Intelligent logistics industry (ILI) based on Blockchain

Doaa Hegazy , Dr. Shimaa Ouf , Dr. Tarek S. Elhabian, Pr. Ibrahim El henawy

Management Information Systems El-Shorouk Academy , Faculty of Business information system (BIS) Helwan University, High Institute for Computer & I.T, El- Shorouk Academy, Faculty of computers and information Zagazig University, Egypt

***Abstract* —** *Although it has been claimed that the blockchain technology will revolutionize business and redefine logistics industry and expected to have far-reaching implications, current research is limited in terms of ways in which the blockchain's application capabilities and implications, particularly in transport and logistics. In this paper, a review of problems documented in GPS where there is a point of deficiency or defect that seems quite appropriate for improvement via blockchain technology is presented, a review of instructions in the literature on determining the applicability of blockchain technology in decision-making (Intelligent logistics industry (ILI)) as a tool designed for application to logistics it also presented, and it is proposes a designing of a blockchain-based model that can be implemented to help decision-making for naval and ship officers in determining location without the need for GPS and without relying on satellites (geospatial blockchain).*

Keywords — *Blockchain, GPS, logistics, geospatial blockchain, Intelligent logistics industry (ILI).*

.

I. INTRODUCTION

Navigation companies have problems locating when using the GPS service, which in some locations is the intended and unintended actual signal disturbance. This problem is summarized as follows: the solitary purpose of disappointment, do not sneak well inside or underground, urban thickness expands a multipath signal, vital mounting parts are not suitable for tools with long maintenance courses and mockery, i.e. deception of a GPS recipient by wrong GPS connection signals. Spatial verification already has tools for geographic verification: Google Maps, Foursquare, OpenStreet Map, and the state-backed Global Positioning System (GPS) rely on. But crypto-cartographers can't always trust them. The commercial maps data are proprietary, and their plotted features sometimes fail to reflect rapid changes in real space. Platform comes with its own hardware infrastructure, protocols, economy, and obfuscator language.

Geospatial blockchain based technology plans to create incentives for operators to build low-power, wide-area networks composed of radio beacons that can access the unlicensed radio spectrum. Zone operators on the geospatial blockchain network are in essence providing comparable work to Bitcoin miners [4].

A blockchain is potentially safer and cheaper than traditional centralised databases, is resilient to attacks, enhances transparency and accountability and puts people in control of their own data. It consists of a distributed database, a decentralized consensus mechanism, and cryptographic algorithms. Transactional data is stored in an infinite sequence of cryptographically interconnected data blocks. These blocks are ordered by a decentralized time stamping algorithm [14]. A next-generation smart contract and decentralized, which allows users to vote on the validity of database updates and eventually agree on the correct order of transactions and a shared system state at any given point in time.

As a result, the users of a blockchain system can interact without the need for a central authority that resolves conflicting views of the correct order and content of transactions. Besides decentralization, the advantages of blockchain-based systems include the absence of a central point of failure and the provision of a complete, transparent, and intrinsically valid historical transaction log. These characteristics Vehicular networks enable vehicles to generate and broadcast messages in order to improve traffic safety and efficiency. In this system, vehicles can validate the received messages from neighboring vehicles using Bayesian Inference Model. Based on the validation result, the vehicle will generate a rating for each message source vehicle.

With the ratings uploaded from vehicles, Roadside Units (RSUs) calculate the trust value offsets of involved vehicles and pack these data into a "block". Then, each RSU will try to add their "blocks" to the trust blockchain which is maintained by all the RSUs. By employing the joint Proof-of-Work and Proof-of-Stake consensus mechanism, the more total value of offsets (stake) is in the block, the easier RSU can find the nonce for the hash function (proof-of-work). Simulation results reveal that the proposed system is effective and feasible in collecting, calculating, and storing trust values in vehicular networks [7].

Within this scope, blockchains allow the resolution of conflicts by publicly providing an unforgivable record of past transactions. Smart contracts provide a tool to build on this basic structure and allow the implementation of program

logic and decentralized applications that go beyond the transfer of simple monetary values [1]. The conceptualization of trust in the blockchain context has received less attention in the field of Information Systems. Blockchain allows sharing data in a decentralized, transparent and immutable way, using a peer-to-peer network, without the need to trust any particular entity [9].

More specifically, many interdisciplinary studies focus on the impact of cryptocurrencies on traditional economic or commercial structures. Discussed topics include the adoption of cryptocurrencies in the corporate world Security and Privacy in Location Based Services for Vehicular and Mobile Communications [5].

Location-Based Services (LBSs) build upon geographic information to provide users with location-dependent functionalities. In such a context, it is particularly important that geographic locations claimed by users are trustworthy. Centralized verification approaches proposed in the last few years are not satisfactory, as they entail a high risk to the privacy of users. A novel decentralized, infra-structure independent proof-of-location scheme based on blockchain technology is presented and evaluated [2]. An oracle run by a mobile network provider can submit network-based positioning information to the contract that compares it with the geofence [19].

Military Intelligence Applications for blockchain Technology suited for improvement via blockchain technology. Guidance from the literature related to determining blockchain technology applicability and proposes a decision aid tailored to military intelligence perspectives. Also propose applying batch queuing theory to enable 11 initial feasibility studies and present analysis toward the first known case study of military intelligence incorporation of blockchain technology, a project reviewing blockchain applicability to an intelligence database that stores geographic locations of units of interest [10].

