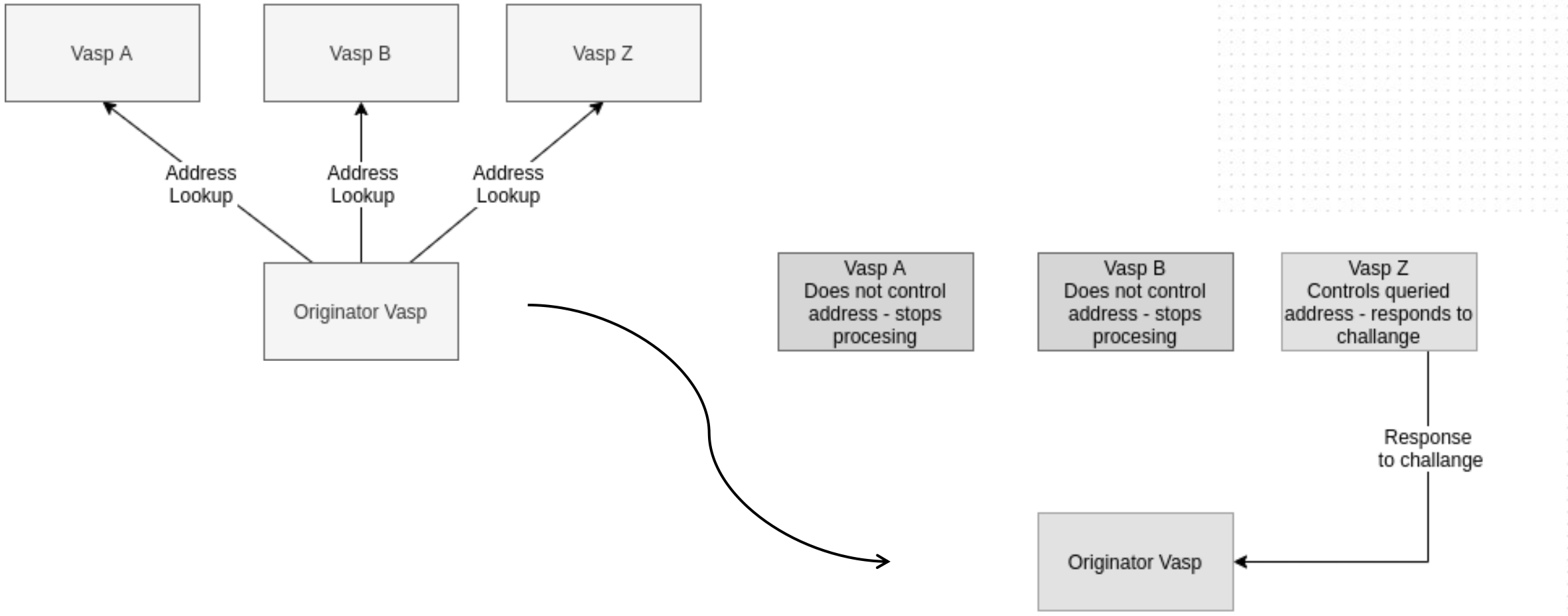
Signature no.1 Created using cryptocurrency private key inline with ECDSA

Challange provided by Originator VASP

Signature no.2 created using VASP Z Network Private key



Example 2 – Travel Rule



Example 2 – Travel Rule

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 799 352 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.03.2021 Bulletin 2021/13

(51) Int Cl.:
H04L 9/32 (2006.01)

(21) Application number: 20199469.6

(22) Date of filing: 30.09.2020

(84) Designated Contracting States:
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 States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: 30.09.2019 EP 19200574

(71) Applicant: Coinfirm Limited
London W1J 6ER (GB)

(72) Inventors:
- Fijolek, Jakub
85-034 Bydgoszcz (PL)
- Kuskowski, Pawel
87-400 Golub-Dobrzyn (PL)
- Aleksander, Pawel Zygmunt
88-150 Kobylniki (PL)

(74) Representative: AOMB Polska Sp. z.o.o.
Ul. Emilii Plater 53
21st Floor
00-113 Warsaw (PL)

(54) **A METHOD FOR SECURE TRANSFERRING OF INFORMATION THROUGH A NETWORK BETWEEN AN ORIGIN VIRTUAL ASSET SERVICE PROVIDER AND A DESTINATION VIRTUAL ASSET SERVICE PROVIDER**

(57) The invention is related to a method for secure transferring of information through a network between an origin Virtual Asset Service Provider and a destination Virtual Asset Service Provider, in a hostile environment, where every entity (party member, network node) must proof its entitlement of the information being exchanged. Hostile environment means that neither any entity/network node nor the network as a whole can be trusted. The present method doesn't require other party member/network node or database to secure information transfer. Neither it requires any other trusted entity or server to guarantee or provide proof of ownership of exchange information. The present method for communicating securely between electronic devices uses asymmetric key encryption.

