47 Documents

Publication numbers	Title	Current assignees
US20180285217 A1	Failover response using a known good state from a distributed ledger	INTEL
IN201847033629 A	Method and system for efficient transfer of cryptocurrency associated with a payroll on a blockchain that leads to an automated payroll method and system based on smart contracts	NCHAIN HOLDINGS
US20180287915 A1	Systems and methods for fair information exchange using publish-subscribe with blockchain	INTEL
WO2018182861 A1	Systems and methods for fair information exchange using publish-subscribe with blockchain	INTEL
US20180285996 A1	Methods and system for managing intellectual property using a blockchain	FUTURELAB CONSULTING
US20180287780 A1	Blockchain verification of network security service	GENERAL ELECTRIC
DE102018104637 A1	FAIL-SAFE RESPONSE USING AN KNOWN GOOD STATE OF AN DECENTRAL GUIDED ACCOUNT BOOK	INTEL
IN201847033324 A	A method and system for securing computer software using a distributed hash table and a blockchain	NCHAIN HOLDINGS
EP3382591 A1	Hierarchical temporal memory for expendable access control	BT
US20180287893 A1	Consumption-based licensing of network features based on blockchain transactions	CISCO TECHNOLOGY
US20180285971 A1	Management of consumer debt collection using a blockchain and machine learning	IBM
WO2018183307 A1	Method and system for identity and access management for blockchain interoperability	Madisetti Dr. Vijay
US20180287797 A1	Distributed logging of application events in a blockchain	IBM
US20180285979 A1	Creating service agreements via blockchain smart contracts	IBM
US20180285810 A1	Systems and methods of blockchain transaction recordation in a food supply chain	RIPE TECHNOLOGY
IN201847033271 A	A method and system for the secure transfer of entities on a blockchain	NCHAIN HOLDINGS
WO2018183768 A1	Trusted food traceability system and method and sensor network	INNIT INTERNATIONAL
US20180285866 A1	Method for producing a cryptographical signed transaction	CCC GROUP
US20180285839 A1	Providing data provenance, permissioning, compliance, and access control for data storage systems using an immutable ledger overlay network	DATIENT
US20180285479 A1	Scalable audit analytics	SUPERNA
WO2018178026 A1	Hierarchical temporal memory for access control	BT

Publication numbers	Title	Current assignees
CN108596617 A	Based on algorithm type of block chain method and a device for sensing an attack event	QIHOO 360 TECHNOLOGY
US20180285970 A1	Due Diligence in Mortgage Documents	FACTOM
US20180285867 A1	Distributed auditing method, device and system	TIDETIME SUN
WO2018176140 A1	Systems and methods for executing and delivering electronic documents	SYNGRAFII
US20180285983 A1	Scalable and distributed shared ledger transaction management	IBM
US20180285838 A1	Scalable and distributed shared ledger transaction management	IBM
US20180284747 A1	Methods and systems for industrial internet of things data collection for equipment analysis in an upstream oil and gas environment	STRONGFORCE IOT PORTFOLIO 2016
WO2018177520 A1	Method of operating an electrical grid	INNOGY
WO2018183033 A1	System and method for presenting content on client devices	COGNANT
CN108600227 A	Medical data sharing method based on a block chain and a device	ZHONG AN INFORMATION TECHNOLOGY SERVICES
WO2018183351 A1	Architectures and systems for managing personal data to be utilized by dynamic sets of external parties	UNISCEN
WO2018183564 A1	Systems and methods for storing electrical energy	OJAI ENERGETICS PBC
WO2018182903 A1	Cloud assisted machine learning	INTEL
US20180287806 A1	Securing communications	Carboni Davide, ...
US20180285767 A1	Cloud assisted machine learning	INTEL
EP3382928 A2	Securing communications	INTEL
WO2018177603 A1	Providing payment options without requiring online shop integration	AVAST SOFTWARE S R O
WO2018176100 A1	A computer system and a computer implemented method for processing gaming data	GEO PRO TEQ IP
US20180288041 A1	Seamless Authentication Device	AT&T
WO2018178878 A1	Biometric authentication for, and secure electronic tracking of, restricted over-the-counter drug sales	BAYER HEALTHCARE
WO2018178028 A1	Initialisation vector identification for encrypted malware traffic detection	BT
WO2018178027 A1	Intialisation vector identification for malware file detection	BT
WO2018183831 A1	Image data integrator for addressing congestion	Burinska Patrizia, ...
US20180285549 A1	Authorization of virtual reality interactions using controlled randomization	Aggarwal Sumiran, ...
US20180285709 A1	Transponder-unit for facilitating authorization associated with an article	Braunstein Kim

Publication numbers	Title	Current assignees
US20180285882 A1	Activity management systems and methods	BATON SYSTEMS

Family 1/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

US20180285217

Application dates

2017-03-31

Publication dates

2018-10-04

Title

(US20180285217)

Failover response using a known good state from a distributed ledger

Abstract

(US20180285217)

Techniques for repair and/or recovery of computer program(s) installed on a programmable device using a distributed ledger that is based on cryptography and blockchain technology are described.One or more self-reliance logic/modules can commit, to a distributed ledger that resides on interconnected devices, records of watchdog communications between the devices.One or more of interconnected devices may include a respective self-reliance logic/module.The logic/modules can use the records of the distributed ledger to check that computer program(s) on the interconnected devices are operating as expected.When a self-reliance logic/module fails to respond to a watchdog communication, the distributed ledger can be updated to include this failure.A self-reliance logic/module can determine, based on the distributed ledger and/or the failure, that an installed computer program is faulty.Furthermore, a self-reliance logic/module can initiate one or more software recovery services based on the determination.Other advantages and embodiments are described.

