Research Article

Iot Network Identity Management Using Smart Contract and Blockchain Technology

Deepika Chauhan[a], Prachi Joshi[b], Dr. Ranjan Walia[c] , Dr. M. Deivakani[d], and Dr. Chaitanya Singh[e]

[a]
Assistant Professor, Department of Computer Science & Engineering, Shivajirao
Kadam Institute of Technology and Management, Indore, M.P, India
[b]Research Scholar, School of Computer Science , Dr. Babasaheb Ambedkar Open University, India
[c]Associate Professor, Electrical Engineering Department, Model Institute of
Engineering and Technology, Jammu and Kashmir, India
[d]Associate Professor, Electronics and Communication Engineering, Psna College Of Engineering and Technology, Dindigul, TamilNadu, India
[e]Associate Professor, Department of Computer Science & Engineering, Shivajirao Kadam Institute of Technology and Management, Indore, M.P, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: The proliferation of Internet of Things (IoT) devices is on the rise, with the number of connected devices exceeding seven billion devices by 2017, and forecasting connects 20-50 billion connections by 2020. Many of those devices have been used in an unusual way and complex networks pose many challenges to the functionality of device management. Among those challenges is patent management related to how devices are verified and authenticated in addition to how devices create mechanisms to authorize and control access to data and services. Blockchain as a computer-distributed computer technology sets itself up as the right person to tackle this challenge. That is mainly due to the use of Blockchain cryptographic indicators, static recording, and background. These features, in combination, provide a platform to use IoT device ID management functions that can ensure global and unique device ownership, and provide a way to maintain it throughout the life cycle of the device. This paper introduces a low-level blockchain-based proprietary management framework that provides features for patenting and transfer of ownership, as well as the ability to manage patents between machine-visited networks. To confirm, we define a set of smart contracts that provide registrar functions and administrative contracts.

Keywords: Identity Management, Internet of Things, Blockchain, Ethereum, Smart Contracts.

1. Introduction

The role of Internet Identity Management (IoT) is expanding, not only by introducing user identifiers and managing their access to a variety of devices and data, but also by looking at how to identify devices, manage their interactions, their services, and control access to sensitive data An important requirement for Identity and Access Management (IAM) is to be able to manage one-to-device, device-to-device management, and / or app / system interactions.

In addition, in most cases IoT devices are connected periodically and / or temporarily and at the same time are required to communicate with other devices, services and infrastructure [1]. Starting communication requires that device authentication and authorization be performed in accordance with a well-managed patent life cycle that can ensure a unique and well-known global process. However, guaranteeing the ability to guarantee, manage and control the rights to access the entire patent life cycle poses many challenges to acceptance existing IAM structures. Those challenges include establishing clear registration processes, maintaining global and unique ownership, and providing access control and authorization frameworks. Other limitations include the growing number of devices and the close relationship between them as IoT devices have become more popular in both consumer and business domains.

However, most IoT platforms are based on a mid-level model in which an authority handles communication between its devices and other devices of other authorities [2]. After that, there are a lot of growing problems; especially in cases where devices need to exchange data in a peer-to-peer manner. This requirement has led to the introduction of a system of land redistribution. Blockchain technology as a shared and distributed platform can facilitate the implementation of low-level IoT platforms, which can keep secure and reliable data exchanges and historical records based on the consistency and anonymity of its targeting system. With such power-enabled architecture, Blockchain acts as a standard logger, keeping accurate records of all transactions and events exchanged between smart devices on a fixed local basis.

In this paper, we propose to use Blockchain technology to address patent management in IoT and to establish a unique and global identity that can be maintained throughout the life cycle of the device. In addition, this approach provides ways to support device ownership management and identity renewal. We use Blockchain techniques based on public and private key identification, distributed and unchanging ledge and the availability of ownership management throughout the life cycle of devices and smart contractual and contractual contracts.

