Blockchain: Research and Applications 2 (2021) 100033

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

B-DRIVE: A blockchain based distributed IoT network for smart urban transportation

Mohammed Zia

GIScience Chair, Institute of Geography, University of Heidelberg, Heidelberg, 69120, Germany

ARTICLE INFO

Keywords:
Blockchain
Open data
Urban traffic
Internet of Things
Vehicle navigation

ABSTRACT

In this paper, I present B-DRIVE—a blockchain-based distributed IoT (Internet of Things) network for smart urban transportation. The network is designed to connect a large fleet of IoT devices, installed on various vehicles and roadside infrastructures, to distributed data storage centers, called as Full-Nodes, to log and disseminate sensor generated data. It connects devices from around the city to multiple Full-Nodes to log timestamped data into the blockchain. These sensors vary from GPS (Global Positioning System), air quality meter, gyrometer to speed cameras in order to facilitate efficient urban mobility. The three identified hardware layers that comprise the network are the IoT layer, Storage layer, and User layer. They consist of Moving/Static-Nodes, Full-Nodes, and Smart devices, respectively. The Moving/Static-Nodes are primarily made up of moving vehicles and road-side infrastructures, respectively, thus acting as various data sources. Whereas, Full-Nodes and Smart devices are institutions and mobile phones, acting as data handler/disseminator and navigator/data visualizer, respectively. The data, or data blocks, received by Full-Nodes get appended into Full and Running-Blockchain, meant for specific purposes. The network is designed to be free from any block mining activity. It provides open access to anonymous sensor data to end-users, especially scientists, policy-makers and entrepreneurs, to develop innovative urban transportation solutions. It is believed that a system like B-DRIVE, along with existing VANETs (Vehicular Ad-hoc NETworks), is capable of answering some of the current urban transportation issues around traffic congestion, navigation, and vehicle parking. Other applications of blockchain data could vary from user activity mapping to VGI (volunteered geographic information) data quality assessment. Two identified limitations of the presented architecture are the low processing power of current IoT devices and the lack of urban IoT infrastructure.

1. Introduction

With the global urban population expected to grow from 4.9 billion to 7.4 billion between the years 2014 and 2050, there is a worldwide need for smart urban transportation solutions. Almost 90% of this increase is expected to take place in developing nations, primarily from Asia and Africa [1]. It is believed that by 2050, there would be around 2–3 billion vehicles running in the world [2]. Smart urban solution refers to the use of Information and Communication Technologies (ICT) to optimize city functions and drive economic growth, primarily by the use of emerging automation, machine learning, and the Internet of Things (IoT)[1]. Lyons [3] has defined smart urban mobility as the use of technology to generate and share data, information, and knowledge that influences decisions to enhance vehicles, infrastructure, and services. One of the biggest threats any metropolitan city faces today is traffic congestion. With every new vehicle added to the street, citizens and city authorities are facing new challenges to find efficient ways to commute, with only limited solutions available [4]. Traffic congestion has a direct effect on a country's economy and citizens' quality of life by increasing the amount of fuel and time consumption on roads and decreasing public health. A 2012 report by Securing America's Future Energy has estimated that the amount of fuel that has been wasted by traffic congestion in the USA alone in the year

Abbreviations: B-DRIVE, Blockchain based Distributed IoT Vehicular Network; Block-VN, Block Vehicular Network; GIS, Geographic Information System; H2C, Human to Computer; H2H, Human to Human; IoT, Internet of Things; V2I, Vehicle to Infrastructure; V2V, Vehicle to Vehicle; VANET, Vehicular Ad-hoc NETwork; VGI, Volunteered Geographic Information.

E-mail address: mohammed.zia33@gmail.com.

[1] http://internetofthingsagenda.techtarget.com/definition/smart-city.

https://doi.org/10.1016/j.bcra.2021.100033
Received 17 May 2021; Received in revised form 29 October 2021; Accepted 9 November 2021

2010 was around 7.19 billion liter [5]. It is loosely believed that almost 30%[2] of all traffic in cities comprises vehicles looking for suitable places to park [6]. Many private companies like Google, HERE, Mapbox, etc., therefore, are actively working on finding innovative ways to improve the daily commute of the public. However, in order to capture early adopters and quickly expand businesses by leveraging the power of existing urban infrastructure, they usually leave the developing and underdeveloped nations behind.

Currently, operational private vendors in the urban transportation sector collect millions of telemetry data worldwide from smart hand held and IoT devices to generate daily traffic maps of various regions of the world [7]. The upside of these maps is ready services for end-users, like the shortest and fastest routing service, etc. However, the downside is limited other services. Partial and restricted access to collected data make it difficult for government IT staff and open source developers to design and develop custom solutions for specific use cases[3,4,5]. Application Programming Interfaces (APIs) of these vendors, claimed to be for solution developers, provide limited access to the dataset usually after data pre-processing [8]. These processes vary from data aggregation, data cropping, metadata alteration to reducing data resolution. It is believed that innovation gets restricted by putting licenses on datasets, known as the tragedy of the anti-commons. There is a current need of geo-data generation by the public for smart urban solutions. One classic example of this philosophy is OpenStreetMap[6]. It is one strong proof of concept as there are over 300 currently operational projects leveraging the power of it. Open source thinkers believe that public data and intellect are public properties, and they should not be left behind under any Terms & Conditions as long as the anonymity of a citizen is intact.

Human to Computer (H2C) interaction as such does not play any direct role in telemetry data generation for traffic maps. Rather it is generated automatically by smart and GPS (Global Positioning System) enabled IoT devices. IoTs are nothing but embedded devices with internet connectivity[7]. They allow the exchange of data packages over Internet Service Providers (ISP)[8]. When connected with GPS, they act as a smart device to generate Longitude-Latitude data, accessible over the internet. A detailed technical specification of why IoTs are currently being used as one major source of telemetry and geo-data is beyond the scope of this introduction [9], however, some of the salient features are (a) autonomous working, (b) low operational cost (except when connected by GSM), (c) low physical space, and (d) low power consumption. The two main limitations of these devices for global coverage are lack of standards for data exchange and lack of network layers for data security [10]. Smart devices, on the other hand, do not provide an efficient source of sensor data because of their “hand held” nature. As soon as the owner of the device leaves the vehicle its data becomes irrelevant to urban transportation. Since users directly interact with these devices, they usually keep the sensors off for power saving.

In order to conduct effective transportation operations such as vehicle routing, traffic monitoring, emergency response, road assistance, etc., researchers have developed a variety of dynamic inter-vehicle networks around wireless technology, called Vehicular Ad-hoc NETworks[9] (VANET) [11]. Researchers have developed a Vehicular Data Cloud platform for smart transportation [12]. These networks offer Intelligent Transportation System (ITS) by integrating ad-hoc networks, cellular and wireless Local Area Network (LAN) technology. They were initially designed by vehicle manufactures, transportation authorities, etc., to support Vehicle to Vehicle (V2V) and Vehicle to roadside Infrastructure (V2I) communication, using a protocol known as Dedicated Short Range Communication (DSRC) [13]. Any mobile device capable of forwarding geo-data by functioning as a router can act as one participating node in these networks [14]. A few applications of VANETs are (a) developing electronic breaking systems in autonomous or semi-autonomous cars, (b) facilitating tandem motion of nearby vehicles, (c) generating traffic maps for vehicle's satellite navigation system, (d) supporting fast emergency rescue operations, etc. Although seems like an ideal smart solution for current urban transportation needs, it is limited by the lack of a storage layer for sensor generated data. The data is typically live transmitted up to 300 m in 360° to all listening nodes, i.e., vehicles and roadside infrastructures, but do not get logged in any systematic manner. Some of the data do get stored but at centralized servers like transportation or revocation authorities. For man-in-the-middle attacks (MITM) it provides a single point of failure [15]. This also limits the access of valuable timestamped sensor data to the public. Pearson [16] has pointed out the security threats of these networks.

Table 1
Centralized vs B-DRIVE network for smart urban transportation.

Centralized Network	B-DRIVE Network
(a) Use of pseudonym and data encryption technology to keep the identity of a user hidden. However, lack of trust between different vendors and users is a security threat.	(a) Data stored in an encrypted block fashion using cryptographic hash function. Decryption is not possible as it is a one way mathematics.
(b) Possibility of change in policy at any point in time.	(b) Policies are more stable because of government's standardization and data's distributed nature.
(c) Provides one single point of failure or attack.	(c) No single point of failure or attack as data is distributed within Full and User-Nodes.
(d) Limited control of data to public.	(d) High control of data to participating nodes.
(e) User needs to buy vendor's service to use it.	(e) Very little or no participating cost.
(f) Limited access of dataset to improve VGI projects.	(f) High access of dataset to improve VGI vector tiles or other open source projects.