The invention comprises also a computer program product comprising program code stored on a computer readable medium, said program code comprising computer instructions for performing the inventive method.

The invention relates also to a system configured and programmed for performing the inventive method.

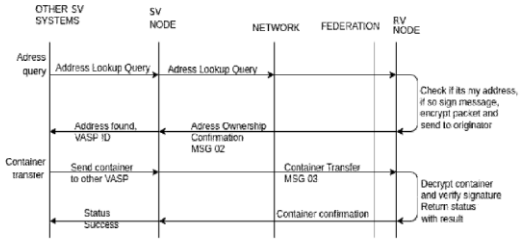


Fig. 1

EP 3 799 352 A1

US011405188B2

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

(10) Patent No.: US 11,405,188 B2
(45) Date of Patent: Aug. 2, 2022

(54) **METHOD FOR SECURE TRANSFERRING OF INFORMATION THROUGH A NETWORK BETWEEN AN ORIGIN VIRTUAL ASSET SERVICE PROVIDER AND A DESTINATION VIRTUAL ASSET SERVICE PROVIDER**

(71) Applicant: **COINFIRM LIMITED**, London (GB)

(72) Inventors: **Pawel Zygmunt Aleksander**, Kobylniki (PL); **Pawel Kuskowski**, Golub-Dobrzyn (PL); **Jakub Fijolek**, Bydgoszcz (PL)

(73) Assignee: **COINFIRM LIMITED**, London (GB)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 79 days.

(21) Appl. No.: **17/039,639**

(22) Filed: **Sep. 30, 2020**

(65) **Prior Publication Data**

US 2021/0099293 A1 Apr. 1, 2021

(30) **Foreign Application Priority Data**

Sep. 30, 2019 (EP) 19200574

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 9/0825*** (2013.01); ***H04L 9/0643*** (2013.01); ***H04L 9/3236*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC ... H04L 9/0825; H04L 9/0643; H04L 9/3236; H04L 9/3247; H04L 9/3271; H04L 2209/38; H04L 2209/56; H04L 9/3239
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,498,542 B2 * 12/2019 Ebrahimi G06Q 20/3827
10,587,609 B2 * 3/2020 Ebrahimi H04L 63/061
(Continued)

FOREIGN PATENT DOCUMENTS

AU 2015389877 A1 * 10/2017 ..... G06Q 20/065
CA 3008705 C * 3/2020 ..... G06F 16/137
(Continued)

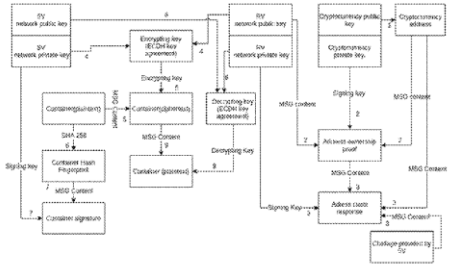
Primary Examiner — Sher A Khan
(74) *Attorney, Agent, or Firm* — Masuvalley and Partners; Peter R. Martinez

(57) **ABSTRACT**

The invention is related to a method for secure transferring of information through a network between an origin Virtual Asset Service Provider and a destination Virtual Asset Service Provider, in a hostile environment, where every entity (party member, network node) must proof its entitlement of the information being exchanged. Hostile environment means that neither any entity/network node nor the network as a whole can be trusted. The present method doesn't require other party member/network node or database to secure information transfer. Neither it requires any other trusted entity or server to guarantee or provide proof of ownership of exchange information. The present method for communicating securely between electronic devices uses asymmetric key encryption.

The invention comprises also a computer program product comprising program code stored on a non-transitory computer readable medium, said program code comprising computer instructions for performing the inventive method.

15 Claims, 5 Drawing Sheets



https://worldwide.espacenet.com/patent/search/family/068109128/publication/EP3799352A1?q=ep3799352

AOMB is member of AIPEX

Jakub Sielewiesiuk

President of the Board
Polish and european
patent attorney

j.sielewiesiuk@aomb.pl

AOMB Intellectual property