This paper is organized as follows. Section II defines the concept of proprietary management and highlights the proposed and applied methods. Section III introduces what Blockchain is, how it works, its key features, and how smart contracts can be used to create processes and rules that govern interaction between devices. Section IV describes the concept of a distributed framework and highlights the relationship model with the life cycle of ownership. In Section V, we describe the details of the proposed framework and process for the adoption of Blockchain features and possible use cases. Later, Section VI introduces a set of smart contracts with a summary of how to use them. Finally, Section VII concludes the work.

2. IoT Identity management

Identity Management (IdM) is an administrative domain that operates by identifying individual businesses in the system (such as a user or tool) and manages access to resources within that system by combining access rights with restrictions and established ownership [3]. This is often defined as validation and authorization and the scope of the definition includes the design and management of the entire patent life cycle.

One of the major mechanisms of IAM is the Identity Relationship Management IRM, funded by the Kanatra Initiative [4], which is regarded as a major river. However, there are many challenges to this river as it needs to manage the many types of relationships that need to be built and maintained. Multi-Factor Authentication (MFA) and Authentication and Authorization for Constrained Environments (ACE), [5], are also common methods that focus on the authorization and authentication of compact devices to ensure that small IoT devices can still maintain the required level of security. .

In [6], Chen et al. propose a IoT framework for user-centric Management Identity, built on a global patent provider responsible for the preservation of a global identity document. Various providers produce property ownership in terms of global ownership, and maintain a vision consistent with global ownership. Therefore, ownership of each property can have their own way of verifying and authenticating. Trnka and Cerny, in their work [2] propose a middle-class ownership management framework, in which their work focuses on creating a unique land ownership held by a central store. Ownership and authorization management all takes place in the central store, and every start of communication and access to services is authorized based on the middle-generation OAuth 2.0 tokens managed by the central store.

Blockchain technology has been promoted through IoT-enabled identity management frameworks. One example is the partnership between IBM and Samsung to develop evidence for the concept of the ADEPT (Autonomous Decentralized Peer- to-Peer Telemetry) platform. ADEPT uses three principles; BitTorrent (ukw le sharing), Ethereum (Smart Contracts) and TeleHash (Peer-to-Peer Messages) on the platform [7]. Chronicled Inc., [8], and provides IoT Registry Registry; where encrypted microchips are used (currently only Bluetooth low Energy and NFC) to assign secure digital identity to the visual object and connect it to a Blockchain record.

In light of the above, we summarize the key points we need in relation to the IAM module of the IoT management framework, and include:

1) Enabling worldwide registration of IoT devices.
2) Develop the necessary processes for the life cycle.
3) Clarify clear registration procedures.
4) Provide management tools to manage device ownership and transfer ownership.
5) Provide a way to track the life cycle of the device back to the root.

3. Blockchain and smart contract

Blockchain technology was discovered a few years ago great interest in various industries, especially finance services. While the first use of Blockchain technology is crypto-currencies, namely Bitcoin, it has been promoted as an alternative to fi money. However, over the past few years the entire ecosystem of new companies and many of the founding companies has made separate Blockchain applications. These applications included a new platform provided by the site that provides quick and secure ways to manage specific domain transactions; in health care, postal, IoT, digital marketing, procurement and more.

Block Chain structure

Blockchain is defined as a shared digital ledger of transactions. It uses public key cryptography to create the identity and anonymity of all participants and low-level compromise systems to keep the ledger strong and secure any transactions. A distributed ledger is created by combining multiple transactions in a block, and hashes their content with the previous block hash value to create a new block hash value. This happens with each newly created block outside the genesis block.

One of the key features of Blockchain is consistency as recorded transactions are irreversible and permanent. For example, a change in account balance is not made by updating the balance, instead the new transaction combined with other transactions is used to create a block that will be active and distributed and linked to the previous block.

The name Blockchain can literally be defined by its two keywords; Firstly that each (n) transaction group forms a single block, secondly the blockchain communication via cryptographic hashes is a consistent chain, such as it is easy to verify the historical record until it reaches the first box (block genesis). In addition to ensuring consistency, this provides a feature of provenance [9].