From the earliest forms of navigation, cartographers' work has been a vital tool upon which commerce and development rely. FOAM Crop have gone from hand drawn maps and non-standardized measurement tools like footsteps, to centralized cartography projects of ordnance surveys, to the most recent high-tech developments in digital cartography that rely on the work done by satellite imaging, geographic information systems and even street view problems [15].

II. BLOCKCHAIN BACKGROUND

Blockchain is a decentralised, immutable, and cryptographically secure distributed ledger technology (DLT), broadly used to eliminate the need for trust in data transfer, and well known for powering the Bit coin crypto currency [1].

A. Blockchain Architecture

A blockchain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain. The first block in the chain is called the **Genesis block**. Each new block in the chain is linked to the previous block. A block also has a hash; it can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique. So once a block is created, any change inside the block will cause the hash to change. Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block. Fig. 1 reveals that every block contains a block header and a varying number of transactions stored in a tree structure. In addition, every block header contains a timestamp and two hash values: one for a previous block's header and another for all the transactions that are carried within that block. Because of this, it is possible to verify the integrity of the whole block, including all the transactions via block header [21].

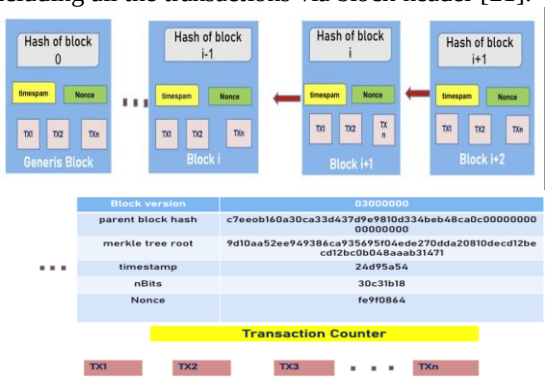

Fig. 1: Blockchain Architecture

Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure. Therefore, changing a single block can quickly make all following blocks invalid.

B. Properties of blockchains

The distribution element of blockchain as a distributed ledger refers to the design of the system on which the blockchain is running and the number of individuals or organizations that control or own said computers. DLTs are built on consensus utilizing algorithms to find agreement among participants [e.g., Proof of Work (PoW), Proof of Stake (PoS)], data replication, and peer-to-peer (P2P) networking.

Decentralization is a subset of distribution concerning ownership and control of the data on the system and decisions about the system itself [2]. Decentralization allows resisting system failure, attacks and manipulations, and collusion of participants. Simply put, increasing the number of participants and the number of unique owners across the system reduces the chance of the system failing or taking over. If a computer stores all data and that

computer fails or is compromised, the system will not be able to recover. Decentralization largely prevents this from happening.

Cryptography is another major property of blockchain technology responsible for several major functions, including proof of data/asset ownership and data validation. Two forms of cryptography commonly employed with blockchains are one-way hashing functions, such as SHA-256 (Secure Hashing Algorithm), and asymmetric encryption (i.e., two-way function) utilizing public and private keys [1], [3]. Each of these tools has a role in securing and proving ownership and preventing non-consensus driven modifications to the ledger. In the case of a one-way hashing function (e.g., SHA-256), the hash of data put into the function cannot be used algorithmically to find what the original data were [4].

Asymmetric encryption, known as public key encryption, is a two-way cryptographic function. It will begin with data and encrypt or scramble them using a key pair, rendering them (the data) useless if they ended up in the possession of anyone not in possession of the requisite key. These encrypted data, however, can be decrypted by the receiving party if they possess the correct key. Public key encryption can be used in two basic ways: to encrypt data that only the private key holder can decrypt and use, and to prove that data came from a trusted source by "signing" with a private key. Imagine a document containing sensitive information while examining two use cases for asymmetric encryption [5]. Hashing and asymmetric encryption are excellent tools used in many different applications.

The final property of blockchain technology is immutability. Immutability implies some data, in this case a record of some type of transaction, cannot be tampered with or changed, only appended. Immutability is conferred from both the distributed nature and the cryptographic tools used for the blockchain. Notably, blockchains do not always have perfect immutability. Rather, through correct implementation and decentralization, ensuring no party owns or controls the majority of the nodes in the blockchain network, is immutability able to be relied upon. Immutability is the by-product of cryptographic security and decentralization. When considering immutability, one must be sure to recognize how it is generated from cryptography and decentralization.

The hash is one layer of protection leading to immutability. Since each block is linked to the next based on its hash, we know that any change that occurs in the data will drastically change the hash value [6]. Every block in the chain that comes after the adulterated block will be invalid. This means that in order to change one block and re-mine its value to validate it, all blocks coming after will also need to be re-mined. This is a very high cost barrier to overcome for robust networks [7-8]. Suppose that an attack here was successful though; our next layer of protection leading to immutability is the distribution and decentralisation. Not only does the entirety of the blockchain after the affected block need to be re-mined, but at least 51% of all distributed copies also need to be modified and subsequently re-mined for the change to take effect [1], [3]. This raises the cost of an attack even more, and demonstrates why, if implemented and maintained correctly, immutability is very reliable.

III. THE VULNERABILITIES OF GPS

Currently there is no reliable and trusted location verification service. It is problematic to rely on GPS and it is not a viable tool when a smart contract needs to execute autonomously on spatial information. A backup for GPS is needed because it can be easily spoofed, jammed, or falsified. This means that there is currently no truly secure way to verify location in blockchain based smart contracts or decentralized applications. GPS is the premier Global Navigation Satellite System (GNSS), consisting of 31 satellites launched by the U.S. for military use and then for civilian and commercial use.