We argue that to answer some of the limitations of the VANET network caused by its lack of storage layer and wireless communication, an IoT-based blockchain system can be developed. The blockchain concept, so far, has proven to be one disruptive technology that was created by Ref. [17] after developing a peer-to-peer electronic cash system called Bitcoin. With initial user as seen to be financial industry, the concept and subsequently developed technology have found applications in wide-ranging areas. It is disruptive in its virtue by negating the very need of any centralized system by maintaining and protecting a distributed ledger of events. When events are stored in a ledger in the form of encrypted blocks, the ledger is called as blockchain. The blockchain system runs on participating nodes where each one contains an exact copy of it, verified by block mining. The system runs on a consensus basis where the 51% attack is needed to subvert any change [18]. Conoscenti et al. [19] have identified eighteen use cases of blockchain in scientific literature, out of which four are explicitly designed for IoT. Some of the key benefits of using this technology with IoT devices for urban transportation, as also explained in Table 1, are (a) data transparency and accountability—preservation and public verification of logged data, (b) data immutability—protection of data by unique hash fingerprinting, (c) very low or no data exchange cost—very little or no payment for nodes to participate to the network, (d) instantaneous data logging—immediate logging of data into the blockchain, (e) data security—high data security and anonymity because of the use of advanced cryptographic hash function, like SHA-256, (f) system resilience—no single point of failure because of distributed network, (g) data control—full

[2] https://archives.sfexaminer.com/sanfrancisco/Content?oid=2580026.
[3] https://www.mapbox.com/vector-tiles/mapbox-traffic-v1.
[4] https://tech.yandex.com.tr/maps/doc/staticapi/1.x/dg/concepts/traffic-docpage.
[5] https://developers.google.com/maps/documentation/javascript/examples/layer-traffic.
[6] https://en.wikipedia.org/wiki/OpenStreetMap.
[7] https://www.codeproject.com/articles/832492/Stage-introduction-to-the-internet-of-things-who.
[8] https://www.computerhope.com/issues/ch001358.htm.
[9] https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network.

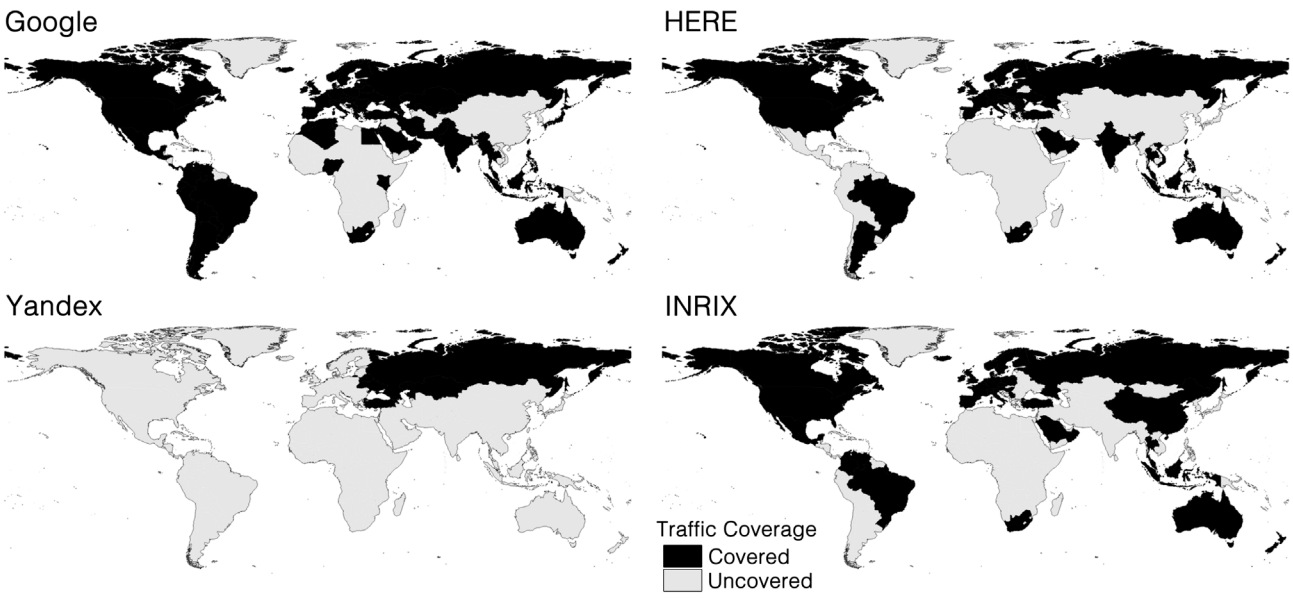


Fig. 1. 2017 global traffic coverage map of countries/regions by four major IT service providers.

control and access of data to the public, acting as participating node, (h) system trustlessness—safe exchange of data without knowing or trusting other nodes. A detailed technical explanation and working principles of blockchain technology are beyond the scope of this literature, however, an insight can be found in Refs. [17,20].

In this study, we present a **B**lockchain-based **D**ist**R**ibuted **I**oT **NE**twork (B-DRIVE) architecture to answer some of the open issues of VANET, as discussed by Ref. [21]. Work like in Refs. [22-24] also supports the idea of using commercial and academic blockchains on the VANETs domain. These issues are primarily around data fusion, architecture scalability, cost of service, and estimation of future traffic. This enabling architecture is completely distributed among participating nodes, Full-Nodes and User-Nodes to be specific (Sections 3.1.3, 3.1.4). Data, like longitude-latitude, air quality, angular speed (gyrometer), timestamp, etc., generated by IoT sensors at Moving and Static-Nodes (Sections 3.1.1, 3.1.2) get logged in the form of encrypted blocks into the city's Full-Blockchain (Section 3.2.1). There is an upper limit of the Running-Blockchain (Section 3.2.2) size depending upon the storage capacity of the smart device at User-Node. This limit is defined by the B-DRIVE's network specification. The running-Blockchain merely contains a fraction of all generated latest blocks at the city level, depending upon the geographical location and storage capacity of the User-Node. Full-Blockchain is managed and kept functional by institutions like transportation agencies, private vendors, scientists, policy-makers, and entrepreneurs, etc., termed as Full-Node. Running-Blockchain, on the other hand, runs on smart devices of end-users, termed as User-Node. Depending upon the number of commuters in a city, one or more Running-Blockchains operate in parallel in order to keep the upper storage and computational limit of the device in check. All User-Nodes in a given region communicate to the same Full-Node or to each other in order to maintain the latest version of Running-Blockchain. Different Full-Nodes also communicate periodically to each other to synchronize and update the city's Full-Blockchain. Newly added User-Node synchronizes with the nearest User-Node or Full-Node for Running-Blockchain. Moving and Static-Nodes act as a source of telemetry data and not a storage point. Secure cryptographic hash functions, like SHA-256, keep the identity of the source node hidden for any identity breach. However, other data remains open for User-Nodes and Full-Nodes. I believe that a system like B-DRIVE, along with existing VANETs, is an answer to the current smart urban transportation call. The rest of the body is organized as follows: Why B-DRIVE?; B-DRIVE Architectural Design; B-DRIVE Applications; B-DRIVE Attacks and Limitations; and Conclusion.

2. Why B-DRIVE?

Private vendors, like Google Maps[10], HERE Traffic Maps[11], Yandex Maps[12], INRIX, etc., who claim to provide live and predicted traffic maps and other value-added services around urban transportation of major world cities, inherently possesses barriers for scientists, policy-makers, and entrepreneurs in terms of (a) limited data access, (b) poor global coverage, (c) low data quality, and (d) biased traffic solutions. Fig. 1 is a traffic coverage map of four IT giants, i.e., Google[13], HERE[14], Yandex, and INRIX[15]. In spite of over a decade long development of Google Traffic, there are many regions in Asia and Africa that are still uncovered[16]. The same could be said for others too. Note that only key major cities of India are covered by Google, in contrary to their claim of nationwide coverage. These vendors collect telemetry data from both the smart user devices and installed IoT devices on selected vehicles. For static data, they usually rely on public generated geo-data[17] like OpenStreetMap[18]. It can be argued that it is unethical to anonymously collect public-generated geo-data (both static-like OpenStreetMap and dynamic-like telemetry) but not allow people complete and open access to that data to encourage the development of innovative solutions building off that data.

Online service providers work either in a centralized or decentralized manner (Fig. 2). They collect, index, process, and manage telemetry data at one or a few of their distributed servers (solid circles in Fig. 2). Some advanced agencies even work in a hybrid manner by developing vehicular cloud networks by leveraging the computational and storage capacities of all participating nodes [12] (hollow circles in Fig. 2). These agencies keep a complete track of user's credential/activity and, thus, possess security threats [21]. Although pseudonyms and data encryption approaches are used to store this data, their centralized storage model

[10] https://www.google.com.tr/maps.
[11] https://wego.here.com/traffic.
[12] https://yandex.com/maps.
[13] https://developers.google.com/maps/coverage.
[14] https://developer.here.com/documentation/traffic/topics/coverage-information.html.
[15] http://inrix.com/resources/inrix-traffic-brochure.
[16] https://googleblog.blogspot.com.tr/2007/02/stuck-in-traffic.html.
[17] https://yandex.com/company/technologies/traffic_jams_technology.
[18] https://en.wikipedia.org/wiki/OpenStreetMap.

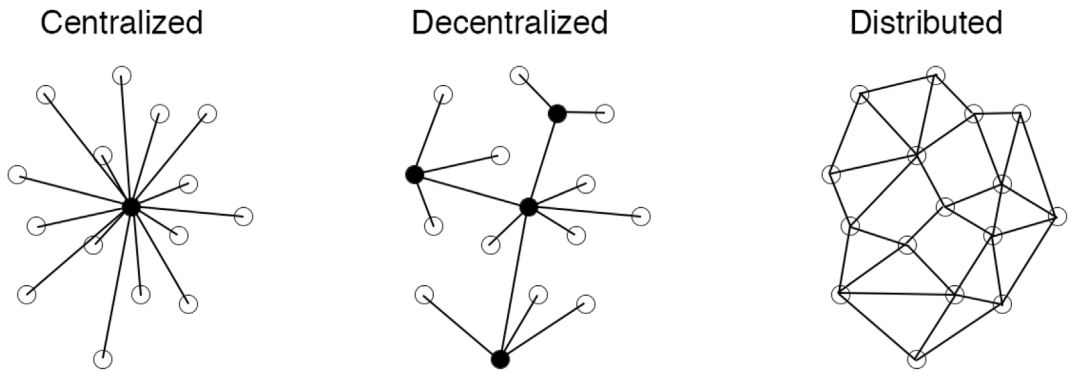


Fig. 2. Different kinds of network architecture. Note that a 100% centralized or distributed network practically does not exist in production environment.