Among the most widely accepted Blockchain platforms is Ethereum, and it is a Blockchain platform with an integrated state-of-the-art database, capable of maintaining systems and their status. These programs are often called Smart Contracts. The smart contract can still be distributed by any Ethereum user and has a function-based interface or Application Binary Interface ABI. If used a smart contract can be referenced by its address, which is a cryptographic identifier. The user calls the smart contract employee by sending the transaction to his or her address as the destination, and with the paid transaction data load containing the work signature and input parameters. Calling for work causes network miners to use the system and restore its status. A smart contractor can capture and send a native Ether token, and may also call for the services of other smart contractors [10].

4. Semi-Decentralized Identity Management In Iot

In this paper, we present a mid-range IoT ownership management framework based on Blockchain technology and smart contracts, a framework that balances between less complex and affordable scenarios. The framework emphasizes three key principles: ownership as a living asset, ownership is unique and global and limits third party authority.

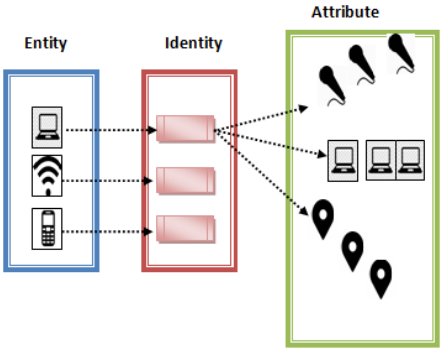


Fig 1: Relationship between Identity, Entity and Attribute

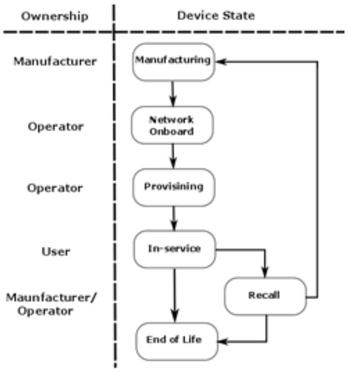


Fig 2: Lifecycle and ownerships of IoT device

A. The concept of Identity for IoT devices

The need for proprietary management is essential for all IT business solutions to handle authentication and authentication. In addition, in IoT, the need is continuously driven by factors related to the high number of devices, complex architectures, and change of ownership and network of intermittent network. Those items require the creation of a global and unique device identifier in order to be able to transfer between networks and owners who have little or no impact on their identification and effectively without losing track of historical records.

In this paper, we define ownership as a living asset, such as that the device was given its own ownership at birth (e.g. manufacturing). The device will retain its identity through updates and versions as pre-defined changes occur, which will be stored in a global registry to allow tracking and testing. According to ISO / IEC 24760-1 an entity is an internal or external information and communication technology system, such as an individual, organization, device, support system, or group of such objects with distinct physical presence, while ownership is "a set of business-related features" [11].

We use that definition to describe the model of business relationships (devices), ownership and features built into the individual relationships between the app and its ownership and the dual and multidimensional relationship between ownership and branding, as seen in Fig. 1. In addition, we need to use an identifier that should be unique, universally recognized and completely anonymous. Therefore, in a business system (n) (Ei), there is (n) each ID with a unique ID (ID), the identity is defined by a list of symbols (A) as defined in Eq. 1.

$E_i \Leftarrow ID_i \Leftarrow < A_{i1}, A_{i2},, A_{in} >$ (1)

B. Device Identity Life Cycle and Ownership

In IoT networks, the device will go through a life cycle that starts from production to the end of life. The proposed IdM framework shows a credit that describes the status of the device and its ownership. In this life cycle, device ownership is maintained by a global register that allows authorized subscribers (e.g. manufacturers) to create new ownership of new devices, and perform patrol management functions or transfer device ownership to users / users.

Ownership as a living asset is kept renewed at various stages, with the release of a new version if necessary as the device owner changes or the status of the device in the network changes from provision to service for retirement; this is shown in Fig. 2.

