Suitability of blockchains to enable and support Networking functions: State of Art

Befekadu G. Gebraselase
NTNU – Norwegian Science and Technology
befekadu.gebraselase@ntnu.no

Bjarne Emil Helvik
NTNU – Norwegian Science and Technology
bjarne@ntnu.no

Yuming Jiang
NTNU – Norwegian Science and Technology
yuming.jiang@ntnu.no

ABSTRACT

The underlying network infrastructure faces challenges from addressing maintenance, security, performance, and scalability to make the network more reliable and stable. Software-defined networking, blockchain, and network function virtualization were proposed and realized to address such issues in both academic and industry wise. This paper analyzes and summarizes works from implementing different categories of blockchains as an element or enabler of network functions to resolve the limitation. *Blockchain as a network function* has been proposed to give support to the underlying network infrastructure to provide services that have less lag, are more cost-effective, have better performance, guarantee security between participating parties, and protect the privacy of the users. This paper provides a review of recent work that makes use of blockchain to address such networking related challenges and the possible setbacks in the proposal.

Keywords

Blockchain; Performance; Security; Network Function

CCS Concepts

• Networks~Peer-to-peer networks • Networks~Mobile ad hoc networks • Security and Privacy ~ Mobile and wireless security

1. INTRODUCTION

Blockchain [26] is a distributed ledger technology that allows information to be distributed. It enables the data not to be centralized or controlled by a single party. In particular, blockchain allows the involved parties to communicate and exchange in a peer-to-peer (P2P) fashion through which distributed decisions are performed by the majority rather than by a centralized authority, [29]. As the word expresses, blockchain is a chain of blocks (records). Each block has a pointer to the previous block (previous hash), nonce, and transaction list, as illustrated in Figure 1. Having the cryptographic hash of the last block makes it hard to temper or reverse the current transaction. Blockchain has been explored/exploited in a variety of fields of studies, such *as a network function in networking*, to build new medical information platforms in medicine, and for money transfer in business, identity management in security, and voting systems in social science. In networking, all current connectionless networks require network-unique addresses, and in all known systems the uniqueness is enforced by some centralized entity, e.g., the IEEE sells MAC addresses, Internet Assigned Numbers Authority (IANA) and the Regional Internet Registry (RIRs) allocate IP addresses, ICANN and the TLDs provide URLs. These entities control related activities using a centralized way. With the current progress in the number of nodes that a network supports and the number of new organizations that emerge, centralized control will reduce the flexibility and quality of service delivered to the users and may become dictatorial since all the control power is from some specific entity. Besides, to add a new network service, we often end up purchasing a dedicated network element that satisfies the service specifications. To remove this dependency between network functions and hardware proprietary vendors, innovative technologies have been proposed. They include software-defined networking, network function virtualization, and blockchain.

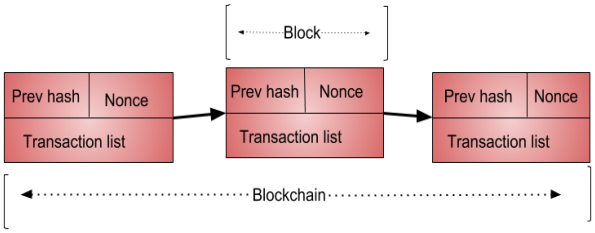

Figure 1. Typical structure of blockchain

Blockchains have properties that could change how the current network infrastructure works: As a distributed ledger, a blockchain can hardly be modified or controlled by a single or group of people or organizations; additionally, while it removes the intermediatory between parties, it still can guarantee trust between participating nodes. These promising properties can be applied to network functions or services that are currently provided only by trusted third-party brokers or using inefficient distributed approaches, which are found in network control, management and security services including AAA (authentication, authorization, and accounting), confidentiality, privacy, integrity, and provenance. In the literature, several such blockchain applications have emerged, where blockchains are exploited to enable, support, or enhance the desired network functions or services. In this paper, we classify and summarize them.