Family 2/47 - FAMPAT - ©Questel

Current assignees

NCHAIN HOLDINGS

Publication numbers

IN201847033383

IN201847033629

Application dates

2018-09-05

2018-09-07

Publication dates

2018-09-28

2018-09-28

Title

(IN201847033383)

Method and system for efficient transfer of cryptocurrency associated with a payroll on a blockchain that leads to an automated payroll method and system based on smart contracts

Abstract

(IN201847033383)

The invention relates to blockchain technologies such as the Bitcoin blockchain, and the tokenisation of assets or entities.It is particularly suited for implementing a payroll on a blockchain platform and comprises a method (100) and system (1) of transferring cryptocurrency from a first node (3) to a second node (7).Both nodes (3, 7) are associated with a payroll and have a respective asymmetric cryptography pair, each pair including a master private key and a master public key.Respective additional private and public keys may be determined based on the master private key, master public key and a generator value at each node.The additional private and public keys may form a hierarchical structure.A common secret may be determined at each of the nodes (3, 7) based on the additional private and public keys.The common secret

may be used to securely transmit confidential information across a communications network (5).

Family 3/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

US20180287915

Application dates

2017-03-31

Publication dates

2018-10-04

Title

(US20180287915)

Systems and methods for fair information exchange using publish-subscribe with blockchain

Abstract

(US20180287915)

Methods, apparatus, systems and articles of manufacture are disclosed to facilitate information exchange using publish-subscribe with blockchain.An example apparatus includes a broker including a processor and a distributed ledger module.The example distributed ledger module stores a message to be relayed by the broker from a publisher to a subscriber.The example processor is to at least compute, triggered by receipt of the message by the broker, a proof-of-work (PoW) function.The example processor is to at least verify the computation of the PoW function.The example processor is to at least transmit, upon verifying the computation of the PoW function, the message to the subscriber.The example processor is to at least process feedback received by the broker to update the PoW function.

Family 4/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

WO2018/182861

Application dates

2018-02-12

Publication dates

2018-10-04

Title

(WO2018182861)

Systems and methods for fair information exchange using publish-subscribe with blockchain

Abstract

(WO2018182861)

Methods, apparatus, systems and articles of manufacture are disclosed to facilitate information exchange using publish-subscribe with blockchain.An example apparatus includes a broker including a processor and a distributed ledger module.The example distributed ledger module stores a message to be relayed by the broker from a publisher to a subscriber.The example processor is to at least compute, triggered by receipt of the message by the broker, a proof-of-work (PoW) function.The example processor is to at least verify the computation of the PoW function.The example processor is to at least transmit, upon verifying the computation of the PoW function, the message to the subscriber.The example processor is to at least process feedback received by the broker to update the PoW function.

Family 5/47 - FAMPAT - ©Questel

Current assignees

FUTURELAB CONSULTING

Publication numbers

US20180285996

Application dates

2018-04-02

Publication dates

2018-10-04

Title

(US20180285996)

Methods and system for managing intellectual property using a blockchain

Abstract

(US20180285996)

A system and methods for managing intellectual property using a blockchain are provided which may include one or more elements which forms a comprehensive foundation for an eco-system for innovation and intellectual property management.The elements may include: an intellectual property distributed ledger, an intellectual property digital policy server, non-binary trust models, automatic ontology induction, modifications to the blockchain “mining” and “proof of work” system, appstore for related applications, partial transparency transactionalized search engine, persistent and encapsulated software trust objects, licensing royalty smart contract with auditable payment tracking, micro-equity incentives, automated fraud detection intellectual property management dashboards, innovation workflow broker, innovation optimization tools, disruption mapping, and intelligent just-in-time learning.The system combines and integrates these functions to enable personal, intra-enterprise, inter-enterprise and extra-enterprise recordation, collaboration, searchability and its benefits, licensing and tracking of information regarding intellectual property over a networked distributed computing system.

Family 6/47 - FAMPAT - ©Questel

Current assignees

GENERAL ELECTRIC

Publication numbers

US20180287780

Application dates

2017-03-28

Publication dates

2018-10-04

Title

(US20180287780)

Blockchain verification of network security service

Abstract

(US20180287780)

According to some embodiments, a system may include a communication port to exchange information with a client device associated with an industrial control system.A network security server coupled to the communication port may include a computer processor adapted to provide a network security service for the client device.The computer processor may further be adapted to record security information about the client device via a blockchain verification process (e.g., by registering a validation result within a distributed ledger).The network security service might comprise, for example, an integrity attestation service providing software verification for the client device.

Family 7/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

DE102018104637

Application dates

2018-02-28

Publication dates

2018-10-04

Title

(DE102018104637)

FAIL-SAFE RESPONSE USING AN KNOWN GOOD STATE OF AN DECENTRAL GUIDED ACCOUNT BOOK

Abstract

(DE102018104637)

Techniques for repair and/or restoration of computer program installed on a programmable device (en) using a guided account book in a decentralized manner (Distributed Ledger), and block chains based on cryptography technology, are described.A (e) or more autonomy logics / - module may, in a decentralized manner on a guided account book, on the devices connected to each other is located, records of monitoring communications between the devices is transferred.One or more interconnected devices can be a (e) corresponding (s) independence to logic / - module include.The logic/modules the records can be guided in a decentralized manner using the account book, in order to check, whether the one or more computer programs on the devices connected to each other are operating as expected.If a (e) independence to logic / - module fails, to respond to a monitoring communication, the book account maintained in a decentralized manner to be updated may be, in order to be able to include this error.A (e) independence logic / - module may determine, based on the guided account book and/or the error in a decentralized manner, a computer program installed is faulty that a.One can also use independence to logic / - module based on the determination to initiate one or more software recovery services.Other advantages and embodiments are described.