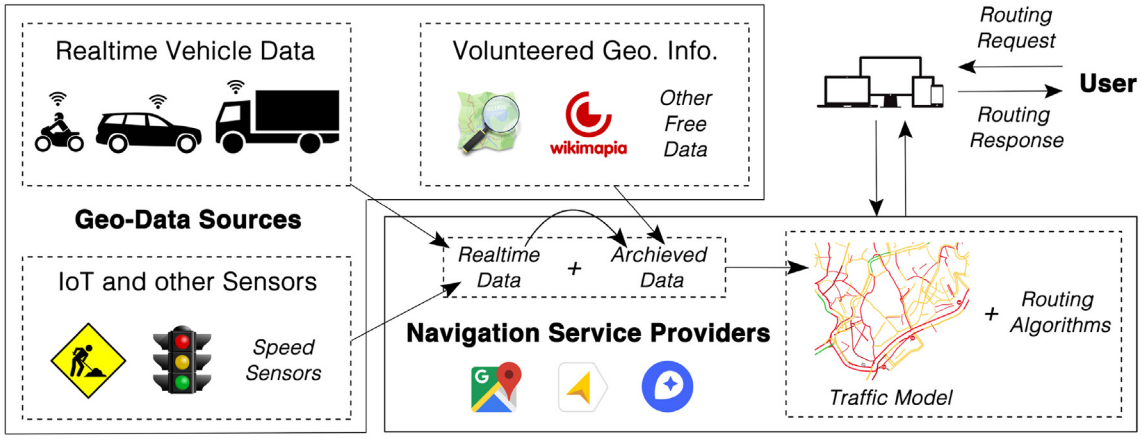


Fig. 3. Schematic diagram showing the working model of urban transportation service providers.

and lack of trust between participating agencies and the public always create concerns about public security[19] [21,25]. Jaworski et al. [26] have argued that for location-based services a privacy scheme will have to be implemented. With any centralized or decentralized data storage model controlled by one single entity, a secure unbiased smart urban transportation infrastructure is hard to attain.

Fig. 3 shows the functioning of a typical traffic solution service provider, along with different data sources and components. Telemetry data from smart and IoT devices gets logged in real-time into different physical or cloud storage centers. They merge this feed with other vectors and raster datasets of the region to generate traffic maps and models. Users connect to their APIs, mobile-applications, web-maps, etc. to navigate through the streets or to create other mobility services. It should be noted that primarily the source of both the telemetry and vector data of these vendors are on-road commuters and Volunteer Geographic Information (VGI) contributors. These vendors, thus, primarily provide a platform to connect different data sources, to log them, and to structure ways to disseminate products out of them to the general public.

The presented B-DRIVE network is built in a distributed manner within a city where no one entity is responsible for the logging and controlling of public generated telemetry sensor data (Fig. 2). Past researchers have already argued the usability of blockchain technology for geospatial[20] data storage points, by coining the concept of Proof of Location[21]. Data generated by IoT sensors gets stored at least at two Full-Nodes. This ensures the distribution of data over the network. However, access to city-wide operational IoT sensors requires legal permission for newly added Full-Nodes from governmental bodies like city transportation or revocation authority. This adds one additional layer of network security. The B-DRIVE concept is similar to Block-VN, as coined by Ref. [27], in terms of data format and V2V and V2I communication, however, it further extends it by circumventing the need of any miner-node and by adding different hardware layers and nodes as network components. Table 1 lists key differences between a centralized network vs B-DRIVE network. By centralized, we refer to both centralized and decentralized.

3. B-DRIVE architectural design

Because of the various technical limitations of participating components, the presented B-DRIVE architecture is divided into three hardware layers. These are (a) IoT layer, (b) Storage layer, and (c) User layer (Fig. 4). The IoT layer consists of a large number of IoT devices generating sensor data at regular intervals of time. This data gets disseminated over ISP bridges to all registered Full-Nodes. Each device in this layer connects to at least two Full-Nodes in the stack. This is to keep the data distributed at different geographical locations and not to give data ownership to one single entity. The majority of the devices, i.e., moving vehicles, of this layer connect to the network through GSM connection, with a few of them, i.e., roadside infrastructure, through LAN connection. The Storage layer consists of all registered entities responsible for the collection and logging of newly generated sensor data. Legal permission from the transportation or revocation department of the city is required for an entity to participate in the network at this layer. The department assigns a fraction of all operational IoTs to it. There are monetary

[19] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks.
[20] https://www.geospatialworld.net/article/blockchain-geospatial-systems.
[21] https://blog.foam.space/introducing-the-foam-protocol-2598d2f71417.

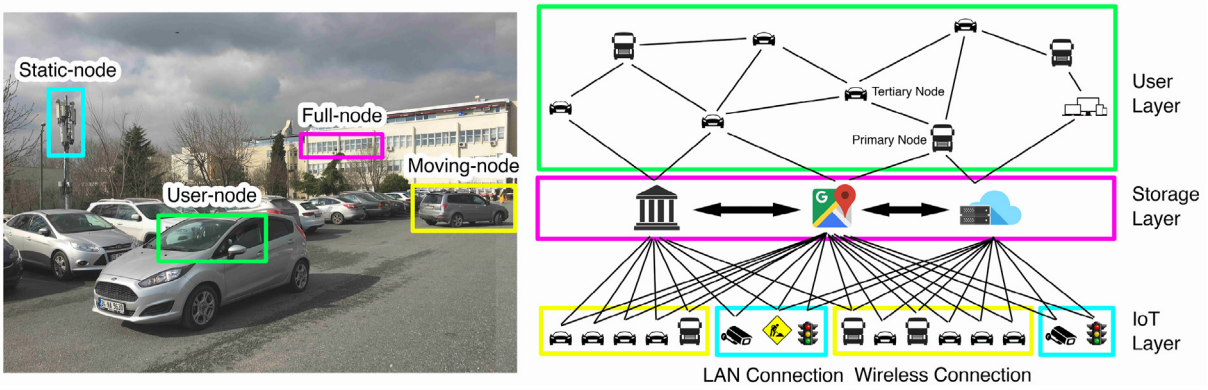


Fig. 4. Different hardware layers and node types in B-DRIVE architecture. In real life scenario, single vehicle can host multiple node types.

incentives in the form of digital tokens, tax relaxation, etc. for organizations or individuals to participate at this layer. The digital token can be understood by the concept of cryptocurrency [18], however, it should not be confused with Full or Running-Blockchain. Finally, the User layer consists of the general public and on-road commuters who try to find or develop optimal ways to navigate through the city, especially during rush hours. The nodes of the User layer that are directly connected to the nearest Storage layer, called as Primary Nodes (Fig. 4), get synchronized for all newly generated IoT data as soon as it gets published at the storage point. However, it does not store old data beyond a certain point, primarily to keep the smart devices operational. Other nodes connected to these Primary Nodes, called as Tertiary Nodes, receive data through a peer-to-peer protocol (Fig. 4). An entity in the User layer overlaps an entity in the IoT layer if the two operate from one single vehicle. In B-DRIVE architecture, nodes connectivity is a function of their geographical separation. Only nodes close to each other connects by default to maintain peer-to-peer low latency communication.

3.1. B-DRIVE node type

The three hardware layers of B-DRIVE architecture consist of four different kinds of nodes. Moving-Node and Static-Node belong to the IoT layer, Full-Node belongs to the Storage layer and User-Node belongs to the User layer (Fig. 4). Their definition, specific role within the network and salient features are further explained in subsequent sections.

3.1.1. Moving-Node

A Moving-Node refers to a GPS sensor connected IoT device on a vehicle. The role of this node is to periodically generate blocks of sensor data for Full-Nodes. These blocks then eventually get logged into the Full-Blockchain. The rate of block generation varies depending upon the type of vehicle and hours of the day. Usually, the period is kept short during work hours of business days, especially in the morning and evening when the traffic is high. The detailed specification of the functioning of this node goes into the B-DRIVE protocol as defined by the city transportation department. An optimal rate of block generation by different Moving-Nodes is crucial for scalability. It is believed that one block per minute is an optimal starting rate for network deployment and depending upon the number of participating nodes it should be tweaked. Generated blocks help other nearby User-Nodes to respond to certain events, like sudden road blockage, accident, approaching ambulance, etc., however, some network latency is possible because of GSM connection and Full-Nodes, unlike VANET. The block gets accessible to all User-Nodes within the vicinity, without any data processing latency. The identity of Moving-Node gets encrypted or ignored at the IoT layer before leaving the gateway. A sample block of humidity and air quality sensor data from a static node might look like this:

Encrypted Node ID: y6543tyr454g42g54t5fq4rgf3542t5
Timestamp (unix format): 1234242342
Speed (magnitude and azimuth): 20.23, 232.34
Longitude-Latitude (WGS84): 23.43, -34.23
State of the Node:
Status (if all sensors are working) - Yes
Emergency (if node is in a state of emergency, like ambulance) - High
Size (type of vehicle hosting this node) - Heavy vehicle

3.1.2. Static-Node

All IoT-enabled roadside infrastructures fall under this node category. They are primarily speed cameras, traffic lights, weather sensors, temporary road maintenance sites, etc. They provide an additional layer of information about the status of streets for navigation and other purposes. Blocks generated by these nodes contain sensor data around pollution, visibility, road condition, and other miscellaneous factors. A directory containing the geographic location of all operational Static-Nodes in a city would be accessible from any Full-Node. The urban transportation department is responsible for the installation and maintenance of them. They connect to their respective Full-Nodes through LAN connections. The rate of block generation, the status of the node (working or paused), etc. is alterable by network admins at the urban transportation department. A sample block of sensor data from this node looks like this:

Encrypted Node ID: y6543tyr454g42g54t5fq4rgf3542t5
Timestamp (unix format): 1234242342
State of the Node:
Status (if all sensors are working) - Yes
Humidity (in percentage) - 76
Air Quality (ppm) - 2.5

3.1.3. Full-Node

All Full-Nodes consist of physical servers responsible for the collection and logging of IoT-generated blocks within a city. They are primarily the city transportation department, vehicle revocation authority, private vendors, scientists, policy-makers and entrepreneurs, etc. Other than data logging, Full-Nodes also develop network protocols and ensure their working. All Moving and Static-Nodes from the IoT layer connect to at least two of these nodes directly. The city transportation department is responsible for assigning IoT devices to different participating Full-Nodes. This is to keep the traffic of incoming data at different Full-Nodes low and properly load balanced. Note that, unlike Static-Node, Moving-Node changes its location with time and, therefore, connects to at least two nearest Full-Nodes at any given point in time. Their physical location within a city is crucial to

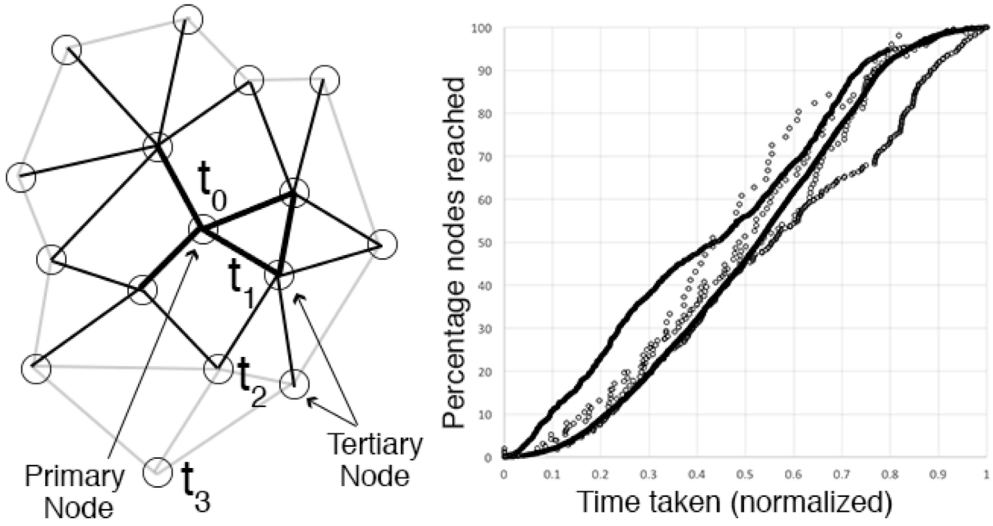


Fig. 5. Propagation of a block with time from Primary to Tertiary nodes (Fig. 4) in a B-DRIVE network. The graph shows the percentage of Tertiary nodes reached by a Primary node at any given time.

maintain low latency of data transmission. They generate, maintain, and store a complete history of all generated blocks in chronological order, although only connect directly to a fraction of them. User-Nodes connect to their nearest Full-Node for Full-Blockchain or Running-Blockchain. The incentives for private vendors and citizen scientists to participate in this layer are digital tokens, advertisements, big data archives, tax relaxation, etc. These nodes in a city periodically communicate with each other to update any missing blocks. Blocks older than a few weeks get clustered in a more hierarchical Merkle Tree and stored in an optimized data structure for storage. A legal procedure and official permit are required to become one such node.

3.1.4. User-node

Daily commuters and the public with smart devices connected to the B-DRIVE network fall under this category. They receive and store the latest blocks (blocks generated recently, let's say in the last 24 h) of IoT data from their geographic region of commute. The blockchain of these latest blocks, specific to a region, is termed as Running-Blockchain. They connect to their nearest Full-Nodes or other User-Nodes to receive it. There are two kinds of User-nodes: (a) Primary node—the one that connects directly to a Full-Node and (b) Tertiary node—the one that connects to a Full-Node through a Primary node (Fig. 4). Note that a Moving-Node refers to a vehicle with an installed IoT device and a User-Node refers to a commuter with a smart device. Block from a Primary node leaves to other connected Tertiary nodes at the same time in a peer-to-peer protocol. Fig. 5 shows the propagation of any such block from Primary to Tertiary nodes with time. It shows the time taken by a block from Primary node to reach the X% of all participating Tertiary nodes in a distributed network. It follows a linear trend, which is what is reported by Ref. [28] about block propagation in the Bitcoin network. Distributed networks tested for the curve are taken from the TSP instance library[22].

3.2. B-DRIVE blockchain types

The two kinds of blockchains that exist in B-DRIVE architecture are Full-Blockchain and Running-Blockchain. Their respective features and use cases are explained below.

3.2.1. Full-Blockchain

As previously described, the Full-Blockchain contains the complete history of all transmitted blocks from the IoT layer since the genesis of the network. They are managed and stored at Full-Nodes. The purpose of storing the complete history of the network is to develop predictive models using big data and machine learning techniques, along with making deep public commute insights using data mining. Data is the new fuel of ICT and one of the main assets of private vendors. A publicly available Full-Blockchain assists citizen scientists and entrepreneurs to develop innovative solutions around urban navigation. It helps data curators to improve street network graphs using a map matching approach [29]. This blockchain gets stored at multiple physical locations to make the network fault tolerant.

3.2.2. Running-Blockchain

Running-Blockchain is a sub-component of Full-Blockchain in the network, i.e., the blocks generated recently by the IoT layer. This blockchain is stored both at the Full-Nodes as well as at the User-Nodes, i.e., commuters' smart devices. The data will help to process instantaneous responses to street events in the vicinity, like traffic accidents, road blockages, available parking spaces, etc. Depending upon the number of Moving and Static-Nodes in the city, one or more Running-Blockchains operate in parallel (Fig. 6). Fig. 6 shows four Full-Nodes and corresponding Running-Blockchains operational in the city of London. The region is divided on the basis of urban population to keep the size of each Running-Blockchain small. However, User-Nodes can store and process multiple Running-Blockchains at a time depending upon their storage and computational capacity. Blocks older than a certain time period get deleted automatically to keep the node operational, except for Full-Blockchain. A newly added User-Node obtains its Running-Blockchain from the nearest connected User-Node or Full-Node. Note in Fig. 6 that since the central part of the city of London is more dense as compared to other adjoining areas, Running-Blockchain_B covers a relatively smaller region (Data Source: European Environment Agency[23]). Overlapped Regions are possible where Running-Blockchain is generated by utilizing overlapping Full-Nodes. The actual network implementation in a real life scenario can get highly complex with multiple parallel Blockchains.

[22] https://www.iwr.uni-heidelberg.de/groups/comopt/software/TSPLIB95.

[23] https://www.eea.europa.eu/data-and-maps/data/copernicus-land-monitoring-service-urban-atlas.

Fig. 6. Different Full-Nodes and Running-Blockchains operational in the city of London, distributed on the basis of urban density—a proxy of traffic congestion.

3.3. *B-DRIVE working principles*

The working principles of a B-DRIVE network can be understood from Fig. 7. All the data generated at the sensor node of an IoT device gets stored in a block. A block is simply an efficient data format to store a rapidly generated text string. In order to keep the identity of the device hidden, its ID gets encrypted using a secure hash function like SHA-256. Once generated, the block gets delivered to the IoT gateway. The IoT gateway acts as a doorway for data to go public. It pushes data to the Internet through one of the many possible connections like Ethernet, Wifi, or GSM. These connections are provided by Internet Service Providers (ISPs). An ISP bridge is the channel through which data flows. This block gets delivered to at least two of the registered Full-Nodes for logging. Registration of an IoT device to a Full-Node is done on the basis of their geographical separation. These nodes listen to any receiving block. However, Full-Nodes keep a complete history of all Moving and Static-Nodes within a city by periodically synchronizing with each other. Received blocks get stored in a more compact data format in clustered fashion after a predefined time. This is mainly to optimize the storage capacity at the Storage layer and to ease the transmission of data during Full-Blockchain download requests. Any User-Node connected to this Full-Node also gets a copy of all recently added blocks, instantaneously. Although User-Nodes keep only the Running-Blockchain of their region of interest, this is just an option. User-Nodes use these blocks along with other value-added services developed by Full-Nodes to find optimal ways to navigate through the city.