The main contributions of this paper are:

- We review the state of the art of blockchains acting as a network function and possible setbacks.
- We presented different architectures based on literature reviews and more insights.

ICENT '19, September 20-22, 2019, Tokyo, Japan

- We presented nine different areas where blockchain claimed to solve a problem and possible limitation.
- We explore the applicability of blockchains bringing robust and reliable network infrastructures.

The remainder of this article organized as follows, Section II gives a short introduction and discusses optional consensus protocols. After that, Section III explains blockchains as an element of network functions to guarantee security between participating parties in different use cases: a cognitive cellular network, mobile communication, and 5G. Section IV provided blockchain as an element of network function to enhance network control and management in various instances: wireless mesh network, Internet of things, and roadside traffic support. Section V addresses blockchain as an element of network function to increase the security in network protocols: named data networking and border gateway protocol. Finally, Section VI gathers the main conclusions obtained and make a future proposal.

2. Blockchains in Brief

This section gives a brief introduction to some aspects of blockchains that are necessary for the remainder of the paper. Readers familiar with these may skip the section.

2.1 Blockchain catagories

There are three types of blockchains public, private, and consortium. The division of the classification of blockchains only relies based on their characteristics. In public blockchain, the infrastructure is available for any users or nodes to join the network. The participating nodes need to download the records to take part in transaction or mining. The public availability of technology attracted popularity and accessibility. The flexibility and convenience of technology face significant challenges from scalability, latency, and performance. For instance, we can consider Bitcoin, one of the great electronic currency transaction. The total value of the currency up-to-date is close to USD 156 billion. Bitcoin faces challenges in increasing throughput capacity. The number of transactions supported by Bitcoin is not good enough to consider it in demanding networking.

Private blockchains are other kinds of blockchains controlled by private organization or communities. In such cases, the main challenges like performance, and latency are not the primary factors as in public blockchains. Access control in private blockchains implemented in different ways. It can be an independent authorizing system, or a set of rules to meet before joining. In private blockchains, it is easy to manage the consensus and membership services since all the nodes in the network are well known. Such alignments enable private blockchain owners or communities to plug and play functions. These properties make private blockchains more suitable for developing applications for many purposes. Developing different forms for different use allows for enhancing pure and easy access.

Consortium blockchain provides almost similar benefits as private blockchains. The main difference lies in performing validation of the transactions. In private blockchain, a single organization or company will be responsible for deciding which node can join the network. Additionally, what kind of pre-requirement must meet by the node. However, Consortium blockchains have a group of nodes or leaders that will decide for the whole network. These make it suitable for collaboration between different company or organizations. These also add enhancing security features of the public blockchain and allowing for a higher degree of control over the network. The most common consortium blockchains examples are Quorum, Hyperledger, and Corda.

2.2 Consensus protocols

In blockchains technology, nodes need to connect in peer to peer fashion and update all the modifications. If the updates are adding new records or amendments, then all the participating nodes receive the notification. Even though different organization implemented their version of consensus algorithms, the primary goal of consensus algorithms is to provide nodes to communicate and to offer validated set to add to the ledger. The most common consensus algorithms are Proof of Work, Proof of stake, Deligated proof of stake, Practical Byzantine fault tolerance, and Ripple.

2.2.1 Proof of work (POW)

POW is one of the consensus algorithms used by public blockchains like Bitcoin and Ethereum. Proof of work leads node with high resources use and computation power a more chance to solve a mathematical puzzle. By doing so, the node will earn some extra benefits. This method has exploited for 51 percent attack [25]. Relying on the computation power of nodes brings limitation on power consumption and resource use. Additionally, as the number of participating nodes rises scalability and latency increases together. Because of such significant limitations, most researchers are pointing out that practical Byzantine fault tolerance has better resource use, as illustrated Table I.