Family 8/47 - FAMPAT - ©Questel

Current assignees

NCHAIN HOLDINGS

Publication numbers

IN201847033324

Application dates

2018-09-05

Publication dates

2018-09-28

Title

(IN201847033324)

A method and system for securing computer software using a distributed hash table and a blockchain

Abstract

(IN201847033324)

A computer-implemented method (100) and system (1) for determining a metadata M for securing a controlled digital resource such as computer software using a distributed hash table (13) and a peer-to-peer distributed ledger (14).This is a blockchain such as the Bitcoin blockchain.The method includes determining (110) a data associated with the computer software and determining (120) a first hash value based on the computer software.A second hash value based on the data and the computer software may be determined (130).The method further includes sending 140 over a communications network (5) the data the first hash value and the second hash value to an entry for storage in a distributed hash table (13).The second hash value may be a key of a key-value pair.The data and the first hash value may be a value in the key-value pair.A metadata (M) that is based on the second hash value may be determined (150) for storage on the peer-to-peer distributed ledger (14).

Family 9/47 - FAMPAT - ©Questel

Current assignees

BT

Publication numbers

EP3382591

US20180285585

Application dates

2017-03-30

2018-03-29

Publication dates

2018-10-03

2018-10-04

Title

(EP3382591)

Hierarchical temporal memory for expendable access control

Abstract

(EP3382591)

A computer implemented method for access control for a restricted resource in a computer system, the method comprising: receiving a first set of records for the computer system, each record detailing an occurrence in the computer system during a training time period when the resource is accessed in an approved manner; generating a sparse distributed representation of the set of records to form a training set for a hierarchical temporal memory (HTM); training the HTM based on the training set in order that the trained HTM provides a model of the operation of the computer system during the training time period; receiving a request to access the resource by a resource consumer; allocating a predetermined quantity of cryptocurrency to the consumer, the allocation being recorded by a blockchain data structure accessible by a network, the blockchain storing digitally signed records validated by network connected miner software components; receiving a second set of records for the computer system, each record detailing an occurrence in the computer system during an operating time period for the computer system in use by the consumer of the resource; generating a sparse distributed representation of the second set of records to form an input set for the trained HTM; executing the trained HTM based on the input set to determine a degree of recognition of the records of the input set; and responsive to a determination that a degree of recognition of one or more records of the input set is below a threshold degree, generating a blockchain transaction to expend at least a portion of the cryptocurrency allocated to the user; responsive to a determination that a quantity of cryptocurrency allocated to the user is below a threshold quantity, identifying the consumer as unauthorised to access the resource.

Family 10/47 - FAMPAT - ©Questel

Current assignees

CISCO TECHNOLOGY

Publication numbers

US20180287893

Application dates

2017-03-29

Publication dates

2018-10-04

Title

(US20180287893)

Consumption-based licensing of network features based on blockchain transactions

Abstract

(US20180287893)

Consumption-based licensing of network features based on blockchained transactions includes receiving, at a server having connectivity to a network including a plurality of network devices, a request from a particular network device of the plurality of network devices for a feature that is licensed in the network on a per-use basis.Feature-specific key blockchain elements and a feature-specific template are generated for the feature and at least one message that includes the feature-specific key blockchain elements and the feature-specific template is sent to the particular network device.The message

enables the plurality of network devices to generate one or more blockchain transactions related to consumption of the feature when a usage interval associated with the feature expires.

Family 11/47 - FAMPAT - ©Questel

Current assignees

IBM

Publication numbers

US20180285971

Application dates

2017-03-31

Publication dates

2018-10-04

Title

(US20180285971)

Management of consumer debt collection using a blockchain and machine learning

Abstract

(US20180285971)

A blockchain of transactions may be referenced for various purposes and may be later accessed by interested parties for ledger verification and information retrieval.One example operation may include one or more of identifying a new event associated with a consumer debtor account, determining whether the new event includes a status change or debt related change, creating a file including the new event, and storing the file in a blockchain.

Family 12/47 - FAMPAT - ©Questel

Current assignees

Madisetti Dr. Vijay

Publication numbers

US20180288022

WO2018/183307

Application dates

2017-12-04

2018-03-27

Publication dates

2018-10-04

2018-10-04

Title

(WO2018183307)

Method and system for identity and access management for blockchain interoperability

Abstract

(WO2018183307)

A method of generating wallets for discrete blockchain networks comprising receiving a primary and a first secondary seeds, generating an enhanced hierarchical deterministic (HD) wallet, comprising deriving an enhanced parent public key and an enhanced parent private key from the primary seed, generating a first toughened HD wallet, comprising deriving a first toughened parent public and private key pair from the first secondary seed, deriving a first toughened primary child public/private key pair from a function including as inputs the first toughened parent public/private key pair, a first parent chain code, and the enhanced parent public key, and performing an identity registration and certification procedure for both the enhanced and the first toughened HD wallets.An identify of a user associated with each of the enhanced and the first toughened HD wallets is verifiable by an external blockchain network because of the identity registration and certification procedures.

Family 13/47 - FAMPAT - ©Questel

Current assignees

IBM

Publication numbers

US20180287797

Application dates

2017-04-04

Publication dates

2018-10-04

Title

(US20180287797)

Distributed logging of application events in a blockchain

Abstract

(US20180287797)

A blockchain of transactions may be used for various purposes and may be later accessed by interested parties for ledger verification.One example method of operation may include one or more of monitoring one or more applications to identify application events, identifying one or more application events, determining a hash of a log message payload associated with the application events and logging the hash of the log message payload in a blockchain.

Family 14/47 - FAMPAT - ©Questel

Current assignees

IBM

Publication numbers

US20180285979

Application dates

2017-04-04

Publication dates

2018-10-04

Title

(US20180285979)

Creating service agreements via blockchain smart contracts

Abstract

(US20180285979)

A blockchain of transactions may be used for various purposes and may be later accessed by interested parties for ledger verification.One example method of operation may include one or more of receiving a request from a user device for a new agreement at a service provider server, identifying a type of service requested, retrieving service history information stored in a user profile associated with the user device, evaluating the service history information to create a smart contract defining a new service agreement, and storing the smart contract in a blockchain.