Fig. 8 shows a B-DRIVE network in action. Sensor data like GPS, latitude-longitude, air quality ppm, humidity percentage, etc. generated at the IoT layer, i.e. at Moving and Static-Node, gets transmitted to their registered Full-Nodes. Each Full-Node maintains two blockchains, one Full-Blockchain and one Running-Blockchain. Block received at a node goes into both of them, as two separate blockchains. However, the Full-Blockchain also communicates with other Full-Blockchains to maintain a complete history of all generated blocks. Network changes depending upon city's geographic structure. A Running-Blockchain maintained by a Full-Node gets distributed to all connected User-Nodes. It should be

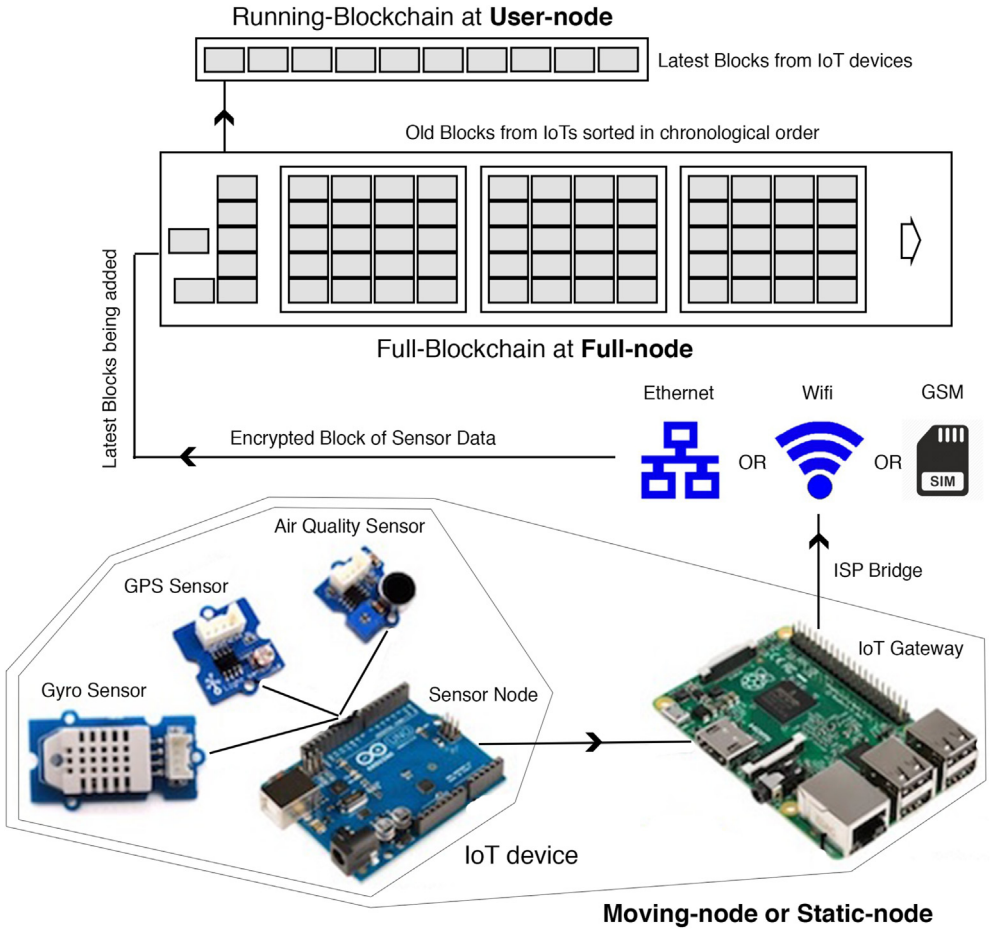


Fig. 7. Different components of a B-DRIVE network.

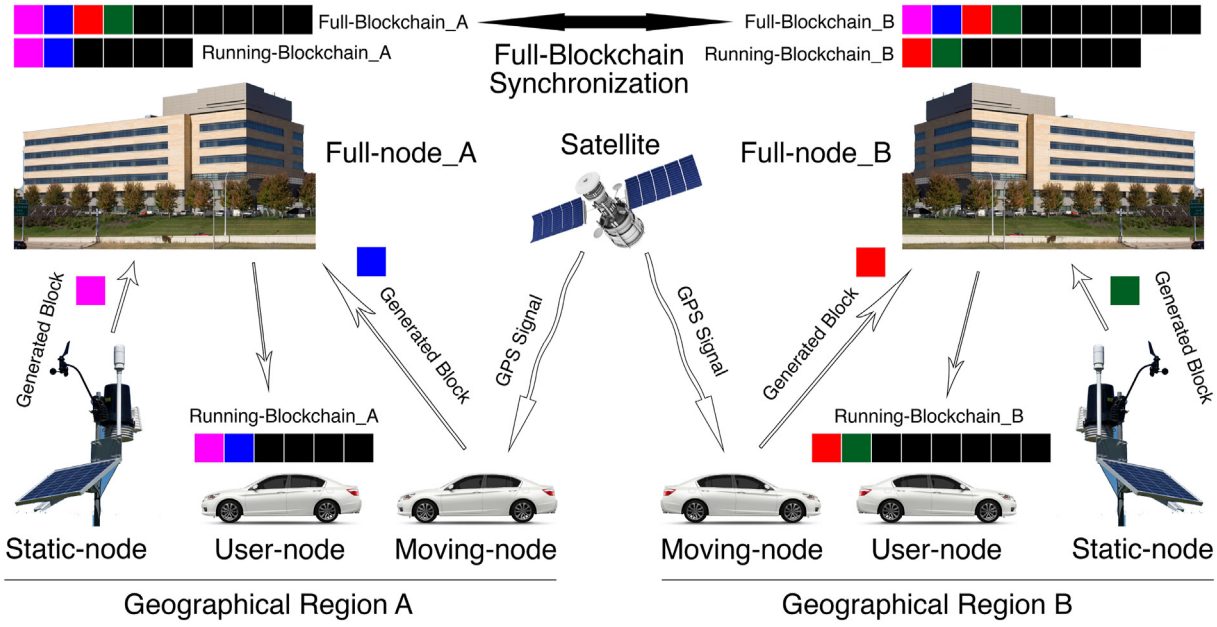


Fig. 8. B-DRIVE network components in action at two different geographical regions.

noted that, unlike a Static-Node, a Moving-Node is dynamic. It changes its location with time. Depending upon the current geographical location (Fig. 6), a Moving-Node connects to its nearest two Full-Nodes to log the block. The same is true for User-Node as well which mainly operates from a moving vehicle. Fig. 8 is one of the simplest depictions of the network and in real life, node configuration will be quite complex.

3.4. B-DRIVE salient features

B-DRIVE network architecture differs from any existing blockchain network architecture, including Block-VN [27], in the following respects.

3.4.1. No block mining is required

The sole reason why blocks are mined in Bitcoin or any other blockchain networks is to stop any possible attack of double spending. A mined block assures that all past transactions are intact and any future alteration requires the 51% consensus attack [18]. The upper limit of the total number of Bitcoins has been kept finite. It is one scarce resource, and so is the computational power. In fact, scarcity is also the reason why gold or diamonds have been used as a backing for money. However, in the B-DRIVE network data generated by the IoT layer does not represent any finite resource. Digital data is an ever growing measurement. The concept of a double-spending attack is, therefore, not applicable in the B-DRIVE network. The acceptability of a node generating sensor data can easily be confirmed by comparing its observation with other nearby nodes. Simple statistical outlier detection is sufficient to identify an anomaly at the node level. Although, it would not be possible to derive instantaneously or within 6–8 min just like in the case of Bitcoin. Since the ID of the device remains encrypted, it would not be possible to physically locate it. However, once located, a filter could be placed for any future incoming blocks from it. Moreover, the effect of a malfunctioning node will not be of significance to the network, as measurements eventually get aggregated and averaged by Full or User-Nodes. An attack on or installation of a large number of malfunctioning devices to subvert the measurements of existing devices is an expensive fare in terms of computational resources and money for an attacker. It is believed that a blockchain ecosystem with no mining requirement is a plus in terms of the network's longevity and scalability. There are incentives for organizations to join the network at Full-Node, other than minted coins by mining activity. Existing blockchain solutions are currently facing a huge energy crisis and governmental regulations because of block mining[24].

3.4.2. Running-Blockchain per region

Depending upon the congestion level of a city, one or more Running-Blockchains operate at Full and User-Nodes (Fig. 6). This is unlike what we observe in Bitcoin and similar networks, where one global ledger of transactions exists to avoid possible a double-spending attack. B-DRIVE network is immune to any double-spending attack as explained in the previous section. Multiple Running-Blockchains keep the network up and manageable at smart devices in spite of their limited computational and storage resources. The reason that multiple Running-Blockchains are possible is that IoT generated data is independent of each other. It is not a limited resource, like cryptocurrency or real estate, where a track of the flow of underlying value is mandatory. Note that just like multiple Running-Blockchains operate at the intra-city level, multiple Full-Blockchains operate at the inter-city level.

3.4.3. Constant block size

The data size of all key-value pairs, as shown in Section 3.1.1 and 3.1.2, is almost constant for a Moving and Static-Node. This primarily depends upon the number of sensors the IoT device is operating on. A compressed binary format of a block, as shown in Section 3.1.1, takes around 140 bytes of disk space [17]. A block of 140 bytes means 1.5 megabytes of data per week if generated at the rate of 1 block per minute. The upside of a constant block size is that any tailored hardware device for B-DRIVE architecture can be developed for data storage efficiency. Also, advanced storage formats are possibly be designed to hold large number of similar sized data packages (Fig. 7). This is unlike what we observe in other blockchain networks where the block size varies depending upon the number of transactions performed. A fixed block size also helps to define custom HTTP protocols for efficient data propagation. Other advanced data compression and querying techniques are also possible to develop in this architecture.