Civil GPS is unencrypted, it has no proof-of-origin or authentication features, and despite dire warnings first raised in 2012, the system remains extremely susceptible to fraud, spoofing, jamming, and cyberattack. Operational Control System (OCX), the putative next generation of GPS "will be the first satellite control system designed after the advent of significant jamming and other cyber threats." However, the project has been continuously delayed, with a scheduled launch date now in 2022. Even so, the OCX design fails to address vulnerabilities, "GPS competitiveness as a worldwide civil system will diminish." The limitations of GPS require at least four beacon signals to be overhead, which makes indoor localization nearly impossible. Urban density and skyscrapers also cause difficulties in receiving four messages and the issue of multi-path signals occurs within the vicinity of high rise buildings. Further, for a device, it can take multiple minutes to acquire an accurate coordinate. When it comes to power consumption, GPS is a drain on battery and is not feasible for low powered Internet of Things (IoT) devices. The goal of Proof of Location is therefore to provide consensus on whether an event or agent is verifiably at a certain point in time and space while accounting for the above vulnerabilities inherent in GPS [15].

IV. GEOBLOCKCHAIN

Bitcoin's recession in recent years has implied that the technology platform on which the cryptocurrency is based on the blockchain has become a well-known and familiar name. Simply put, the blockchain is not perishable from transactions that are securely deployed across a peer-to-peer network. These transactions do not need to be financial in nature. It can be anything as long as it is

valuable. Because the nature of the technology, so that the transaction log is not owned by any one entity. A block is part of a decentralized database and connected to the input before and after it, forming a series of irreversible and irreversible events. As such, this technology is not only able to penetrate piracy, but also promotes transparency and accountability. Hence, technology giant IBM is convinced that this technology will work for businesses on what the Internet has done to communicate. We are convinced that site awareness and visualization all play a major role in the blockchain ecosystem.

Currently, there are no standards for embedded locations, physical addresses, or coordinates in smart contracts. In order for smart contracts to remain interoperable, they will need a shared language for them to reference and index the physical world. Throughout history, there have been many ways of encoding physical location into addresses from longitude and latitude all the way to the more recent geohash. While autonomous car companies are racing for more accurate location data, the fact remains that most of the Earth's surface lacks addresses. According to the United Nations, 70% of the world is unaddressed, including more than half of the world's sprawling urban developments.

A. Adding proof of location to blockchain

Of course, we already have tools for geographic verification, Google Maps, Foursquare, Open Street Map, and the state-backed Global Positioning System (GPS) they rely on. But crypto-cartographers say we can't always trust them. The commercial maps' data are proprietary, and their plotted features sometimes fail to reflect rapid changes in real space. Crowdsourced tools such as OpenStreetMap are dogged by problems: insufficient funding, confusing usage policies, the failure to create incentives for contributors, and difficulty with accuracy. And GPS, some critics say, is poorly suited for use in dense urban environments and indoors, drains cell phone batteries, and is centralized (a big downside for blockchain advocates). According to PoL upstart Foam, "Civil GPS is unencrypted, it has no proof-of-origin or authentication features, and despite dire warnings first raised in 2012, the system remains extremely susceptible to fraud, spoofing, jamming, and cyberattack.

As a keeper of records, a regular blockchain tells the users 'what' transaction has happened. But if an immutable proof of location is also associated with the blockchain, it is empowered to reveal 'where' that transaction has happened. Bring sensors to the mix and you will be able to understand the circumstances also under which the transaction took place. Spatially-enabled blockchains enable highly-accurate spatiotemporal mapping of physical world events. And several industries stand to benefit from these geo-blockchains.

So the blockchain now allows data to be shared in a secure, verified, and transparent manner, and this stands true for location data as well. When location records are transferred over a blockchain, it is a confirmation that people and assets are where they say they are. In the case of crowdsourced spatial data, which is no stranger to problems like vandalism, the blockchain acts as a proof of location. Whereas for companies that provide commercial geospatial data, sharing the information using blockchain protocol helps to ensure that the data is going to authorized customers only. Currently, there are no standards for embedded locations, physical addresses, or coordinates in smart contracts. In order for smart contracts to remain interoperable, they will need a shared language for them to reference and index the physical world.

The FOAM protocol will enable different agents, parties and smart contracts to negotiate with each other on top of shared location data. Smart contract protocols need to be modular so that diverse network participants can be connected, from users to developers and service providers. Being a protocol allows FOAM to be detached from any singular application or use case, creating open building blocks that anyone can access and use in their applications. Implementation-wise, FOAM [48] is a good example of a geospatially-enabled blockchain using a crypto-spatial coordinate (CSC) system. A FOAM blockchain does not just record an entry's specific time, but also requires and validates its associated proof of location, giving an immutable spatial context that regular blockchains lack, and allowing the accurate mapping of physical world events in a temporal sequence [46], [49- 50].

B. Crypto-Spatial Coordinate

Crypto-Spatial Coordinates (CSC) are Ethereum smart contract addresses with corresponding addresses positioned in physical space that are verifiable both on- and off-chain. This allows for physical addresses in the built environment to have a corresponding smart contract address that is accessible for decentralized applications.

The CSC standard can be adopted by any smart contract to make a claim to, or reference, a location in the physical environment. When adopted across verticals and use cases, the CSC allows smart contract transaction activities to take on a spatial dimension as shown in Fig.2.

The CSC acts as an index for spatial events that works for any kind of transaction on the blockchain. Since geohashes are basically hierarchical, it also means that a contract referencing a building, and a contract referencing an IoT device located within that building, automatically have a spatial relationship Another benefit of the geohash standard is that it is in the public domain. This doesn't mean that the geohash doesn't have limitations. Therefore, it allows

for changing this in future versions if we find it to be too limiting [15].