Family 15/47 - FAMPAT - ©Questel

Current assignees

RIPE TECHNOLOGY

Publication numbers

US20180285810

Application dates

2018-03-29

Publication dates

2018-10-04

Title

(US20180285810)

Systems and methods of blockchain transaction recordation in a food supply chain

Abstract

(US20180285810)

Embodiments disclosed herein provide a system, method, and computer program product using blockchain and applying the internet of things concept to the food system in order to provide an infrastructure to which data can be recorded, shared and validated while data privacy and security is maintained.The collection of this data enables virtual histories of shipments to be created, which can be used to increase efficiency, create new business practices and potentially restructure marketplaces.Overall the solution presents a novel and new method to understanding of our food.

Family 16/47 - FAMPAT - ©Questel

Current assignees

NCHAIN HOLDINGS

Publication numbers

IN201847033271

Application dates

2018-09-05

Publication dates

2018-09-28

Title

(IN201847033271)

A method and system for the secure transfer of entities on a blockchain

Abstract

(IN201847033271)

The invention provides a secure method for exchanging entities via a blockchain.The invention incorporates tokenisation techniques and also techniques for embedding metadata in a redeem script of a blockchain transaction.Embodiment(s) provide a method of: generating a first script the first script comprising: a first set of metadata associated with a first invitation for the exchange of a first entity by a first user the first set of metadata comprising an indication of the first entity to be offered for exchange and a first location condition for the exchange a first user public key (P1A) associated with the first user wherein the first user public key (P1A) is part of an asymmetric cryptographic pair comprising the first user public key (P1A) and a first user private key (V1A).The script may further comprise a first third-party public key (P1T) associated with a first third-party wherein the first third-party public key (P1T) is part of an asymmetric cryptographic pair comprising the first third-party public key (P1T) and a first third-party private key (V1T) The method further comprises the steps of hashing the first script to generate a first script hash and publishing the first script and the first script hash on a distributed hash table (DHT).

Family 17/47 - FAMPAT - ©Questel

Current assignees

INNIT INTERNATIONAL

Publication numbers

US20180284093

WO2018/183768

Application dates

2018-03-29

2018-03-29

Publication dates

2018-10-04

2018-10-04

Title

(WO2018183768)

Trusted food traceability system and method and sensor network

Abstract

(WO2018183768)

A food traceability and alert system utilizing blockchain or similar structures with cryptographic signatures, distributed sensors throughout the supply chain, and cloud infrastructure to provide trusted information from all states of the supply chain is disclosed.

Family 18/47 - FAMPAT - ©Questel

Current assignees

CCC GROUP

Publication numbers

US20180285866

Application dates

2018-04-03

Publication dates

2018-10-04

Title

(US20180285866)

Method for producing a cryptographical signed transaction

Abstract

(US20180285866)

The invention relates to a method for producing a cryptographically signed transaction for the transfer of an amount of a currency within a blockchain.The transaction comprises one or more inputs and one or more outputs.The method comprises: - - retrieving the one or more inputs, the inputs being a reference to one or more previous transactions, - determining the one or more outputs, each output defining an amount to be transferred to a receiver indicated in the respective output, - adding security information, the security information defining directly or indirectly a maximum amount to be spent with the transaction, and - cryptographically signing the transaction by adding signature information.

Family 19/47 - FAMPAT - ©Questel

Current assignees

DATIENT

Publication numbers

US20180285839

Application dates

2017-05-05

Publication dates

2018-10-04

Title

(US20180285839)

Providing data provenance, permissioning, compliance, and access control for data storage systems using an immutable ledger overlay network

Abstract

(US20180285839)

A data management system is disclosed for data provenance and data storage that allows multiple independent parties (who may not trust each other) to securely share data, track data provenance, maintain audit logs, keep data synchronized, comply with regulations, and handle permissioning and control who can access the data.The system leverages security guarantees derived from the computer systems already trusted to control billions of dollars of Bitcoin and Ethereum cryptocurrencies to create a secure and completely auditable system of document tracking that can be shared among

untrusted parties over a computer network.Certain instances work both with public blockchains like Bitcoin and Ethereum and with private blockchains.

Family 20/47 - FAMPAT - ©Questel

Current assignees

SUPERNA

Publication numbers

US20180285479

Application dates

2018-04-02

Publication dates

2018-10-04

Title

(US20180285479)

Scalable audit analytics

Abstract

(US20180285479)

The present invention provides a method to translate audit record data from NAS systems into distributed multi storage and query node structure to allow parallel search and analytical queries to be scaled to millions or billions of records.This invention covers translation and transformation of data, relational query schema and methods to access and analyze audit data for specific patterns of user data access behavior for the purpose of securing the data.A system that allows external auditors to validate the integrity of an audit record and ensure immutable audit records stored on commodity storage devices.Modern enterprise-grade NAS devices are capable of generating massive amounts of audit data, with events rates of hundreds of millions of events per day.This invention provides a method to archive, search, and cryptographically sign the audit events to ensure long term persistence and immutability of the enterprise's file activity.

Family 21/47 - FAMPAT - ©Questel

Current assignees

BT

Publication numbers

WO2018/178026

Application dates

2018-03-26

Publication dates

2018-10-04

Title

(WO2018178026)

Hierarchical temporal memory for access control

Abstract

(WO2018178026)

A computer implemented method for access control for a restricted resource in a computer system, the method comprising: receiving a first set of records for the computer system, each record detailing an occurrence in the computer system during a training time period when the resource is accessed in an approved manner; generating a sparse distributed representation of the set of records to form a training set for a hierarchical temporal memory (HTM); training the HTM based on the training set in order that the trained HTM provides a model of the operation of the computer system during the training time period; receiving a second set of records for the computer system, each record detailing an occurrence in the computer system during an operating time period for the computer system in use by a consumer of the resource; generating a sparse distributed representation of the second set of records to form an input set for the trained HTM; executing the trained HTM based on the input set to determine a degree of recognition of the records of the input set; and

responsive to a determination that a degree of recognition of one or more records of the input set is below a threshold degree, identifying the operation of the computer system by the consumer as unauthorised.