4. B-DRIVE applications

Many envisaged geospatial applications around urban transportation are possible with the B-DRIVE architecture. They could vary

[24] https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency.

from real-time traffic mapping to predictive modeling. Fig. 9 shows four examples of them. In Fig. 9, using longitude, latitude, and timestamp data collected by Moving-Nodes, live traffic speed estimation is possible for different road profiles. Machine learning techniques can be used for traffic prediction at different hours and days of the week. This kind of data is useful to develop artificial intelligence for autonomous and semi-autonomous vehicles. Using a private key to the device, a commuter can create a time-series user activity map of a Moving-Node. This node could be his/her own vehicle. GPS data of a stationary Moving-Node could be used for the generation of parking maps. Historical data of nodes could be used to predict the availability of parking spots at certain hours of the day (Fig. 9). It is believed that this kind of visualization is useful to lessen traffic congestion and fuel consumption. Predictive models could be helpful for transportation authorities to better channelize available infrastructural resources to improve public mobility by constructing new parking spaces, traffic lights, fly-overs, etc. Additionally, Moving-Node data could be used to improve existing VGI datasets (Fig. 9). These datasets limit their advanced usability in GIS by poor data point precision and high feature generalization [30]. A high-rate block generation protocol is useful to generate big data of streets to overcome such limitations. This is useful to detect missing or newly constructed road sections in different parts of the city. A detailed discussion of possible use cases of a B-DRIVE generated dataset is beyond the scope of this study, however, Rathore et al. [9] provide a range of areas where IoT generated sensor data can be used for Smart Transportation Systems.

Different software frameworks and visualization tools can be used to process blockchain data. These frameworks are capable enough to handle big data. Apache Hadoop and MongoDB are two of the many open-source and proprietary options available online. Rathore et al. [9] have used Apache Hadoop, with MapReduce and Hadoop Distributed File System (HDFS), to perform big data analytics on thousands of IoT captured measurements. They are primarily used for Data Mining to detect hidden patterns and deep insights. For data storage, services like Amazon Web Services (AWS) S3 bucket are a good choice, considering its cheap S3 buckets. A Kinesis connected S3 bucket can be set up to act as a Full-Node (Fig. 10). For data querying and visualization purposes, AWS Athena and Quicksight tools are useful. Programming packages like TensorFlow and Scikit-Learn can be used for machine learning applications. They provide out-of-the-box features like various classification, regression, and clustering algorithms, including support vector machines, random forests, gradient boosting, k—means, etc. A plethora of different options and combinations are possible for anyone trying to leverage the power of generated IoT data. B-DRIVE data stored in a database could be queried using simple SQL statements. Fig. 11 shows a database table containing randomly generated IoT layer data. Note the irrelevance of a few columns for Moving and Static-Nodes (empty cells of the table). Also, note that Speed (magnitude) and Speed (azimuth) are columns generated during data post-processing. As such the Moving-Nodes only generate longitude, latitude, and timestamp sensor data, as other values like speed, acceleration, etc. could be derived from them. Pseudo queries to extract

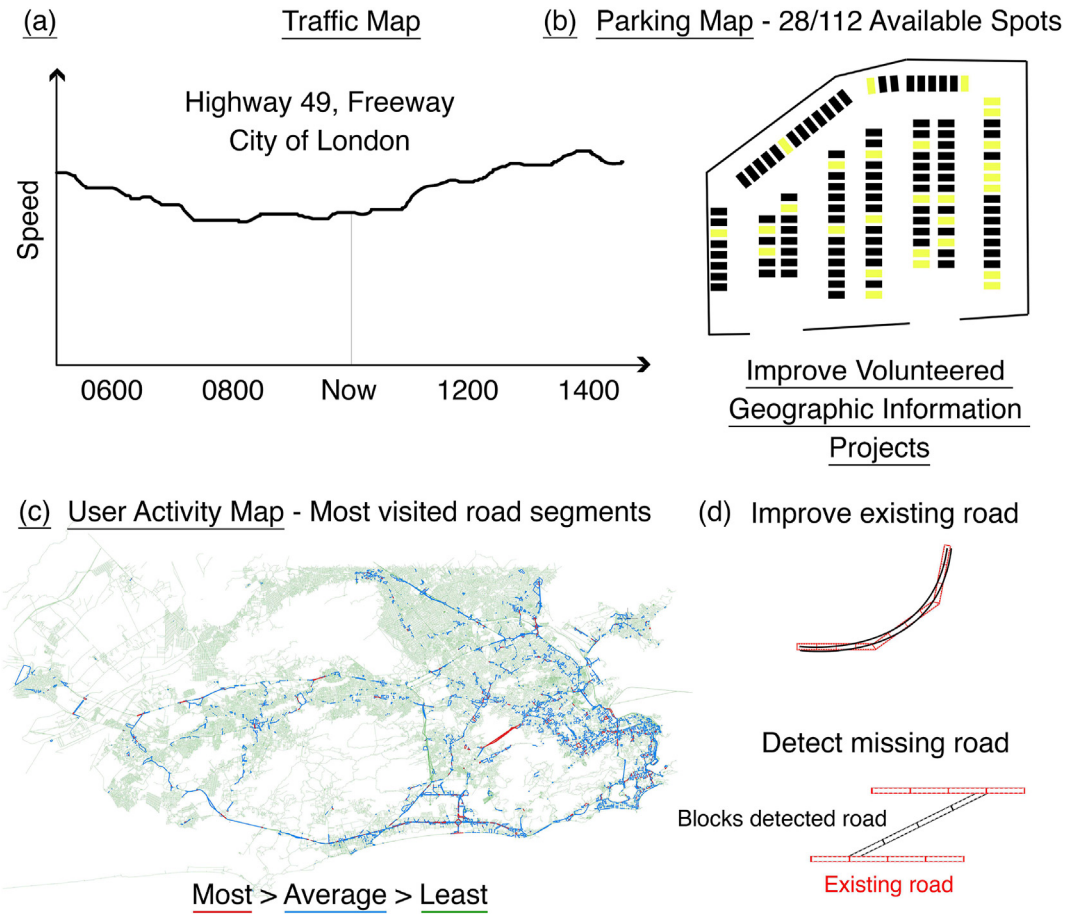


Fig. 9. Four different use case scenarios for Full-Blockchain data around urban transportation.

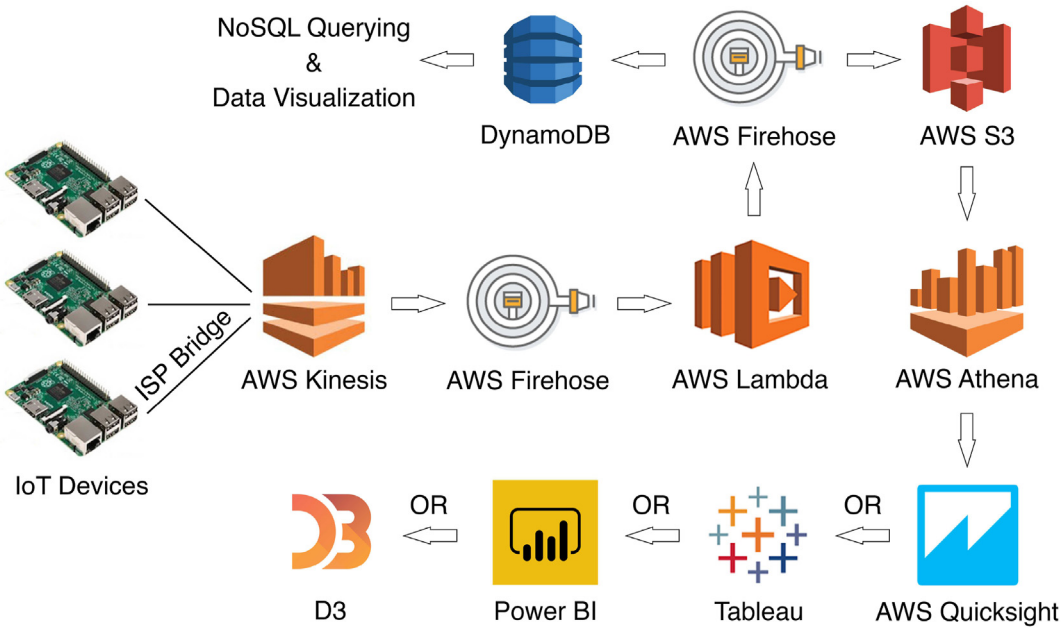
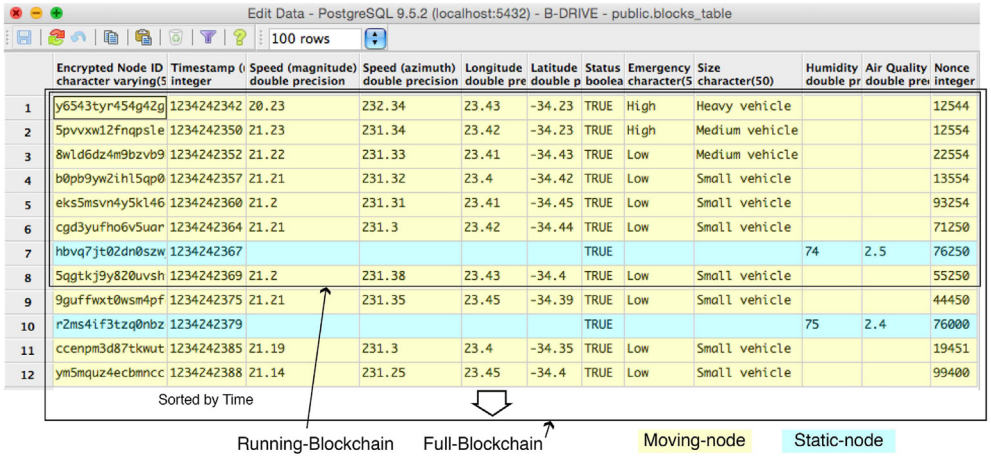


Fig. 10. One possible combination of software modules to setup a cloud-based Full-Node for data logging and visualization, mainly using Amazon Web Services (AWS) stack.