5. Blockchain-Based System Architecture

The total architecture proposed is based on Keychain blockchain concepts used to match the objectives of establishing a global register with a unique and global identifier for each device, a high level of anonymity, irreversible records tracked in the form of patent creation, and a third-party sub-authority.

A distributed Blockchain ledger is used, with more smart contracts, to create a land register with specific rules to enable authorized and identifiable businesses for device ownership. Public key cryptography is used as the purpose of ensuring the establishment of a global and unique identifier for each device. In Blockchain, especially in Ethereum, each account (e.g. device) will have a private key and a public key created, and receive a Blockchain address depending on the effect of public key operations, details of which are described in the following paragraphs.

A. Creation of identity

Identity creation is largely based on the public key of cryptography and hashing functions. Identity is made up of a small set of symbols, <Ai1, Ai2 ,, Ain>, which are required to produce a unique and global device identity in a global registry. That is done in two steps: the creation of cryptographic keys with a Blockchain address and the creation of a digital block-based identity.

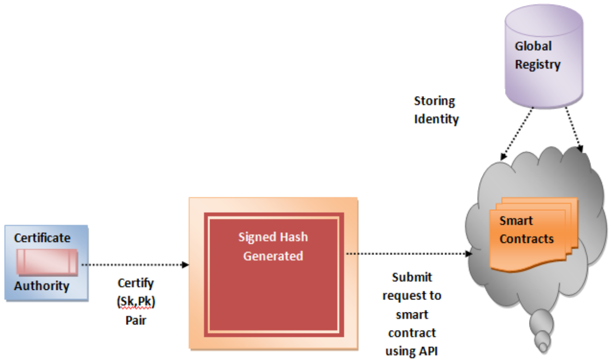


Fig 3: Identity creation and registration

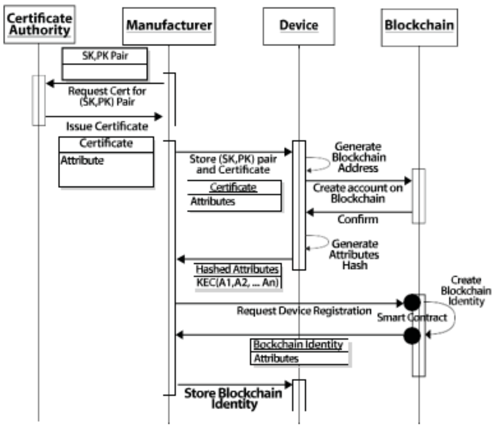


Fig 4: Detailed Process Flow for Device Identity Creation.

1) Private and public key generation: Devices start their life cy l method will authorize the manufacturer to make the device's private and public keys, and then issue an (Ethereum) Blockchain address based on the public key. We first suggested that those key pairs be certified and issued with a device certificate which should be uploaded to the device with the (manufacturer's) certificate certificate [10].

2) Digital Device Identity in Blockchain: A unique and global ID represented by a Blockchain address, used to issue a birth certificate for device ownership with contracts used for copyright and patent management.

A smart patent building contract requires each device to have its own set of cheap features using the Keccak hashing function [12] to generate a digital product ID of 20 bits. This accelerated amount will be signed using the device's private key to verify its operation and transmitted to the contract interface. A small set of symbols may include the device's phone number, device manufacturer name or other identifiers such as MAC / IP address.

Using a two-dimensional identifier, both Ethereum ads and hash symbols are also stated with a time stamp based on the current block to make an internal reference to a smart agreement. This will be used as a key indicator for maintaining the digital identity of the device in the global Blockchain registry, a fully automated overview and a detailed process shown in Fig. 3 and Fig. 4, respectively.

Therefore, digital ownership contains digital offers of the device depending on its characteristics, unique international ID representing its address, unique global address holder, ID type to show any updates, first and last block numbers and ag to show certain permissions on device ownership such as transfer, assignment , reviews and withdrawal capabilities.