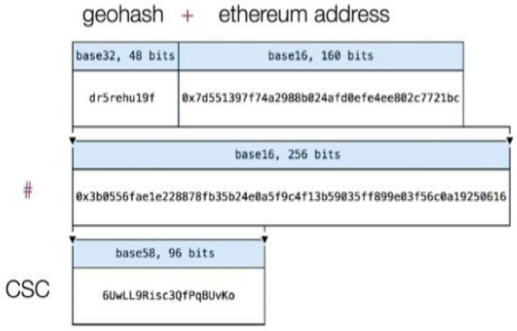

Fig. 2 Crypto-Spatial Coordinate

V. INTELLIGENT LOGISTICS INDUSTRY SUGGESTED SYSTEM MODEL

We consider a set of IoT devices (called nodes) that collaborate together to determine their position. The model has the following features: Decentralization, P2P Communications: The IoT devices communicate with its neighbour's nodes to determine their positions, in a peer-to-peer network architecture, no central trust: does not require a central trusted entity that manages the security between nodes or detects the existing of malicious nodes.

According Foam plan the operators will build low-power, wide-area networks composed of radio beacons that can access the unlicensed radio spectrum.

There are a number of radio technologies and techniques for localization/positioning systems without the use of GPS. These alternative position systems use a range of localization processes and techniques, which include Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA) and Received Signal Strength (RSS).

Among WiFi, RFiD and cellular radio a new class of radio that is emerging and highly promising for internet of things devices called Low Power Wide Area Networks (LPWAN) [15].

This technology is at the core of the geoblockchain vision for its ability to scale, cover large distances and remain available due to the low power. A node on the geoblockchain network will need to offer accurate time synchronization over radio transceivers. This kind of beacon is called a zone Anchor [8], [15].

The zone anchors then timestamp, Location can be triangulated via timestamp differences. Mobile actor can then cryptographically prove it was the creator of the message. Zone Anchor beacons use Byzantine fault tolerant clock synchronization. So the above theory mainly considers faulty parties that may have errors about their time or position. But in the crypto world we also need to consider adaptive malicious actors.

The PoL of a mobile beacon is provided by 4 zone-anchors that have formed a zone and can synchronize clocks with the mobile beacon and sign messages. zone Anchor beacons running the geoblockchain protocol will need to provide accurate time synchronization for a set period of time in order to not be seen as faulty. A distributed system is Byzantine fault tolerant when the coordination of untrustworthy participants will always convey honest information, given more than 2/3 act honestly. It is important that a time synchronization is able to self-stabilize if a number of nodes are broken or malicious [8].

All radio frequency (RF) location systems rely on clock precision. The most accurate approaches require clock synchronization. use a BFT clock synchronization algorithm to provide the best possible support for RF Time of Flight algorithms. The Proof of Location protocol is open for Zones to autonomously form and operate as utility providers that compete for transactions fees by providing location verification services.

The crypto-economic staking incentives to grow network coverage and utilize a validator set for fraud proofs, and enforce protocol rules. Safety deposits allow for attributable byzantine behaviour in the form of slashing conditions. The system further encompasses a data store and validator set, the specifics of these mechanisms will be detailed in a forthcoming post [8].

A. The Proof of Location protocol

Intelligent logistics industry (ILI) blockchain model seven-layer conceptual model for characterizing and standardizing the typical architecture and major components of blockchain systems, and briefly describes its underlying key techniques. Due to space limitations, the technical details for implementation are beyond the scope of this paper and thus are omitted. As is shown in Fig., similarly as the well-known open system interconnection reference model, the blockchain model has seven layers stacked as below.

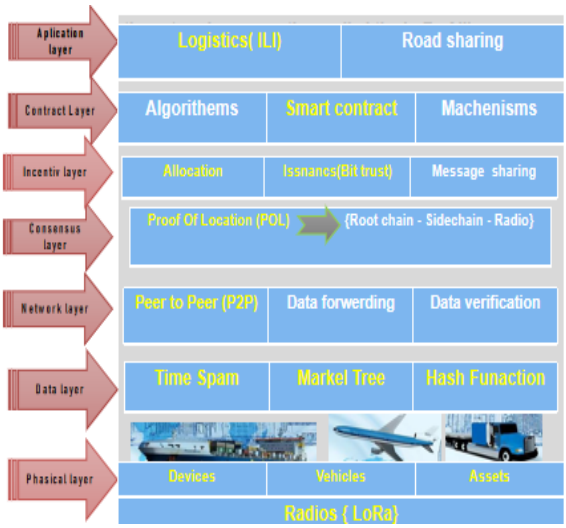

Fig. 3: : seven-layer protocol model

Physical Layer: The physical layer encapsulates various kinds of physical entities (e.g., devices, vehicles, assets and other environmental objects). The key technique in this layer is IoT, which enjoys enhanced device security and data privacy when integrated with blockchain. Large numbers of physical entities, nowadays typically managed by central authorities in intelligent logistics industry (ILI). ILI entities can establish a secured and trusted communication network on blockchain and also form a self-organized, self-adaptive, and decentralized autonomous ILI ecosystem.

The Proof of Location protocol is open for four or more zone anchors form a zone, the quorum that maintains clock sync for a given region. Once synchronized, the zone can determine the location of a requesting node by using time of arrival measurements to verifiably triangulate position. One of the most promising new radios is a called LoRa, a physical layer technology that can travel 5–15km at 150 MHz and 1 GHz bands, which can provide bidirectional communication with a special chirp spread spectrum (CSS) techniques for long range with properties that make it harder to detect or jam.