	Encrypted Node ID character varying(5	Timestamp integer	Speed (magnitude) double precision	Speed (azimuth) double precision	Longitude double pre	Latitude double p	Status boolea	Emergency character(5	Size character(50)	Humidity double pr	Air Quality double pre	Nonce integer
1	y6543tyr454g42g	1234242342	20.23	232.34	23.43	-34.23	TRUE	High	Heavy vehicle			12544
2	5pvvxw12fnqpsle	1234242350	21.23	231.34	23.42	-34.23	TRUE	High	Medium vehicle			12554
3	8wld6dz4m9bzvb9	1234242352	21.22	231.33	23.41	-34.43	TRUE	Low	Medium vehicle			22554
4	b0pb9yw2ihl5qp0	1234242357	21.21	231.32	23.4	-34.42	TRUE	Low	Small vehicle			13554
5	eks5msvn4y5kl46	1234242360	21.2	231.31	23.41	-34.45	TRUE	Low	Small vehicle			93254
6	cgd3yufho6v5uar	1234242364	21.21	231.3	23.42	-34.44	TRUE	Low	Small vehicle			71250
7	hbvq7jt02dn0szw	1234242367					TRUE			74	2.5	76250
8	5qgtkj9y8Z0uvsh	1234242369	21.2	231.38	23.43	-34.4	TRUE	Low	Small vehicle			55250
9	9guffwxt0wsm4pf	1234242375	21.21	231.35	23.45	-34.39	TRUE	Low	Small vehicle			44450
10	r2ms4if3tzq0nbz	1234242379					TRUE			75	2.4	76000
11	ccenpm3d87tkwut	1234242385	21.19	231.3	23.4	-34.35	TRUE	Low	Small vehicle			19451
12	ym5muz4ecbmncc	1234242388	21.14	231.25	23.45	-34.4	TRUE	Low	Small vehicle			99400

Fig. 11. A database table containing recorded IoT sensor data (random dataset). Records are sorted by time. Running-Blockchain contains only a fraction of all latest records generated from a region.

information from any such kind of table look like this:

1. Estimate the average current speed of heavy vehicles on Highway 49, Freeway -

```
WITH TimeTable AS
   (SELECT Longitude, Latitude, Timestamp FROM blocks table
      WHERE Longitude AND Latitude ON "Highway 49, Freeway"
      AND Size IS "Heavy vehicle"),
SpeedTable AS
   (SELECT [(Longitude2-Longitude1)^2+(Latitude2-Latitude1)^2]^0.5/(Timestamp2-
   Timestamp1)
   AS Speed FROM TimeTable)
SELECT SUM(Speed)/COUNT(*) AS Average_Speed FROM SpeedTable
```

2. Create a User Activity Map of certain Encrypted Node ID for last week -

```
SELECT Longitude, Latitude, Timestamp FROM blocks_table
   WHERE Timestamp INBETWEEN (NOW AND 7 days ago)
   AND "Encrypted Node ID" IS "y6543tyr454g42g54t5fq4rgf3542t5"
```

These models would be effective for road navigation, traffic management, infrastructure remote monitoring, urban surveillance, information and entertainment, business intelligence, etc. to meet the requirements of a smart city.

5. B-DRIVE attacks and limitations

The two observed limitations of a B-DRIVE architecture to fully function are (1) weak currently available IoT hardware, and (2) a lack of urban infrastructure. Because of the slow processor in IoT devices Node ID encryption using a cryptographic hash function is still a challenge[25]. Encryption requires fast processors to perform heavy mathematical computation. Full-fledged device authentication, security, and control layers are more complex to build with existing IoT electronics. Botnets can attack these devices to perform Distributed Denial-of-Service (DDoS) attacks. These hardware challenges need to be addressed in the future development of the B-DRIVE concept. Another limitation of this network is the lack of existing infrastructure. Only a fraction of all on-road vehicles

[25] https://www.forbes.com/sites/delltechnologies/2017/06/27/how-blockchain-could-revolutionize-the-internet-of-things.

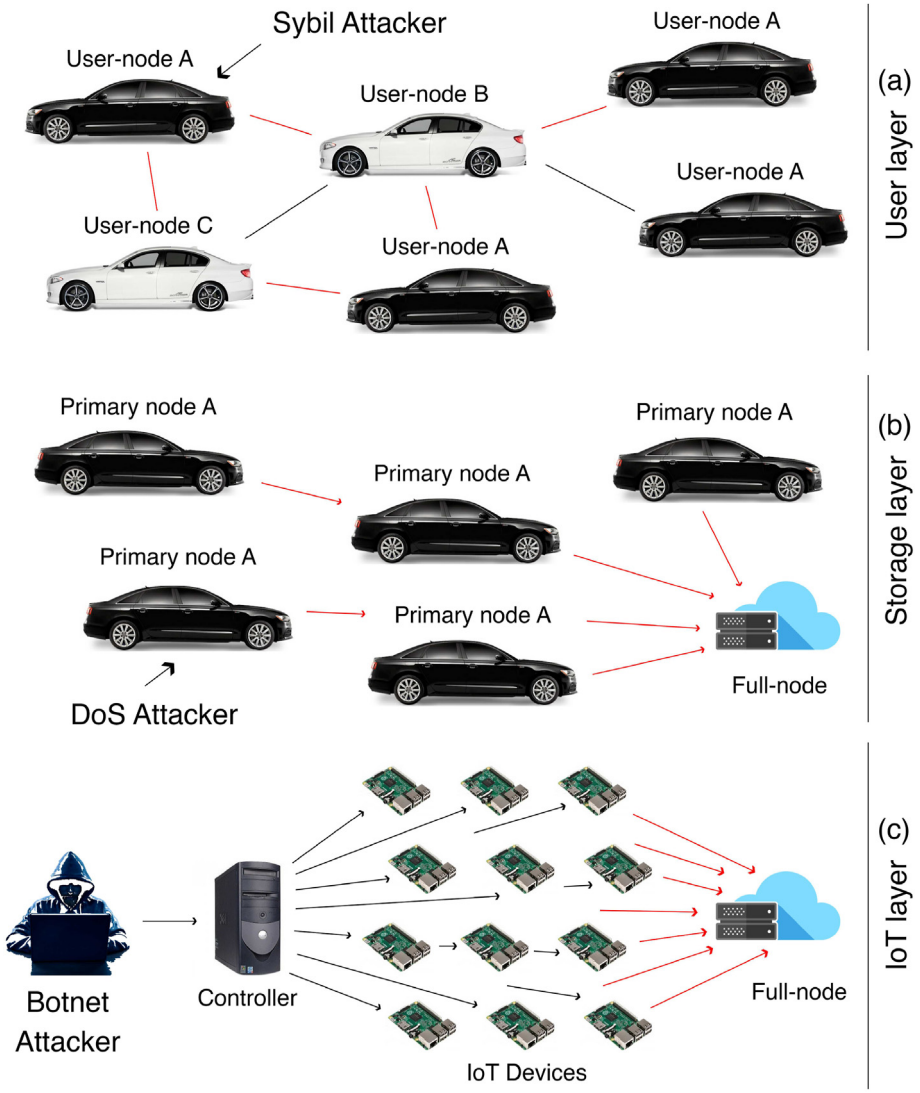


Fig. 12. User layer—Sybil attack in action, Storage layer—Denial-of-Service attack in action and IoT layer—Botnet attack in action.

and roadside infrastructures currently connect to the internet. A government initiative is required to invest funds in IoT devices and to incentivize daily commuters to connect vehicles as Moving-Nodes to the network. Legal restrictions on the use of IoT devices within a city, safety issues of commuters, lack of skilled workforce, etc. are other limitations in B-DRIVE architecture.

Because of these limitations, three major network attacks are possible at different hardware layers (Fig. 12). A "Sybil attack" at the User layer is an attack where a single node controls or acts as a source of multiple nodes in a network (Fig. 12a). It can create multiple IDs and pretend that they all exist in the same vicinity. Thus, other nodes can perceive that there is bulky traffic ahead. One way to avert this attack is by setting up an Event-Based Reputation System (EBRS), in which a dynamic reputation and trusted value for each event are hired to stop the expansion of false messages [31]. A large number of other good nodes can help subvert the computational power of attackers as well. A "Denial-of-Service" (DoS) attack is the most common way by which a Primary node (User-Node) can overwhelm a Full-Node (Fig. 12b). This attempts to flood the B-DRIVE network at the Storage layer with external requests for Running-Blockchain, making the service unavailable for other Primary nodes. DoS attacks usually target the entire network, in this case, affecting the maximum acceptable limit of Full-Nodes. One potential attack at the IoT layer is Botnet (Fig. 12c). It is a cluster of Internet-connected devices, used to perform any DoS attacks. The reason for this attack is the lack of security layers in IoT devices [32]. Botnets could control up to a few hundred of thousands of IoT devices at a time drastically hampering any service. It is one key issue of IoT technology. Khan and Salah [10] have argued that blockchain technology can be used for secure communication, authentication, authorization, device integrity, and Identity of Things (IDoT) governance for IoT security. This further backs the conceptual design of the B-DRIVE network for smart and secure urban transportation.

6. Conclusion

B-DRIVE IoT network, as presented in this paper, is a distributed network of sensor-enabled IoT devices within a city. It consists of three hardware layers (a) IoT layer, (b) Storage layer, and (c) User layer. The IoT layer consists of Moving and Static-Nodes which generate sensor data of various kinds periodically. These sensors are primarily GPS, air quality meter, gyrometer, etc. The generated data is stored into a block with encrypted node ID before any dissemination through the IoT gateway. Encryption is done using a cryptographic hash function. The IoT gateway connects to respective Full-Nodes via ISP bridge. Full-Nodes belong to the the Storage layer. They log and create a blockchain of the full history of all received IoT data. This blockchain is called as Full-Blockchain. Each Full-Node connects to a certain number of functional IoT devices depending upon their geographical location. Along with Full-Blockchain, it also maintains a Running-Blockchain for connected User-Nodes.