B. Ownership

The deployment of IoT devices goes through the steps outlined above in the life cycle. Those steps define the owner of the device and control the transfer of ownership. Managing patent management in IoT brings a lot of attention to proprietary management to determine the actual state of the assets and the corresponding procurement management procedures. Another factor is security concerns and trust, as many attacks on an IoT device are designed to begin with the acquisition and casting of device ownership and ownership.

On the basis of IoT security [13], it is noteworthy to limit IoT devices in changing ownership throughout their lives, and an important function in identity management is to maintain device and data security throughout its life cycle. Therefore, as devices are transferred from one owner to another, the ownership management framework should support:

- A secure description of the transfer of device ownership from one user to another. Transferring device ownership will require a secure transfer process that ensures the security of sensitive device data.
- Shortcut approval. In some applications, device ownership may be separated between different owners, e.g. an IoT device in a smart home environment may belong to the employer as its data, but Hardware is still its owner or operator.

- Change of ownership should not affect device security updates. Ownership of the device and any transfer must be agnostic to security operations and processes.

Alternatively, in the proposed method, we add two other IoT device ownership requirements and ownership transfer, and this;

- Identity tracking. As device ownership changes through the life cycle and ensures the ability to research and track any device data problem and enable us to build a device’s reputation, it removes ownership through the life cycle and all transfers must be traced back to the patent source.
- Ownership and ownership. While the devices are the owner of the change, device ownership will retain their presence in the system separately from the presence.

C. Blockchain-based approach towards transfer of identity ownership

The above-mentioned requirements for device ownership management are implemented in this work with Blockchain and smart contracts. Proprietary ownership is guaranteed to meet the requirements by accepting the flexibility and features of the Blockchain and using the digital identity presented in the previous section.

The Blockchain ID created by the birth of the device is made up of a set of symbols that include the Blockchain addresses of the device itself and the original owner (man- ufacturer) in addition to other attributes. The identifiable ownership stored in this distributed charger contains many features, and the most important of this feature of the work is the address of the owner.

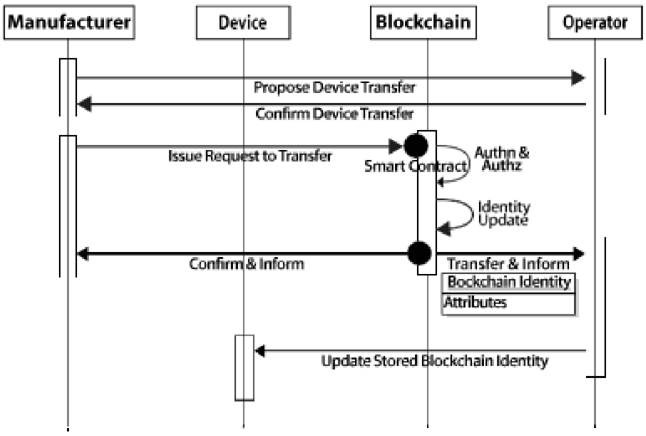


Fig 5: Detailed Process Flow for Device Identity Transfer of Ownership.

Ownership is identified with a Blockchain owner address, and by a smart contractor, the latter is limited to access to a smart contract holder only. Therefore, a transfer of ownership can only be made by the device owner, who ensures a secure transfer of ownership from one business to another. In addition, the change of ownership is based on changing the previous Blockchain owner address and the new owner address, and that may ensure the anonymity of the phone. Detailed details of this process are shown in Fig. 5.

For shortcuts, we suggest changing the concept of a different identifier with the device app. To use it, built-in Blockchain IDs are created with a data structure that contains the features described in Table. Mina.

Therefore, by using the features of the first block number and the last number in addition to the basic functions of the blockchain, device ownership and transfer of ownership can be tracked to ensure its originality and consistency. A list of all ownership updates and transfers is recorded in a data structure in a distributed ledger that will use each ID update number to store the number of block transactions being made, adding a visible chain layer to increase speed access to the track track.