There is already the enterprise consortium called the LoRa Alliance, designing an open standard and defining architecture and layers above the LoRa physical layer. Further there are open development communities in major cities around LoRa open libraries cantered around the Things network. Because these radios allow for bidirectional communication, mesh network topology significantly extends range.

Data Layer: This layer process the data blocks with cryptography features such as hash algorithm, Merkle tree to make secure blocks. A Merkle root is the hash of all the hashes of all the transactions that part of a block in a blockchain network. Every transaction on the blockchain network has a hash associated with it. However, these hashes are not stored in a sequential order on the block, rather in the form of on upside down tree structure, each transaction is hashed, then each pair of transaction hashes is concatenated and hashed together, and so on until there is one root hash for the entire block.

As shown in Fig.4. each computing node wining the consensus competition will be empowered to create a new block, packaging all transportation-related data generated within a specific time period into a Merkle-tree structured data block with time-stamps indicating the creating time of this block.

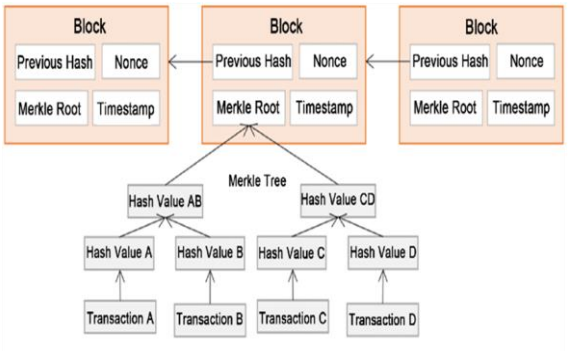

Fig. 4: Merkle tree

Network Layer: The network layer specifies the mechanisms of distributed networking, data forwarding and verification. Therefore, a geospatial blockchain for intelligent logistics industry (ILI) can be topologically modelled as a P2P network. Peers are equally privileged, equipotent participants without any central coordinator or hierarchical structure, and can be categorized into full-client and lightweight nodes. The former has a complete copy of all blockchain data since the genesis block, while the latter (typically smartphones, IoT devices, etc.) only have a small fraction but can request the necessary data from neighbouring nodes using specific protocols.

Once a piece of data or a new block is created, it will be broadcast to the network, to which all nodes keep listening. Each node will have verified the received data or new blocks according to predefined specifications, discard invalid ones and forward the others to neighbouring nodes. This way, data or blocks passing verification from a majority of nodes will be appended into blockchain. As such, blockchain can be viewed as the next generation of "completely decentralized" big data technology.

Blockchain data is stored on each and every node, and can be easily synchronized and restored even in the worst case of failure in all but one node. This is particularly useful in communication and interaction among intelligent logistics industry (ILI) entities.

Incentive Layer: This layer incorporates economic reward into blockchains, and specifies its issuance and allocation mechanisms.

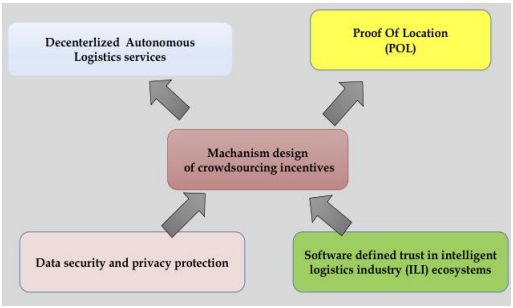

Fig. 5: Incentive Layer mechanisms

Blockchain can possibly help build up a verified, trusted and decentralized intelligent logistics industry (ILI) biological system. Be that as it may, from a

explore point of view, a few key research gives still need to be tended to for geospataial blockchain for intelligent logistics industry (ILI) to arrive at its maximum capacity. In this segment, we abridge the essential research issues as appeared in Fig., and quickly talk about the related research openings and potential experiences.

Each computing node (e.g., IoT) devices, vehicles, or other entities with computing power) can be viewed as an autonomous "agent" in this (ILI). Large numbers of nodes can be connected and communicate with each other via various kinds of blockchain based decentralized Apps (Dapps), resulting in decentralized autonomous organizations (DAOs) dedicating to specific requirements or scenarios, and in the macro-level forming a decentralized autonomous system and even society (DAS).

1) ***Mechanism design of crowdsourcing incentives:*** Essentially, the distributed consensus competition can be viewed as a crowdsourcing task to large numbers of ITS nodes, which contribute their computing power to verify blockchain data. These nodes are self-interested agents, so that incentive compatible crowdsourcing mechanisms must be designed to make individual behaviour of revenue maximization aligned with the system-wide target of guaranteeing a secured and trusted ITS ecosystem. Equipped with such mechanisms, blockchain can be used to aggregate all possible computing resources in ITS to solve previously intractable problems.

2) ***Software defined trust in intelligent logistics industry (ILI):*** Blockchain-powered trust plays a significant role in building a decentralized and disintermediated intelligent logistics industry (ILI), making it possible for lots of application scenarios including point to point trading, payment and communication. This kind of trust is guaranteed by code, mathematics and verification from the majority, and thus can be considered as "software-defined" trust. It has the potential of greatly reducing the structural complexity and in turn social complexity of intelligent logistics industry (ILI), making it possible for money and asset flowing freely among intelligent logistics industry (ILI) entities.