Running-Blockchain is a fraction of the latest blocks of Full-Blockchain. Finally, the User layer consists of User-Nodes who are primarily city commuters and end-users. A user-node connects to its nearest Full-Node or other User-Node for Running-Blockchain to perform specific navigation tasks. A node directly connecting to a Full-Node is called as Primary node. Multiple Running-Blockchains operate within a city's B-DRIVE network to meet the storage and computational requirements of smart devices. Full-Nodes also communicate with each other to maintain an exact replica of the complete history of generated blocks.

Salient features of B-DRIVE architecture over other centralized systems for smart urban transportation solutions are (a) data transparency and accountability, (b) data immutability, (c) very low or no data exchange cost, (d) instantaneous data logging, (e) data security, (f) system resilience, (g) data control, (h) system trustlessness, and (i) data standard format. No block mining activity is required as double-spending attack is irrelevant in IoT generated data. Any attacker or malfunctioning device is detectable and would be filtered out using statistical outlier detection techniques. Also, the blocks generated at the IoT layer are of similar data size and format. It improves the data storage efficiency by designing custom formats. Data mining and machine learning concepts are useful to develop predictive models using Full-Blockchain for vehicle navigation. These solutions vary from traffic modeling, user activity mapping, parking mapping to VGI dataset curation. Two identified limitations of B-DRIVE architecture are the limited processing power of existing IoT devices and the limited roadside and on-road infrastructure. These limitations can cause Sybil, DoS, or Botnet attacks.

This paper presents a preliminary and initial conceptual design of a blockchain-based distributed IoT data network around urban transportation. Future work consists of a detailed analysis of different participating components and layers of it. It is believed that a collaborative effort by geospatial scientists, application developers, IoT manufacturers, policy makers, blockchain developers, and IT professionals can bring in a better and more pragmatic B-DRIVE design. We hope that a vehicular network like B-DRIVE, working with VANET, can answer some of the lingering issues of current urban transportation. Openly accessible IoT data is believed to be useful for city commuters and dwellers, automobile manufactures, transportation authorities, and health care departments to name a few.

Declaration of competing interest

The author declare that he have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

I acknowledge financial support by Deutsche Forschungsgemeinschaft within the funding programme Open Access Publishing, by the Baden-Württemberg Ministry of Science, Research and the Arts and by Ruprecht-Karls-Universität Heidelberg. I am thankful to Prof. Dr. Charles M. Schweik (University of Massachusetts Amherst) for valuable proof reading and constructive feedback.

References

[1] United Nations, World Urbanization Prospect - 2014 Revision, Department of Economic and Social Affairs, 2015. https://esa.un.org/unpd/wup. (Accessed 5 January 2018).
[2] M.N. Smith, The Number of Cars Worldwide is Set to Double by 2040, 2016. https://www.weforum.org/agenda/2016/04/the-number-of-cars-worldwide-is-set-to-double-by-2040. (Accessed 21 March 2018).
[3] G. Lyons, Getting smart about urban mobility—aligning the paradigms of smart and sustainable, Transport. Res. Part A 115 (2018) 4–14, https://doi.org/10.1016/j.tra.2016.12.001.
[4] B. Jo, Z. Baloch, Internet of Things-based arduino intelligent monitoring and cluster Analysis of seasonal variation in physicochemical parameters of Jungnangcheon, an urban stream, Water 9 (3) (2017) 220, https://doi.org/10.3390/w9030220.
[5] Securing America's Future Energy, Congestion in America A growing challenge to U.S. Energy security, Secur. Am. Future Energy 48 (2012). https://www.ourenergypolicy.org/wp-content/uploads/2012/05/SAFE-Congestion-in-America.pdf.
[6] D.C. Shoup, Cruising for parking, Transport Pol. 13 (6) (2006) 479–486, https://doi.org/10.1016/j.tranpol.2006.05.005.
[7] T. Sexton, Asset Tracking for Transportation and Logistics, 2018. https://blog.mapbox.com/asset-tracking-for-transportation-logistics-cd8404a08e4. (Accessed 21 March 2018).
[8] Yandex Yandex Traffic jam technology Overview. https://yandex.com/company/technologies/traffic_jams_technology. Accessed 21-March-2018.
[9] M.M. Rathore, A. Paul, W. Hong, et al., Exploiting IoT and big data analytics: defining smart digital city using real-time urban data, Sustain. Cities Soc. 40 (2018) 600–610, https://doi.org/10.1016/j.scs.2017.12.022.
[10] M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Generat. Comput. Syst. 82 (2017) 395–411, https://doi.org/10.1016/j.future.2017.11.022.
[11] S. Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular Ad Hoc network, J. Netw. Comput. Appl. 37 (2014) 380–392, https://doi.org/10.1016/j.jnca.2013.02.036.
[12] W. He, G.J. Yan, L.D. Xu, Developing vehicular data cloud services in the IoT environment, IEEE Trans. Ind. Inform. 10 (2) (2014) 1587–1595, https://doi.org/10.1109/TII.2014.2299233.
[13] P. Papadimitratos, A.D.L. Fortelle, K. Evenssen, Vehicular communication systems: enabling technologies, applications, and future outlook on intelligent transportation, IEEE Commun. Mag. 47 (11) (2009) 84–95, https://doi.org/10.1109/MCOM.2009.5307471.
[14] E.C. Eze, S.J. Zhang, E.J. Liu, Vehicular ad hoc networks (VANETs): current state, challenges, potentials and way forward, in: 20th International Conference on Automation and Computing; 12–13 Sep 2014; Cranfield, UK, IEEE, Piscataway, NJ, USA, 2014, pp. 176–181, https://doi.org/10.1109/IConAC.2014.6935482.
[15] V.H. La, A.R. Cavalli, Security attacks and solutions in vehicular ad hoc networks : a survey, Int. J. AdHoc Netw. Syst. 4 (2) (2014) 1–20, https://doi.org/10.5121/ijans.2014.4201.
[16] S. Pearson, Taking account of privacy when designing cloud computing services, in: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing; 23–23 May 2009; Vancouver, BC, Canada, IEEE, Piscataway, NJ, USA, 2009, pp. 44–52, https://doi.org/10.1109/CLOUD.2009.5071532.
[17] S. Nakamoto, Bitcoin: a Peer-to-peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf. (Accessed 5 January 2018).
[18] A. Narayanan, J. Bonneau, E. Felten, et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, Princeton, NJ, USA, 2016, 0691171696 9780691171692.
[19] M. Conoscenti, A. Vetrò, J.C. De Martin, Blockchain for the Internet of Things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA); 29 Nov–2 Dec 2016; Agadir, Morocco, IEEE, Piscataway, NJ, USA, 2016, pp. 1–6, https://doi.org/10.1109/AICCSA.2016.7945805.
[20] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inform. Syst. Eng. 59 (3) (2017) 183–187, https://doi.org/10.1007/s12599-017-0467-3.
[21] T. Mekki, I. Jabri, A. Rachedi, M. Jemaa, Vehicular cloud networks: challenges, architectures, and future directions, Veh. Commun. 9 (2017) 268–280, https://doi.org/10.1016/j.vehcom.2016.11.009.
[22] Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu, A privacy-preserving trust model based on blockchain for VANETs, IEEE Access 6 (2018) 45655–45664, https://doi.org/10.1109/ACCESS.2018.2864189.
[23] R.A. Michelin, A. Dorri, R.C. Lunardi, et al., SpeedyChain: a framework for decoupling data from blockchain for smart cities, arXiv (2018) arXiv: 1807.01980.
[24] R. Shrestha, R. Bajracharya, A.P. Shrestha, S.Y. Nam, A new type of blockchain for secure message exchange in VANET, Digit. Commun. Network. 6 (2) (2020) 177–186, https://doi.org/10.1016/j.dcan.2019.04.003.
[25] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: a survey, IEEE Commun. Surv. Tutorials 17 (1) (2014) 228–255, https://doi.org/10.1109/COMST.2014.2345420.
[26] P. Jaworski, T. Edwards, J. Moore, K. Burnham, Cloud computing concept for intelligent transportation systems, in: 14th International IEEE Conference on Intelligent Transportation Systems (ITSC 2011); 5–7 Oct 2011; Washington, DC, USA, IEEE, Piscataway, NJ, USA, 2011, pp. 391–936, https://doi.org/10.1109/ITSC.2011.6083087.
[27] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: a distributed blockchain based vehicular network architecture in smart city, J. Inform. Process. Syst. 13 (1) (2017) 184–195, https://doi.org/10.3745/JIPS.03.0065.
[28] C. Decker, R. Wattenhofer, Information propagation in the Bitcoin network, in: IEEE P2P 2013 Proceedings; 9–11 Sep 2013; Trento, Italy, IEEE, Piscataway, NJ, USA, 2013, pp. 1–10, https://doi.org/10.1109/P2P.2013.6688704.
[29] P. Newson, J. Krumm, Hidden Markov map matching through noise and sparseness, in: GIS '09: 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems; 4–6 Nov 2009; Seattle, WA, USA, ACM, New York, NY, USA, 2009, pp. 336–343, https://doi.org/10.3745/JIPS.03.0065.
[30] A. Ruas, Map Generalization. Encyclopedia of GIS, Springer, Boston, MA, USA, 2008, pp. 631–632.
[31] S. Sharma, S. Sharma, A review: analysis of various attacks in VANET, Int. J. Adv. Res. Comput. Sci. 7 (3) (2016) 249–253.
[32] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: Mirai and other Botnets, Computer 50 (7) (2017) 80–84, https://doi.org/10.1109/MC.2017.201.