D. Portability through A global and Unique Identity

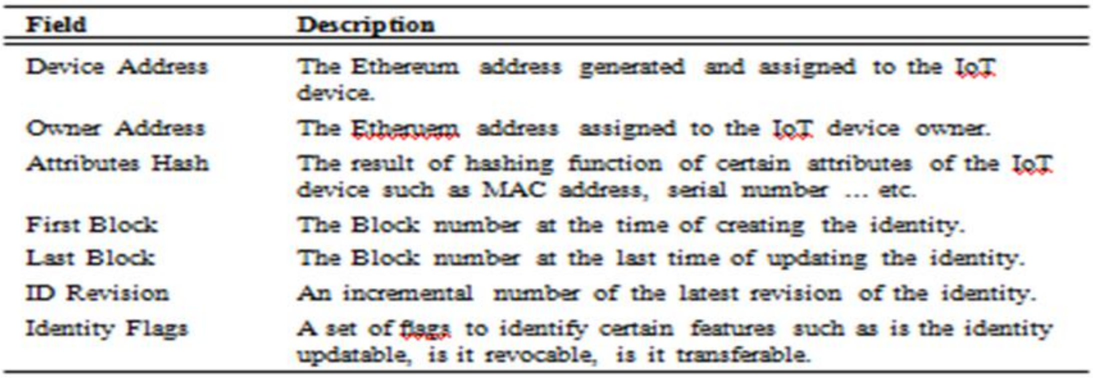
One of the key areas in which this art focuses is the land ownership and diversity of the device in addition to treating it as a living thing. Balancing these two opposing factors is proposed in this work using a blockchain-based technology and proprietary-based blockchain. This proposal brings a global and unique identity that is guaranteed to be unique in terms of the concept of using cryptographic keys. On the other hand, treating this ownership as a living asset is done through the control of revision and storage of numbers. In light of those factors that define this function the concept of BYODID as a patent management solution (will be explained in the next section). This concept uses a global and unique identity to easily facilitate the transfer and use of devices between different locations.

E. The BYODID Concept

Proposed digital ownership as a global and unique identity; but may be retained for renewal and review; you are ready for the patent of ownership. The reason for the patent is based on how devices (businesses in general) can maintain their built-in identity as they move from one system to another. This is a very important issue for

IT business networks in general and the most important ones for IoT. For example, the BYOD (Bring-Your-Device) model is one of the leading models that rely heavily on portable ownership.

TABLE 1: DIGITAL IDENTITY DATA STRUCTURE.



Field	Description
Device Address	The Ethereum address generated and assigned to the IoT device.
Owner Address	The Ethereum address assigned to the IoT device owner.
Attributes Hash	The result of hashing function of certain attributes of the IoT device such as MAC address, serial number … etc.
First Block	The Block number at the time of creating the identity.
Last Block	The Block number at the last time of updating the identity.
ID Revision	An incremental number of the latest revision of the identity.
Identity Flags	A set of flags to identify certain features such as is the identity updatable, is it revocable, is it transferable.

However, shortcut ownership purposes may still be used in the sense of device provision including the use of access rights and policy. The reason is that shortcuts can be used in long-term device transfers and may require clear boundaries between owners of what they have and what they can do. Understanding what each user or device owner can do is provided directly by the access policy description, which we do not discuss in this post. In addition, the provision of the device will allow you to deal with the conditions of the incoming connection from time to time without any change in the identity of the device. Unlike a shortcut ownership case that will require two steps for the transfer of device ownership.

F. Traceability and Auditing

In accordance with the Blockchain features and features of provenance, all transactions are stored in a distributed ledger and that cannot be modified and can be traced to genesis. This concept is promoted by many in the industry through IT networks of users (people) to enable them to enter a single user identity as they move from one business to another or from one service to another. While those methods use open and standard authentication principles such as (OpenID and OAuth2) [3], [14], however, those methods rely heavily on public intervention to simplify the user verification process. In some cases, this method is mainly to allow a single login status, but without the ownership of the identity.