3) ***Proof Of Location and Smart contract:*** serves as an "activator" of blockchain, endowing static data with diversified algorithms and high-level business logics to build a programmatic intelligent logistics industry (ILI) and improve the intelligence of intelligent transportation system (ITS) applications. The self-executing smart contracts also significantly reduce the social complexity of ITS by lowering the importance of human factor, and can act as software agents on behalf of their creator or even themselves. Therefore, there is a critical need to study the design and implementation of specific smart contracts, as well as smart-contract-based intelligent logistics industry (ILI) management and control.

4) ***Data security and privacy protection blockchain:*** has shown strong robustness to security risks and threats in cryptocurrencies, its asymmetric encryption framework should be further strengthened in intelligent logistics industry (ILI) scenarios with large numbers of lightweight devices so as to protect against the possibly easier 51% attacks.

Consensus Layer: The consensus layer packages all possible consensus algorithms. Generally speaking, efficiently reaching consensus in decentralized systems has long been an important question in distributed computing and intelligent logistics industry (ILI).

One of blockchain's key advantages is promoting all decentralized nodes reaching consensus on the data validity, which is the foundation of mutual trust among nodes. Various kinds of consensus algorithms have been designed. Creating architecture that can be summarized as follows:

- Incentivization for producing and validating location data (Presence claims) can be governed using smart-contracts on Ethereum.Bottom.
- The data produced can be transmitted to and validated on local blockchains and produce cryptographically proven Presence claims.
- Consumer radio hardware run a byzantine fault-tolerant time. Three radios are consistently engaging in a time synchronization protocol over radio and thus have the ability to locate a user within their reach.

Contract Layer: This layer packages various scripts, algorithms and smart contracts, which serve as important activators to the static data, money or assets stored in blockchain. To be specific, smart contracts are a group of self-verifying, self-executing, and self-enforcing state-response rules that is stored on and secured by the blockchain. Generally speaking, once two or more parties consent to all of the terms within the contract, they cryptographically sign the smart contract and broadcast it to the P2P network for verification.

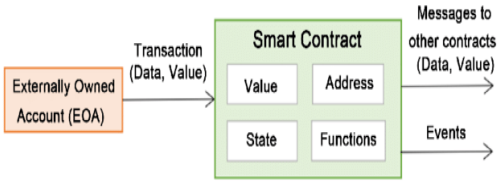

Fig. 6 Contract Layer operations

Smart contract is similar to legal document, create terms between two parties. Smart contract is coded, self -executing digital contract. It helps to exchange money, property, shares, or anything of value in a

transparent, conflict-free way, smart contract try to avoid the services of a middleman. Smart contracts can exist without the blockchain but the smart contracts naturally sit on the blockchain layer to enhance trace ability and trust, contracts use public ledger for storage purposes.

Application Layer: This layer packages potential application scenarios and use cases of geospatail blockchain for intelligent logistics industry (ILI). In practice, blockchain technology is still in its infancy, especially logistics serves. However, lots of novel business models and start-up companies have been emerged in many areas including blockchain-based logistics serves data storage and verification, P2P trading and payment, asset management, among others.

VI. CONCLUSIONS

A preliminary study on the emerging geoblockchain for decentralizes system and its potential applications in logistics research are presented. The goal of the Proof of Location protocol is to provide the framework and infrastructure to develop a decentralized, privacy preserving, highly accurate, censorship resistant alternative to the Global Positioning System (GPS). We design ITS-oriented, seven-layer conceptual model, propose the research framework of blockchain based intelligent logistics industry (ILI) and discuss its key research issues.

REFERENCES

[1] Xiwei Xu NICTA, "*The blockchain as a software connecter"* Australia CS,2016

[2] Michele Amoretti, Giacomo Brambilla, Francesco Medioli, Francesco Zanichelli "*Blockchain-based Proof of Location "*University of Parma, Italy,2018 .

[3] John R. Douceur. "*The Sybil attack. In Proceedings of the First International Workshop on Peer-to-Peer Systems* " pages 251–260, 2002.

[4] Ji Fang, Cao Yan, and Chen Yan. "*Centralized identity authentication research based on management application platform. In Proceedings of the First International* "Conference on Information Science and Engineering", pages 2292–2295, 2009.

[5] Yuan Zhuang,Yuan Zhuang,Jun Yang,"*Towards Positioning, Navigation, and Location Based Services (PNLBS) for Internet of Things*",IEEE Internet of Things Journal Special Issue on http://mc.manuscriptcentral.com/iot

[6] Weimin Luo, Jingbo Liu, Jiang Xiong, and Ling Wang. "*Defending against whitewashing attacks in peer-to-peer file-sharing networks.* In Proceedings of the 4th International Conference on Computer Engineering and Networks", pages 1087–1094, 2015.

[7] Satoshi Nakamoto. *"Bitcoin: A peer-to-peer electronic cash system[online]*". available: https://bitcoin.org/bitcoin.pdf, 2008.

[8] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. "*Bitcoin and Cryptocurrency Technologies*" A Comprehensive Introduction. Princeton University Press, 2016.

[9] (2009) Bitcoin NS. "*A peer-to-peer electronic cash system*". Bitcoin.org [online]. . https://bitcoin.org/bitcoin.pdf. Accessed 14 June 2018.

[10] Buterin V. "*The meaning of decentralization. Medium [online].. 2017*". https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Accessed 14 June 2018.

[11] Goldreich O. "*Foundations of cryptography: volume 1, basic tools. Cambridge: Cambridge University Press*"; 2008.

[12] Waldman J. Blockchain—Blockchain fundamentals. MSDN [online]. 2018 Mar. https://msdn.microsoft.com/en-us/magazine/mt845650.aspx. Accessed 14 June 2018.