Family 22/47 - FAMPAT - ©Questel

Current assignees

QIHOO 360 TECHNOLOGY

Publication numbers

CN108596617

Application dates

2018-04-23

Publication dates

2018-09-28

Title

(CN108596617)

Based on algorithm type of block chain method and a device for sensing an attack event

Abstract

(CN108596617)

The present invention discloses an algorithm-based method and a device for sensing whether an attack event block chain type, wherein, the method comprising: reading an algorithm for each block in the block chain type data; determine whether it conforms to the type of algorithm for each block type of algorithm audit policy; if true, then the resulting sensing result of the attack event.The present invention protocol by using, for each block of the type of algorithm audit policy audits through algorithmic type data, thereby enabling to automatically and timely perceived from the type of algorithm angle of attack event, whether an attack event for that block chain are performed by facilitating, in order to avoid causing a loss in the miners exclusive hollowed Ore Attacker other.

Family 23/47 - FAMPAT - ©Questel

Current assignees

FACTOM

Publication numbers

US20180285970

Application dates

2017-03-31

Publication dates

2018-10-04

Title

(US20180285970)

Due Diligence in Mortgage Documents

Abstract

(US20180285970)

Due diligence of mortgage documents is faster and simpler.An electronic mortgage application often contains or references a collection of many separate electronic mortgage documents.Electronic data representing an original version of an electronic mortgage document and its current version may be hashed to generate digital signatures.Any auditor may then quickly conduct the due diligence by comparing the digital signatures.If the digital signatures match, then the due diligence reveals that the electronic mortgage document has not changed since its creation.However, if the digital signatures do not match, then the electronic mortgage document has changed since its creation.The auditor may thus flag the electronic mortgage document for additional due diligence.Regardless, a result of the due diligence may be incorporated into one or more blockchains.

Family 24/47 - FAMPAT - ©Questel

Current assignees

TIDETIME SUN

Publication numbers

US20180285867

Application dates

2017-08-25

Publication dates

2018-10-04

Title

(US20180285867)

Distributed auditing method, device and system

Abstract

(US20180285867)

A distributed auditing method includes the steps of providing a to-be-audited information stored by using a hash tree method, wherein the to-be-audited information is related to a plurality of user ends; utilizing a processor, creating a condensed status code according to the to-be-audited information by using a hash function; corresponding to the user ends, creating a plurality of slices according to the to-be-audited information; providing the condensed status code and each of the plurality of slices to each of the corresponding plurality of user ends respectively; and auditing the to-be-audited information according to feedbacks from each of the plurality user ends.A distributed auditing device and its system are also disclosed.

Family 25/47 - FAMPAT - ©Questel

Current assignees

SYNGRAFII

Publication numbers

WO2018/176140

Application dates

2018-03-28

Publication dates

2018-10-04

Title

(WO2018176140)

Systems and methods for executing and delivering electronic documents

Abstract

(WO2018176140)

A computer-implemented system and method for annotating or signing an electronic document are provided.The method includes steps of: receiving or retrieving an electronic document available for annotation or execution by one or more parties; transmitting the electronic document for display on a first computing device to the first computing device at a first location; authenticating an identity of a first user of the first computing device; receiving electronic signals representing an user input of the first user from the first computing device; generating digital data representative of an indicia based the user input of the first user from the first computing device; and applying the digital data to the electronic document to form a first annotation or signature from the first user.

Family 26/47 - FAMPAT - ©Questel

Current assignees

IBM

Publication numbers

US20180285983

Application dates

2017-04-04

Publication dates

2018-10-04

Title

(US20180285983)

Scalable and distributed shared ledger transaction management

Abstract

(US20180285983)

A shared ledger of transactions may be used for various purposes and may be later accessed by interested parties for ledger verification.Authenticity of transactions requires active measures to ensure transaction participants including parties to the transactions, observers to the transaction, etc., are providing accurate information for each transaction.One example method of operation may include one or more of identifying a set of participants to one or more transactions, transmitting a request from an initiating participant to enable each of the set of participants to generate local numbers based on a number source, forwarding the local numbers to one or more of the set of participants before expiration of a specified time interval, receiving the local numbers at the initiating participant, and generating a final number based on the local numbers received, so that after a last participant among the set of participants has forwarded the local number, none of the set of participants can obtain the final number until after a limited amount of time.

Family 27/47 - FAMPAT - ©Questel

Current assignees

IBM

Publication numbers

US20180285838

Application dates

2017-04-04

Publication dates

2018-10-04

Title

(US20180285838)

Scalable and distributed shared ledger transaction management

Abstract

(US20180285838)

A shared ledger of transactions may be used for various purposes and may be later accessed by interested parties for ledger verification.Authenticity of transactions requires active measures to ensure transaction participants including parties to the transactions, observers to the transaction, etc., are providing accurate information for each transaction.One example method of operation may include one or more of performing one or more transactions between a subset of participants of a shared ledger system or subsystem which includes the subset of participants and witnesses assigned to the subset of participants, and synchronizing the one or more transactions exclusively by the subset of participants and the assigned witnesses, so the one or more of the transactions between the subset of participants exist with no common witnesses.

Family 28/47 - FAMPAT - ©Questel

Current assignees

STRONGFORCE IOT PORTFOLIO 2016

Publication numbers

US20180284756
US20180284755
US20180284736
US20180284754
US20180284758
US20180284757

US20180284745
US20180284752
US20180284743
US20180284744
US20180284753
US20180284737
US20180284749
US20180284746
US20180284741
US20180284742
US20180284735
US20180284747

Application dates

2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07
2018-05-07

Publication dates

2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04
2018-10-04

2018-10-04

Title

(US20180284758)

Methods and systems for industrial internet of things data collection for equipment analysis in an upstream oil and gas environment

Abstract

(US20180284758)

In embodiments of the present invention improved capabilities are described for a monitoring system for data collection in an industrial drilling environment comprising a data collector communicatively coupled to a plurality of input channels, wherein a subset of the plurality of input channels are communicatively coupled to sensors measuring operational parameters from an industrial drilling component; a data storage structured to store a plurality of collector routes and collected data that correspond to the plurality of input channels, wherein the plurality of collector routes each comprise a different data collection routine; a data acquisition circuit structured to interpret a plurality of detection values from the collected data, each of the plurality of detection values corresponding to at least one of the plurality of input channels; a data analysis circuit structured to analyze the collected data from the plurality of input channels to detect an anomalous condition associated with the industrial drilling component; and a data response circuit structured to switch one of the data collection routines from a first data collection routine to a second collection routine based on the detection of the anomalous condition.