In a proposed way, Blockchain's core infrastructure and digital identity diversification enables the patent management framework to provide patent authentication. Status can take up one Blockchain network and integrated Blockchains. BYODID's concept is based on a global and unique identity as well as the key identifiers that represent cryptographic keys and Blockchain addresses. These indicators will allow device ownership to be transferred between businesses and may allow you to manage your reputation and reputation history as they are transferred.

In the case of a wearable device brought by an employee to work, the standard approach would be to rely heavily on the business system to locate and validate the device and authorize it. Global ownership by BYODID may allow an IT business plan to draw (in line with global recognition) the security challenges of the device and to evaluate itself in accordance with the rules of the policy.

In some cases, such as a rented home thermostat or a connected car, the manufacturer will build the actual device ID, when transferring the device to the operator and then to the agency or user reputation.

6. Smart Contract Implementation

In this section, we present the details of using two smart contracts. The other is responsible for maintaining the registrar of organizations for activities related to the registration of registrants and authorizing access to the register by creating and updating digital ownership. The second contract covers the functions of ownership building, transfer ownership, and ownership verification.

A. Intelligent Contract Implementation Details

According to the registrar's agreement, it is assumed that a viable business or consortium will manage prudent contract management; with regard to adding a subscriber or authorizing features. Subscriber contract contains a data structure that holds all subscribers' (sellers) records and their rank. Once again, the registrant is identified by a global and unique ID based on the Ethereum address and all transactions can be subscribers (subscribers) or subscribers on the map to its Blockchain address and are protected in pairs (PK, SK).

In a global ID management contract, the contract manages all device IDs that will map each device's IDs, Blockchain address and other features into a separate digital ID. The contract contains the composition of the data per table. I, where the owner's address is the registered address, and the identity details set out one of the four factors (durable, flexible, removable, and shared). As Contract provides excellent functions related to building, updating, transferring, verifying, reporting and revoking device ownership.

Algorithm 1: Contract global registry

Require: main registrar address public address main registrar;

public struct{

```
address assignee address, String assignee details, Byte1 assignee privileges ;}
public struct {
address registrant address, String registrant details, Byte1 registrant status, Byte1 registrant privileges,
Integer registrant reputation ;}
Constructor{
main registrar            sender address; }
PolicyControlModifiers{
Is sender = main registrar; Is sender = assignee address;
Is sender = registrant address;
 Is assignee privileges = requested task;
Is registrant privileges= requested task;
Is sender credit > transaction value;}
Contract Functions{
if sender = registrar then
add assignee(); delete assignee(); update assignee();
else
retrun unauthorized;
end if
if sender = registrar    sender = assignee then
add registrant(); delete registrant(); update registrant();
else
retrun unauthorized;
   end if=0
}
```

In addition, the provision of adoption management services are a few of the methods used to control ownership and management. This includes the combined ownership of the device owner, securing subscriber rights, avoiding duplication of ownership, and ensuring that subscribers have sufficient credit. The final invitation uses Ether crypto-currency or other privately agreed tokens to enable the charging method.

Algorithm 2: Contract ID management

```
Require: main registrant address public address main registrant;
public struct{
address owner, String device,
Byte20 attributes hashedvalue Integer 1st block,
Integer last block, Integer ID revision, Byte1 identity flags, Byte1 blocked device;}
public struct{
Integer ID   revision, Integer previous blockNo ;}
Constructor{
main registrant= sender address;
owner = sender address;}
PolicyControlModifiers{
 Is sender = owner; Does ID exist;
Is registrant privileges = requested task;
Is sender credit > transaction value;}
ContractFunctions{
if sender = owner then create deviceIdentity();
update deviceIdentity();
assign device();
withdraw deviceIdentity();
else
retrun unauthorized;
end if
if sender = registrar && sender = assignee then
block device;
verifiy deviceIdentity();
else
retrun unauthorized;
end if
query deviceIdentity owner()=0;
}
```

7. Conclusion

In this paper, we have introduced a separate patent management approach to IoT, introduced a blockchain-based digital ID and a patented management system that verifies device ownership globally. This approach introduces the framework and process for patents and transfer of ownership. It provides a solution that can allow both authentication and ownership through the use of Blockchain sub-functions and features, cryptographic assets in particular, consistency, visibility, and the proposed device ID framework. The proposed approach also introduces the concept of BYODID and highlights how it can allow proprietary portability that can ensure the device is secure when mounting and transmitting from one network to another. The proposed method defines a patent management framework throughout the life cycle of the device.