2.2.2 Practical Byzantine fault tolerance (PBFT)

PBFT is a consensus algorithm inspired by majority voting. The primary objective is reaching in consensus between distributed nodes with or without the presence of malicious nodes that sends wrong information. All the nodes communicate to one to another heavily to guarantee the transaction is not falsify and to come up an agreement through majority voting. This technique could be a useful a consensus protocol when the number of nodes is small but if the number of participating devices increases then it will be hard to reach a consensus since all the nodes should talk and update every time. Additionally, it could be easily attacked by a single entity with a vast amount of nodes. Even if there are some limitations, these techniques still considered in different kind of blockchains, e.g., Hyperledger [9].

Table I. CONSENSUS ALGORITHMS COMPARISON

Cases	**POW [4] [26]**	**PBFT [4] [9] [25]**	**POS [4] [35] [40]**	**DPOS [4] [26] [40]**	**Ripple [4] [25] [26] [40]**
Limitations	Energy consumption	Scalability	Unbalanced distribution	decentralization for speed and scalability	Highly Centralized
Energy Efficient	No	Yes	Yes	Yes	Yes
Permission	No	No	No	Yes	No
Adversary Tolerance	25%	33%	Unknown	Less than 20%	20%
Transaction Per Seconds	7-10	10-20	7	unknown	1500

2.2.3 *Proof of Stake (POS)*

POS is also a consensus algorithm like POW. These algorithms designed to overcome the disadvantages of POW, in particular, high energy consumption, as showed table I row two. This algorithm is more deterministic in ways that the node that supposes to make the mining is the one which holds more wealth or stake. Although proof of stake developed to replace POW, this method has more limitations. For instance, a node can create a transaction that it can reverse later, the more wealth hold, the more chance to earn more. A node can create a secret channel for cheating. To remove these limitations of vulnerability and the richer get more prosperous concept new consensus protocol emerged: delegated proof of stake. The most known blockchain applications to use POS method are Peercoin, blackcoin, and NXT [18].

2.2.4 *Delegated proof of stake (DPOS)*

DPOS is a similar consensus algorithm like POS. This method adds flexibility by including delegates. The delegates take part in choosing the block size, transactions fee, and the amount of payment the witness should pay. Each stakeholder has the right to take part in voting for witness but allowed to vote only once for a witness at a time. The group of witnesses will be responsible for generating and adding a transaction to the blockchains. They earn rewards for their effort. The most significant enhancement from proof of work is a reduction in energy consumption. However, since the current underlying network infrastructure will not allow too many validators to take part, achieving the devolution will be a difficult task. Although, such limitation did not stop this algorithm from used by BitShare, Nano, Lisk, and more [19].

2.2.5 *Ripple protocol consensus algorithms (RPCA)*

RPCA is a method implemented outside of using blockchain technology [19]. The primary goal of the algorithms is to reach consensus between the participating entities. It helps to maintain the correctness and agreement of the network. Once consensus achieved, the current ledger considered "closed" and becomes the last-closed ledger. This method got much criticism because of most of the coin close to 61% are already mined and controlled by Ripple Lab. It is centralized [19], and the developers have more control over when and how many coins should be released or not.

3. Blockchains to enable network-based security services

The amount of traffic generated by social networking takes second place after video streaming. The increasing demand in cellular network forces the development of higher radio spectrum. It will enable dynamic spectrum access that leads users to seek secondary access to many carriers. To make the access enabled more personal data has to share with carries. The standard protocol AAA has limitations to protect the privacy of the users. The shared information needs protection from authorized, unauthenticated, and unauthenticated access. Moreover, the performance of the AAA protocol affected by network hops, latency, and jitter. Khashayar et al. [10] proposed an algorithm that uses a public blockchain to allocates the spectrum. They managed to use virtual currency as a payment mechanism. By including a public blockchain, they offered a fair opportunity for primary users to take part in service verification. Raju et al. [1] implemented private blockchains in cellular cognitive networks. By doing so, they manage to identify and measure the credibility of the user.