[13] Sedgwick K. "*You can now 51% attack a coin for as little as $500. Bitcoin.com [online]".* 2018 May. https://news.bitcoin.com/you-can-now-51-attack-a-coin-for-as-little-as-500/. Accessed 14 June 2018.

[14] Walport M. "*Distributed ledger technology: beyond block chain*". UK Government Office for Science, 2015, pp. 1–88. https://assets.publishing.service.gov.uk/government/uploads /system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Accessed 14 June 2018.

[15] Gordon W, Wright A, Landman A. "*Blockchain in health care: decoding the hype*". NEJM Catalyst [online]. 2017 Feb. https://catalyst.nejm.org/decoding-blockchain-technology-health/. Accessed 14 June 2018.

[16] Roehrs A, da Costa CA, da Rosa RR. OmniPHR: "*a distributed architecture model to integrate personal health records".* J Biomed Inform. 2017;71:70–81. https://doi.org/10.1016/j.jbi.2017.05.012.

[17] Piper Jaffray—Research (2018). http://www.piperjaffray.com/3col.aspx?id=103. Accessed 14 June 2018.

[18] Hashed Health (2018). https://hashedhealth.com/. Accessed 14 June 2018.

[19] Geer L. "*Illinois opens Blockchain development partnership with hashed health*". The Illinois Blockchain Initiative [online]. 2017 Aug. https://illinoisblockchain.tech/illinois-opens-blockchain-development-partnership-with-hashed-health-fe3891e500bb. Accessed 14 June 2018.

[20] "*Professional Credentials Exchange*" (2018). https://www.procredex.com/. Accessed 14 June 2018.

[21] Naujeck J. Blockchain is the 'shiny new penny'. The Ledger (Nashville Edition). 2018;42(20): online. http://www.tnledger.com/editorial/Article.aspx?id=106706 (requires access from a US IP address). Accessed 14 June 2018.

[22] Chaudoin K. *"College of pharmacy & health sciences, hashed health partner to develop innovative system to verify graduation credentials using blockchain technology*". LIPSCOMB now: [online]. 2017 Dec. https://www.lipscomb.edu/news/filter/item/0/32178. Accessed 14 June 2018.

[23] GitHub—decentralized-identity/hubs: Storage and compute nodes for decentralized identity data and interactions. GitHub [online]. 2018. https://github.com/decentralized-identity/hubs. Accessed 14 June 2018.

[24] "*Decentralized Identity Foundation. Decentralized Identity Foundation Grows To 56 Members In Our First Year*". Medium [online]. 2018 May. https://medium.com/decentralized-identity/decentralized-identity-foundation-grows-to-56-members-in-our-first-year-3ec117e811d8. Accessed 14 June 2018.

[25] Clauson KA, Breeden EA, Davidson C, Mackey TK. "*Leveraging blockchain technology to enhance supply chain management in healthcare. Blockchain Healthc*" Today. 2018;1:20. https://doi.org/10.30953/bhty.v1.20.

[26] Bell L, Buchanan WJ, Cameron J, Lo O. "*Applications of Blockchain within healthcare. Blockchain Healthc Today*". 2018;1:8. https://doi.org/10.30953/bhty.v1.8.

[27] IBM. Blockchain for supply chain (2018 Jun). https://www.ibm.com/blockchain/supply-chain/. Accessed 14 June 2018.

[28] Gammon K. "*Experimenting with blockchain: can one technology boost both data integrity and patients*" pocketbooks? Nat Med. 2018;24(4):378–81. https://doi.org/10.1038/nm0418-378.

[29] Benchoufi M, Ravaud P. "*Blockchain technology for improving clinical research quality*". Trials. 2017;18(1):1–5. https://doi.org/10.1186/s13063-017-2035-z.

[30] Choudhury O, Sarker H, Rudolph N, Foreman M, Fay N, Dhuliawala M, Sylla I, Fairoza N, Das AK." *Enforcing human subject regulations using blockchain and smart contracts. Blockchain Healthc Today*". 2018;1:10. https://doi.org/10.30953/bhty.v1.10.

[31] Kuo TT, Kim HE, Ohno-Machado L. "*Blockchain distributed ledger technologies for biomedical and health care applications"*. J Am Med Inform Assoc. 2017;24(6):1211–20. https://doi.org/10.1093/jamia/ocx068.

[32] Roman-Belmonte JM, De la Corte-Rodriguez H, Rodriguez-Merchan EC." *How blockchain technology can change medicine*". Postgrad Med. 2018;130(4):420–7. https://doi.org/10.1080/00325481.2018.1472996.

[33] Ward G. April Nashville Blockchain Meetup. Hashed Health [online]. 2018 Apr. https://hashedhealth.com/april-nashville-blockchain-meetup/. Accessed 14 June 2018.

[34] Tennessee (State). Legislature. General Assembly. Amendment to Tennessee Code Annotated, Title 12; Title 47; Title 48; Title 61 and Title 66, relative to electronic transactions—SB 1662 (Dickerson), HB 1507. 2018. http://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=HB1507. Accessed 14 June 2018.

[35] Orcutt M. States that are passing laws to govern "*smart contracts" have no idea what they're doing. Legislation meant to clarify things for blockchain developers could end up hurting innovation*. MIT Technology Review (online). 2018 Mar. https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/. Accessed 14 June 2018.

[36] (Anonymous). The $272 billion swindle. "*Why thieves love America's health-care system"*. The Economist [online]. 2014 May. https://www.economist.com/united-states/2014/05/31/the-272-billion-swindle. Accessed 14 June 2018.