Our research continues to address the issues of high-level authorization and accreditation as well as to examine Microsoft's recently released digital patent framework in partnership with the Decentralized Identity Foundation (DIF), which is aligned with this approach [15].

Finally, it is clear how Blockchain as a distributed system provides cryptographic infrastructure for experimental and operational intelligence management. However, this work does not address issues related to failure and limitations due to delays in transaction processing. These issues are the subject of ongoing research in Blockchain technology that once resolved will accelerate their acceptance into business plans.

References

1. O. Vermesan and P. Friess and P. Guillemin. ”Internet of things strategic research roadmap,” The Cluster of European Research Projects, 2009, [Online] Available: http://www.internet-of-things- research.eu/pdf/IoTClusterStrategicResearchAgenda2009.pdf.
2. M . Trnka and T. Cerny. ”Identity Management of Devices in Internet of Things Environment,” 6th International Conference on IT Convergence and Security (ICITCS), 2016.
3. D. Recordon and D. Reed. ”OpenID 2.0: a platform for usercentric identity management,” in DIM ’06: Proc. 2nd ACM Workshop on Digital Identity Management, 2006, pp. 11-16.
4. ”Identity Relationship Management 18,” Kantara Initiative, 2017, [On- line] Available: https://kantarainitiative.org/irmpillars/, Accessed March 17, 2017.
5. L. Seitz and S. Gerdes and G. Selander and M. Mani and S. Kumar. ”Use Cases for Authentication and Authorization in Constrained Environments,” RFC 7744, DOI 10.17487/RFC7744, January 2016, [Online] Available: http://www.rfc-editor.org/info/rfc774.
6. J. Chen and Y. Liu and Y. Chai. ”An Identity Management Framework for Internet of Things,” IEEE 12th International Conference (ICEBE) on e-Business Engineering, 2015, pp. 360-364.
7. Empowering the edge. Practical insights on a decentralized Inter- net of Things,” IBM Institute for Business Value. Somers, NY, United States of America, Apr. 2015. [Online] Available: https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf.
8. Linking the Physical World to the Blockchain,” Chronicled. San Francisco, CA, United States of America. [Online] Available: http://www.chronicled.com, Accessed on: Jan 12, 2017.
9. V. Buterin. ”Ethereum: A next-generation smart contract and decentral- ized application platform,” Ethereum Foundation, 2014. [Online] Avail- able: https://github.com/ethereum/wiki/wiki/White-Paper, Accessed on: Dec 5, 2016.
10. G. Wood. ”Ethereum: A secure decentralised generalised transaction ledger,” 2014. [Online] Available: http://gavwood.com/paper.pdf, Ac- cessed on Dec 8, 2017.
11. Information technology security techniques: a framework for identity management part 1: Terminology and concepts,” International Standard ISO/IEC 24760-1, 2011.
12. G. Bertoni and J. Daemen and M. Peeters and G. Assche. ”The keccak sha-3 submission,” Submission to NIST (Round 3) 6.7, 2011.
13. IoT Security Foundation, [Online] Available: https://iotsecurityfoundation.org/, Accessed on: Jan. 2017.
14. OAuth 2.0, [Online] Available: https://oauth.net/2, Accessed on: Feb. 2017.
15. Decentralized Identifiers (DIDs) v0.9, [Online] Available: https://w3c- ccg.github.io/did-spec/, Accessed on: Feb. 2018.