A good example is Hyperledger that uses PFTB to reach consensus between participating parties. From in Table I, this protocol cannot reach all the available nodes if they distributed. Leverage the property of the private blockchain could be a good option.

Table II. BLOCKCHAIN APPLICATIONS

Cases	**VN [7] [27]**	**CCN [19] [22]**	**MC [20] [28]**	**BGP [2] [31]**	**WMN [1] [32]**	**5G [10] [20]**	**IOT [3] [29] [39]**
Scope	Incident propagation, Transactions	Identity Management	Route Announcements, Transactions	Route Announcements	Route Announcements, Database	Route Announcements, Transactions	Software updates, supply-chain transactions
Addressed Issues	Security, Performance, Scalability	Privacy, Performance	Privacy, Performance	Security	Privacy, Performance	Performance, Security	Scalability, Performance
Unaddressed Issues	Time critical	Scalability	Time critical	Scalability, Performance	Security, portability	Scalability, Performance, Latency	Latency
Implementation	Ethereum	Private Blockchain	Ethereum	BGPcoin	Bitcoin	Private Blockchain	Slock.It, Filecoin
Testbed	Simulation	Simulation	Simulation	Simulation	Simulation, Live system	Simulation	Simulation
Limitations	Power Consumption, Maintenance, Latency, Security	Power Consumption, Maintenance	Power Consumption, Maintenance, Scalability, Monitoring/ Controlling	Performance, Maintenance, Latency	Network congestions, spectrum limitation, bandwidth consumption	Maintenance cost, latency	Power Consumption, resource utilization, transparency

3.1 Authorization of mobile communication services (MC)

The service level agreement prepared by the service providers is unfair and undistributed. These service-level objects developed to increase the benefit of the company. It will make the amount of payout per individuals to become similar while the number of service usages is varying. Most of our day to day activities involve using different communication media like Wifi, WiMax, 5G, and communication. The service level agreement provided by the providers does not consider per usage rather per income. The current service level agreement mechanisms lack clarity, integrity, visibility, and maintainability. Kiyomoto et al. [28] proposed blockchain-based authorization architecture to separate communication services from billing services. The architecture has central gateway servers. Blockchains are used to make authentication and authorizations. They suggested that users can see the service level agreement and change it according to consumptions. These will enable users or customers to believe and use the available infrastructure. There is always a tradeoff when realizing a new technology. Most of the information transmitted in mobile communication is time-critical and urgent. The currently available blockchain technologies are not suitable to play in a time-critical application. The main reason is consensus protocols tasks bring latency to the system. For instance, implementing a public blockchain will bring latency in the communications channels. While considering private blockchain will bring scalability issues. Moreover, the end layer devices will be forced to take part in tasks related to mining. The main factors we should consider to install blockchains in mobile communication are power consumption, resource use, maintenance, monitoring/controlling, and latencies.

3.2 5G: Blockchain-based Trusted Authentication

Starting 3G network architecture divided into a baseband unit and remote radio unit. The division gives more flexibility to the core network to control and manage route exchange between sub-networks. But this also put too much load to the core network to control the security issues of all sub-network. In the near future, 5G will take over the cellular network. All the connected terminals will generate a massive amount of traffic to the core network. Since there is no security mechanism proposed, yet this will also open security attacks. Yanling et al. [38] propose a software-defined networking solutions. The software-defend networking controller manages traffics generated. It forwards flows tables routes to the authentication and database server. They realized a Dijkstra algorithm to calculate many routes for different media types. The authentication and database server connected to the centralized SDN controller. These may bring to a single point of failure and miss-configuration. The Dijkstra algorithm to calculate many routes has a limitation on resource use. It is a greedy approach that looks for the best routes through blind search. In such cases, implementing blockchain technologies will give more support to the technology. To address similar dilemmas Yang et al. [10] proposed blockchain-based trust authentication (BTA) architecture in C-RoFN. This architecture enables to authenticate network access with the user. It also helps to authenticate the network operator in the access area. By using the architecture, it is possible to reduce network connection cost and enhance the radio frequency. The proposal removes unified authentication in a core network and brings decentralized agreements. The virtualized edged layer take part as a middleware to process requests in data pre-processing. It also involves in aggregation, security, and privacy enhancement using blockchain technology.