Family 29/47 - FAMPAT - ©Questel

Current assignees

INNOGY

Publication numbers

WO2018/177520

Application dates

2017-03-29

Publication dates

2018-10-04

Title

(WO2018177520)

Method of operating an electrical grid

Abstract

(WO2018177520)

The invention relates to a method of operating an electrical grid (102, 202) having at least one electrical consumer (111, 211) and a plurality of electrical producers (112, 212.1, 212.2, 214, 216), the method comprising providing at least one consumption prediction for the electrical consumer (111, 211), providing respective production predictions for each electrical producer (112, 212.1, 212.2, 214, 216) of at least a part of the plurality of electrical producers (112, 212.1, 212.2, 214, 216), determining the respective distances between the electrical consumer (111, 211) and each electrical producer (112, 212.1, 212.2, 214, 216) of the part of the plurality of electrical producers (112, 212.1, 212.2, 214, 216), allocating at least one electrical producer (112, 212.1, 212.2, 214, 216) of the part of the electrical producers (112, 212.1, 212.2, 214, 216) to the electrical consumer (111, 211) in a first allocating step such that the provided consumption prediction of the electrical consumer (111, 211) matches to the provided production prediction of the at least one electrical producer (112, 212.1, 212.2, 214, 216) and such that the determined distance between the electrical consumer (111, 211) and the at least one electrical producer (112, 212.1, 212.2, 214, 216) is at least smaller than at least one first distance limit.

Family 30/47 - FAMPAT - ©Questel

Current assignees

COGNANT

Publication numbers

US20180285949

WO2018/183033

Application dates

2018-03-20

2018-03-20

Publication dates

2018-10-04

2018-10-04

Title

(WO2018183033)

System and method for presenting content on client devices

Abstract

(WO2018183033)

Implementations of the present disclosure are directed to a method, a system, and an article for providing content on client devices.An example computer-implemented method can include: providing an offer unit on a client device; presenting, using the offer unit, an offer to provide content on the client device; receiving, using the offer unit, an acceptance of the offer on the client device; completing, using the offer unit, a transaction based on the accepted offer; connecting, based on the completed transaction, the client device with a server configured to provide the content; and providing the client device with access to the content.

Family 31/47 - FAMPAT - ©Questel

Current assignees

ZHONG AN INFORMATION TECHNOLOGY SERVICES

Publication numbers

CN108600227

Application dates

2018-04-26

Publication dates

2018-09-28

Title

(CN108600227)

Medical data sharing method based on a block chain and a device

Abstract

(CN108600227)

The present invention discloses a method and apparatus for sharing medical data based on block chain, which belongs to the technical field of a block chain.Method comprises: constructing a P2P network of nodes having a plurality of medical; is selected based on the unique identification number is defined for the patient, is generated for the patient using the public key and private SM2, patient remains private key, the public key is disclosed to a plurality of medical node; a predetermined node in the plurality of medical patient medical data using a public key of the medical node encrypts the information, encrypted text block chain structure through a structured information; a preset validation check rule based on an agreement is reached, the structured information is broadcast to other nodes more healthcare medical node; the structured information writing block chain.The present invention not only can increase the efficiency of data sharing between a hospital, and can guarantee privacy and security of information from the art, the advantages of the application in the medical field adapted to be carried out.

Family 32/47 - FAMPAT - ©Questel

Current assignees

UNISCEN

Publication numbers

US20180285594

WO2018/183351

Application dates

2018-03-27

2018-03-27

Publication dates

2018-10-04

2018-10-04

Title

(WO2018183351)

Architectures and systems for managing personal data to be utilized by dynamic sets of external parties

Abstract

(WO2018183351)

Techniques and architectures to manage personal data.Permissions are maintained information for one or more portions of the electronic personal record.Connection information for the one or more portions of the electronic personal record are maintained.At least one of the one or more portions of the electronic personal record information from a static document provided by the user and dynamic information obtained via an integration with an external data source.The one or more processors further to evaluate claims on portions of the electronic record from providers utilizing attribute-based security mechanisms.The corresponding portions of the electronic personal record are selectively provided in response to results of the evaluation.

Family 33/47 - FAMPAT - ©Questel

Current assignees

OJAI ENERGETICS PBC

Publication numbers

WO2018/183564

Application dates

2018-03-28

Publication dates

2018-10-04

Title

(WO2018183564)

Systems and methods for storing electrical energy

Abstract

(WO2018183564)

The present disclosure provides capacitors for storing electrical energy.The capacitors can comprise, at least in part, bast fiber, bast powder, hurd fiber, hurd powder, or a derivative thereof.In some instances, a dielectric of a capacitor can be formed of bast fiber, bast powder, hurd fiber, hurd powder, or a derivative thereof.In other instances, one or both electrodes of the capacitor can be formed of bast fiber, bast powder, hurd fiber, hurd powder, or a derivative thereof.The resulting capacitors can be configured to have various power densities and various energy densities over various minimum numbers of charge/discharge cycles at a certain specified range of operating temperatures.

Family 34/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

WO2018/182903

Application dates

2018-02-27

Publication dates

2018-10-04

Title

(WO2018182903)

Cloud assisted machine learning

Abstract

(WO2018182903)

A method for training an analytics engine hosted by an edge server device is provided.The method includes determining a classification for data in an analytics engine hosted by an edge server and computing a confidence level for the classification.The confidence level is compared to a threshold.The data is sent to a cloud server if the confidence level is less than the threshold.A reclassification is received from the cloud server and the analytics engine is trained based, at least in part, on the data and the reclassification.