[37] Dyer O. "*Medicare's top billing doctor is convicted of medical fraud*". BMJ. 2017;357:j2188. https://doi.org/10.1136/bmj.j2188.

[38] Bellod Cisneros JL, Aarestrup FM, Lund O. Public health surveillance using decentralized technologies." *Blockchain Healthc*" Today. 2018;1:17. https://doi.org/10.30953/bhty.v1.17.

[39] McKernan KJ. "*The chloroplast genome hidden in plain sight, open access publishing and anti-fragile distributed data sources*". Mitochondrial DNA A DNA Mapp Seq Anal. 2016;27(6):4518–9. https://doi.org/10.3109/19401736.2015.1101541.

[40] (Anonymous). "*Rise in Population Genomics: Local Government in India Will Use Blockchain to Secure Genetic Data. The Medical Futurist [online]"*. 2018. http://medicalfuturist.com/rise-in-population-genomics-local-government-in-india-will-use-blockchain-to-secure-genetic-data/. Accessed 14 June 2018.

[41] Kamel Boulos MN, Al-Shorbaji NM. "*On the Internet of Things, smart cities and the WHO Healthy Cities*". Int J Health Geogr. 2014;13:10. https://doi.org/10.1186/1476-072X-13-10.

[42] Kamel Boulos MN, Tsouros AD, Holopainen A. '*Social, innovative and smart cities are happy and resilient': insights from the WHO EURO 2014 International Healthy Cities Conference*. Int J Health Geogr. 2015;14:3. https://doi.org/10.1186/1476-072X-14-3.

[43] Ellehauge J. "*Blockchain in geospatial applications. GIM* "Int. 2017;31(5):43–45. https://www.gim-international.com/content/blog/blockchain-in-geospatial-applications-2?output=pdf. Accessed 14 June 2018.

[44] Jonuschat H, Crespi B, Nagel I, Garcia Canales J, Akkermans L, van Den Bergh G. "*Guide2Wear mobile devices for the future traveller (Public transport services with wearable devices for different mobility types)—Deliverable D3.1: Overview on functionalities of technologies for seamless travelling. Guide2Wear EU-funded Project, 2015 Feb"*. http://www.tmleuven.be/project/guide2wear/G2W_D3.1.pdf. Accessed 14 June 2018.

[45] Zipline—Lifesaving Deliveries by Drone (2018). http://www.flyzipline.com/. Accessed 14 June 2018.

[46] Thaa B. "*3 ways GIS and blockchain technology are shaping the future. GEOSYMP [online]"*. 2017 Aug. https://geosymp.com/3-ways-gis-blockchain-technology-are-shaping-the-future/. Accessed 14 June 2018.

[47] Dasgupta A. "*The Game Changer of Geospatial Systems—Blockchain. Geospatial World [online]"*. 2017 Sep. https://www.geospatialworld.net/article/blockchain-geospatial-systems/. Accessed 14 June 2018.

[48] Fierro N. "*How Augmented Reality can change how we navigate a natural disaster. MIMIR Blockchain*" Publication on Medium [online]. 2017 Sep. https://medium.com/mimir-blockchain/how-augmented-reality-can-change-how-we-navigate-a-natural-disaster-d7fbde0d735b. Accessed 14 June 2018.

[49] FOAM. 2018. https://www.foam.space/. Accessed 14 June 2018.

[50] Anderson J. FOAM: The Future of Geospatial Data, on the Ethereum Blockchain. Steemit [online]. 2017 July https://steemit.com/ethereum/@protegeaa/foam-the-future-of-geospatial-data-on-the-ethereum-blockchain. Accessed 14 June 2018.

[51] Tewelow W. "*Bitcoin, blockchain and GIS could change the world. Geospatial Solutions [online]"*. 2018 Mar. http://geospatial-solutions.com/bitcoin-blockchain-and-gis-could-change-the-world/. Accessed 14 June 2018.

[52] Orcutt M. "*How to get blockchains to talk to each other. MIT Technolohy Review [online]"*. 2018 May. https://www.technologyreview.com/s/611187/how-to-get-blockchains-to-talk-to-each-other/. Accessed 14 June 2018.

[53] Orcutt M. "*How secure is blockchain really? MIT Technology Review [online]"*. 2018 Apr. https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/. Accessed 14 June 2018.

[54] Orcutt M. Self-serving cryptocurrency miners are attacking small blockchain networks. MIT Technology Review [online]. 2018 May. https://www.technologyreview.com/the-download/611238/self-serving-cryptocurrency-miners-are-attacking-small-blockchain-networks/. Accessed 14 June 2018.

[55] Silver A. "*3 Obstacles to Moving Social Media Platforms to a Blockchain. IEEE Spectrum [online]"*. 2018 May. https://spectrum.ieee.org/tech-talk/computing/networks/3-obstacles-to-moving-social-media-platforms-to-a-blockchain. Accessed 14 June 2018.

[56] PubMed query using the keyword 'blockchain' (retrieved 40 items on 13 June 2018). https://www.ncbi.nlm.nih.gov/pubmed/?term=blockchain. Accessed 14 June 2018.

[57] Maxmen A ."AI researchers embrace Bitcoin technology to share medical data". Nature. 2018;555(7696):293–4. https://doi.org/10.1038/d41586-018-02641-7.

[58] Corbyn Z. How can I make money from my DNA? The Guardian [online]. 2018 Feb. https://www.theguardian.com/science/2018/feb/18/genetics-how-do-you-make-money-from-your-dna. Accessed 14 June 2018.