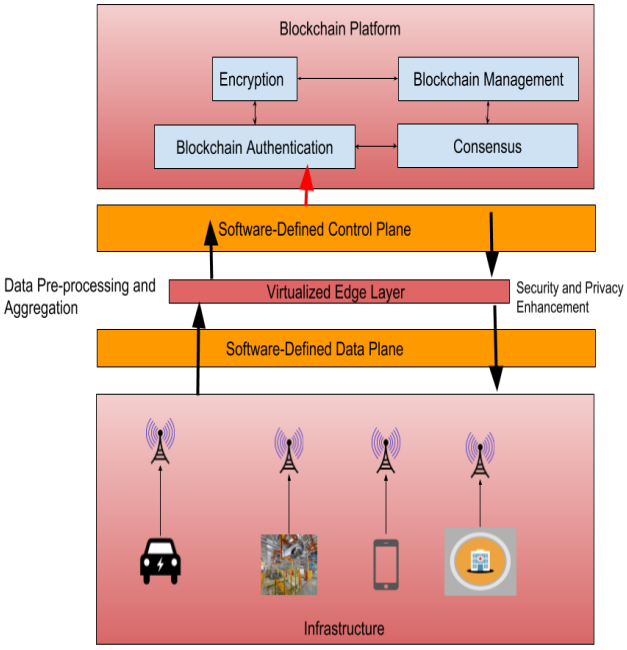

Figure 2. Blockchain-based Trusted Authentication (Edge-Enabled)

3.3 5G: Blockchain-based Network Slice

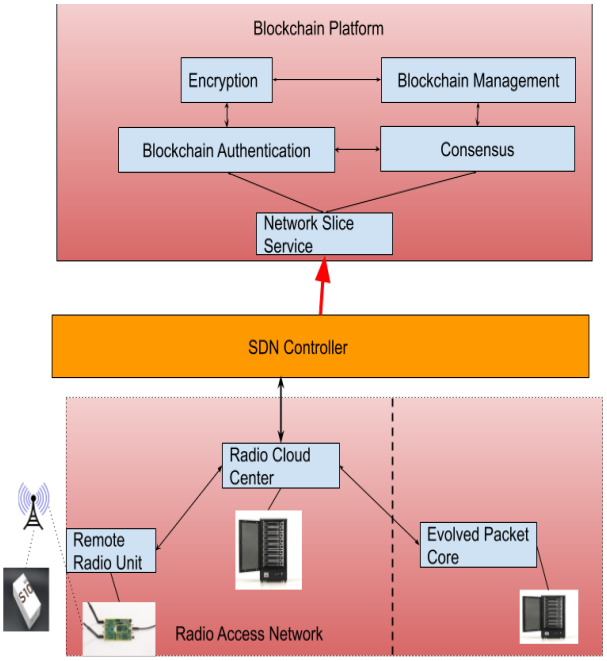

Figure 3. Blockchain-based Slice orchestration

Network slicing is one of the significant enablers in 5G services. It enables the facility to compose logical networks over shared physical infrastructures [13]. 5G network architecture is being defined by 3GPP to support connectivity and service deployments. These properties allow the service to include network function virtualization and software-defined networking. Different network vendors and researcher proposed slicing architecture that utilities NFV and SDN. The main disadvantages of previous architectures are not aware of how to provide slice isolation and sharing. In this work, we are summarising proposals that use blockchains as a use case to realize network slicing. Blockchains have significant properties guaranteeing security between participating parties. Figure 3 realizes one of the architectures proposed to enhance network slice security in 5G. Jere et al. [38] proposed blockchain-based slice leasing ledger to reduce service creation time. They offered an architecture that enables manufacturers to get slice more efficient ways. They utilize NFV and SDN for 5G network slicing and smart contract for Slice Leasing Ledger.