Family 35/47 - FAMPAT - ©Questel

Current assignees

Carboni Davide

Haghighi Mo

Nolan Michael

Smith Ned M.

Publication numbers

US20180287806

Application dates

2017-03-31

Publication dates

2018-10-04

Title

(US20180287806)

Securing communications

Abstract

(US20180287806)

A method for securing the communications between a publisher and a subscriber in an Internet of things networks.An example method includes receiving a challenge vector from a subscriber and determining a response vector using a physically unclonable function (PUF) for each challenge value in the challenge vector to generate a response value.The response vector it is sent to the subscriber.

Family 36/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

US20180285767

Application dates

2017-03-30

Publication dates

2018-10-04

Title

(US20180285767)

Cloud assisted machine learning

Abstract

(US20180285767)

A method for training an analytics engine hosted by an edge server device is provided.The method includes determining a classification for data in an analytics engine hosted by an edge server and computing a confidence level for the classification.The confidence level is compared to a threshold.The data is sent to a cloud server if the confidence level is less than the threshold.A reclassification is received from the cloud server and the analytics engine is trained based, at least in part, on the data and the reclassification.

Family 37/47 - FAMPAT - ©Questel

Current assignees

INTEL

Publication numbers

EP3382928

Application dates

2018-02-21

Publication dates

2018-10-03

Title

(EP3382928)

Securing communications

Abstract

(EP3382928)

A method for securing the communications between a publisher (402) and a subscriber (404) in an Internet of things networks.An example method includes receiving a challenge vector (406) from a subscriber and determining a response vector using a physically unclonable function (PUF) for each challenge value in the challenge vector to generate a response value.The response vector it is sent to the subscriber (408).

Family 38/47 - FAMPAT - ©Questel

Current assignees

AVAST SOFTWARE S R O

Publication numbers

US20180285845

WO2018/177603

Application dates

2018-03-20

2018-04-03

Publication dates

2018-10-04

2018-10-04

Title

(WO2018177603)

Providing payment options without requiring online shop integration

Abstract

(WO2018177603)

Initiation of a purchase at an online shop or other retailer can be detected.In addition to, or instead of a payment method integrated with the online shop, one or more alternative payment services that are not integrated with the online shop or retailer can be considered for selection.A non-integrated payment service can be selected based on terms offered by the non-integrated payment service.The selected goods or services can be paid for by the non-integrated payment service using a virtual credit card.The user can reimburse the non-integrated payment service under the terms offered by the non-integrated payment service.

Family 39/47 - FAMPAT - ©Questel

Current assignees

GEO PRO TEQ IP

Publication numbers

WO2018/176100

Application dates

2018-03-29

Publication dates

2018-10-04

Title

(WO2018176100)

A computer system and a computer implemented method for processing gaming data

Abstract

(WO2018176100)

There is provided a computer system (106) for processing gaming data from two or more gaming systems.The computer system (106) comprises a memory device (108) configured to store machine-readable instructions, a processor (110) connected to the memory device (108) and a first communication interface (112) connected to the processor (110) and configured to connect to a first gaming system (102) and a second communication interface (114) connected to the processor (110) and configured to connect to a second gaming system (104) that is different from the first gaming system (102), a third communication interface (116) connected to the processor (110) and configured to connect to a first server (120), wherein the processor (110) obtains the machine-readable instructions from the memory device (108) and is configured by the machine-readable instructions to receive, via the first communication interface (112), first gaming data from the first gaming system (102), the first gaming data being generated by the first gaming system (102) based on a first protocol, receive, via the second communication interface (114), second gaming data from the second gaming system (104), the second gaming data being generated by the second gaming system (104) based on a second protocol that is different from the first protocol, determine, from the first gaming data and based on the first protocol, identity information associated with a user and first usage information associated with use of the first gaming system (102) by the user, determine, from the second gaming data and based on the second protocol, the identity information associated with the user and second usage information associated with use of the second gaming system (104) by the user and send the identity information, the first usage information and the second usage information to the first server (120) via the third communication interface (116).

Family 40/47 - FAMPAT - ©Questel

Current assignees

AT&T

Publication numbers

US20180288041

Application dates

2017-03-30

Publication dates

2018-10-04

Title

(US20180288041)

Seamless Authentication Device

Abstract

(US20180288041)

According to one embodiment, an authentication system includes an authentication device.The authentication device includes a biometric scanner, a processor, and an interface.The biometric scanner receives biometric data for a user.The

processor authenticates the user by comparing the received biometric data for the user to predetermined biometric information for the user.The processor generates an authentication token in response to the authentication.The processor continuously authenticates the user.The interface communicates the authentication token to a content providing device, the authentication token indicating the authentication of the user.The interface receives content from the content providing device in response to the authentication token.

Family 41/47 - FAMPAT - ©Questel

Current assignees

BAYER HEALTHCARE

Publication numbers

US20180285880

WO2018/178878

Application dates

2018-03-27

2018-03-27

Publication dates

2018-10-04

2018-10-04

Title

(WO2018178878)

Biometric authentication for, and secure electronic tracking of, restricted over-the-counter drug sales

Abstract

(WO2018178878)

A mobile device is provided that includes biometric sensor(s), and a processor that causes the biometric sensor(s) to acquire a physiological marker of a user, and identify and authenticate the user.The processor sends a message to an authentication server that indicates the user is authenticated, and receives a response from the authentication server that includes a unique authentication code.The processor receives selection of a thereby selected over-the-counter (OTC) drug, and communicates with a point-of-sale (POS) system with contactless payment capability.The processor sends a purchase message to the POS system that includes the unique authentication code, an identifier of the selected OTC drug, and payment information.And the POS system communicates with the authentication server to validate the unique authentication code, and with an authorization server to authorize payment for the selected OTC drug based on the payment information.

Family 42/47 - FAMPAT - ©Questel

Current assignees

BT

Publication numbers

WO2018/178028

Application dates

2018-03-26

Publication dates

2018-10-04

Title

(WO2018178028)

Initialisation vector identification for encrypted malware traffic detection

Abstract

(WO2018178028)

A method for identifying malicious encrypted network traffic associated with a malware software component communicating via a network, the method comprising: defining, for the malware, a portion of network traffic including a plurality of

contiguous bytes occurring at a predefined offset in a network communication of the malware; extracting the defined portion of network traffic for each of a plurality of disparate encrypted network connections for the malware; training an autoencoder based on each extracted portion of network traffic, wherein the autoencoder includes: a set of input units each for representing information from a byte of an extracted portion; output units each for storing an output of the autoencoder; and a set of hidden units smaller in number than the set of input units and each interconnecting all input and all output units with weighted interconnections, such that the autoencoder is trainable to provide an approximated reconstruction of values of the input units at the output units; selecting a set of one or more offsets in the definition of a portion of network traffic as candidate locations for communication of an initialisation vector for encryption of the network traffic, the selection being based on weights of interconnections in the autoencoder; and identifying malicious network traffic based on an identification of an initialisation vector in the network traffic at one of the candidate locations.

Family 43/47 - FAMPAT - ©Questel

Current assignees

BT

Publication numbers

WO2018/178027

Application dates

2018-03-26

Publication dates

2018-10-04

Title

(WO2018178027)

Intialisation vector identification for malware file detection

Abstract

(WO2018178027)

A method for detecting a malware file in encrypted form comprising: receiving multiple versions of the malware file, each version encrypted using a different initialisation vector; training an autoencoder based on each version of the malware file, wherein the autoencoder includes: a set of input units each for representing information from a byte of malware file; output units each for storing an output of the autoencoder; and a set of hidden units smaller in number than the set of input units and each interconnecting all input and all output units with weighted interconnections, such that the autoencoder is trainable to provide an approximated reconstruction of values of the input units at the output units; selecting a set of one or more offsets in the malware file in encrypted form as candidate locations for storage of an initialisation vector for encryption of the malware file, the selection being based on weights of interconnections in the autoencoder; and identifying the malware file based on an identification of an initialisation vector in an encrypted form of the malware file at one of the candidate locations.

Family 44/47 - FAMPAT - ©Questel

Current assignees

Burinska Patrizia

Hoffman Michael

Kaloyeros Alain Elie

Lubrano-Birken Brenda

Payette, JR. Joseph

Publication numbers

US20180286239

WO2018/183831

Application dates

2018-03-30

2018-03-30

Publication dates

2018-10-04

2018-10-04

Title

(WO2018183831)

Image data integrator for addressing congestion

Abstract

(WO2018183831)

A system, method and program product for that: receives image data from at least one provider such as a drone, on-board vision system, fixed camera, satellite, wearable, smart phone, etc.; processes the image data to identify congestion-based information such as parking spot availability, standby location information, traffic flow information, and line waiting time information; and outputs the information to devices and applications, such as user apps, vehicle fleets, event operators, etc.

Family 45/47 - FAMPAT - ©Questel

Current assignees

Aggarwal Sumiran

Akkapeddi Venkata Krishna Prasad

Choudhary Mohit

Khare Prateek

Sonkar Siddhant

Publication numbers

US20180285549

Application dates

2017-04-04

Publication dates

2018-10-04

Title

(US20180285549)

Authorization of virtual reality interactions using controlled randomization

Abstract

(US20180285549)

Embodiments of the disclosure are directed to the use of controlled randomization in authorizing virtual reality interactions.More specifically, a user of a virtual reality (VR) device may seek to initiate an interaction within the virtual reality environment.In order for the interaction to be allowed for the user, a processing computer may need the user to supply an additional credential.In some cases, the user may enter the additional credential using a series of virtual keypads that are rendered in the virtual reality environment.These keypads may have varying layouts that are determined in a controlled manner (e.g., pseudo-randomly) using pre-determined mathematical procedures.The layout of a subsequent keypad may be partially based on the user's selection in a preceding keypad.The keypad positions for the user's selections may be provided to the processing computer to solve for the credential which can be used for validation purposes.

Family 46/47 - FAMPAT - ©Questel

Current assignees

Braunstein Kim

Publication numbers

US20180285709

Application dates

2018-03-28

Publication dates

2018-10-04

Title

(US20180285709)

Transponder-unit for facilitating authorization associated with an article

Abstract

(US20180285709)

Disclosed is a transponder-unit for facilitating authorization associated with at least one article is provided.The transponder-unit may include a planar base including a planar cavity.Further, the planar cavity may include a transponder configured to transmit at least one identifier associated the at least one article.Further, the planar cavity may include a processor configured to process data.Further, the planar cavity may include a battery configured to provide power to operate at least one component of the transponder-unit.Further, the planar cavity may include an antenna array configured to provide wireless communication with a transponder registration system.Further, the transponder-unit may include an affixing means configured to attach the transponder-unit to a container including the at least one article.Further, the transponder-unit may include a static indicium including a static display surface.Further, the transponder-unit may include an electrical information upload port communicatively coupled to the processor.

Family 47/47 - FAMPAT - ©Questel

Current assignees

BATON SYSTEMS

Publication numbers

US20180285882

Application dates

2018-03-30

Publication dates

2018-10-04

Title

(US20180285882)

Activity management systems and methods

Abstract

(US20180285882)

Example activity management systems and methods are described.In one implementation, a financial management system receives membership criteria from a client clearing guarantor and receives additional membership criteria from a clearinghouse.The financial management system creates a direct clearing client and communicates access information to the direct clearing client, which creates multiple accounts.The systems and methods then identify approval of the direct clearing client by the client clearing guarantor and the clearinghouse.