For services like 5G, the infrastructure requires fast access and high performance. The service needs to be fast enough to deliver end to end transport within 1-5 milliseconds. The availability of the infrastructure must provide low downtimes close to 5 minutes per year. The maintenance cost will be high since the blockchain handles most of the security part. Based on the current blockchains standards from private to the public are very far from reaching such specifications.

Table III. TYPES OF SYSTEMS

Cases	Centralized	Decentralized	Distributed
Pros	Easy to develop and maintain	High Availability	No intermediator
Cons	Single point of Failure	Difficult to Maintenance	Difficult to achieve consensus
Example	Microsoft passport	Blockchain	Multiplayer online game

3.4 Blockchain-based security for Software-defined networking

Network function is a defined functional block of network infrastructure. The infrastructure has a well-defined interface and essential behavior. Some of network function examples are routing, switching, and network broking monitoring. To add a new network service, we end up purchasing a dedicated network element that satisfies the service specifications. To remove the dependency between network function and vendor proprietary different techniques are proposed. These methods include network function virtualization and software-defined networking. Software-defined networking gives more flexibility by splitting the control plane and data plane. The control plane is responsible for handling routing and security tasks but also makes it more vulnerable to security. To address this limitation, blockchain proposed to give support to the control plane. The integrated blockchain enables security through record keeping and distributed ledger [30]. The control planes will have the same copy of records and security log entries that control the bridge in one controller will not affect the rest.

The main limitation on such realization is that the control plane tasked to perform blockchain jobs. Other than this, the main restriction comes from realizing and integrating two technologies. The main contribution of software-defined networking relies on the internet of things. In such low power devices integrating two technologies requires resource consumption reduces performance. Besides to all these facts, software define-networking has more problem by itself like software aging. Adding blockchain technologies in software-defined networking must realize the domain of implementation.

3.5 Routing payment on the Lightning Network

Blockchain is one of the technologies that transform the current way of the transactions without a third-party. There are some challenges to solve first, like scalability, performance, and latency. For instance, in bitcoin, the main problem arises with the block size. If the block size increased from 1Mb to 32Mb then loses the idea of decentralization. The full nodes will hold a vast amount of the transaction, plus all the request will be redirected to the full node that contains the longest chain. However, if the size remains the same, then the scalability still will be an open problem to address. To solve this challenge, payment routing on the lightning network proposed [7]. The lightning network is an overlay network between peer to peer communication in the underlying network infrastructure. This protocol works on the top of the blockchain. This method has similar properties like off-chain blockchain [8] [16]. Off-chains is one of the methods implemented by the blockchain community to handle transaction between two parties. It makes a transaction until a certain amount satisfied and agreed. Jourenko et al. [8] summarized all the off-chain transaction taxonomies. They presented the necessary components that play a significant role in the scalability of cryptocurrency. These include a mechanizes to create a network on the opened channel and way of managing the network. By using a lightning network, for two nodes in the network to exchange message, they open a channel to transfer the transaction like off-chain blockchain. However, the main difference arises when the number of nodes to communicate is more than two nodes. In such cases, the sending node sends the message through the intermediate node by appending a secret password. Since all the participating parties must gain a benefit so that they proposed routing payment on the lightning network, for instance, let say the peer connection between A and B, B to C established. However, we want to make the transaction between A to C, and now we can put away of payment to each node forwarding the packet to a different station. When A makes a forward from itself to B charges, some payment and B to C charges some Payment as Well. In the end, The receiver Node C uses the password to decrypt the payment and complete the transaction by closing the channel. By using the Lightning network, the performance of the network increase. The scalability also achieved without the consideration of the block size and bandwidth capacity.

Implementing a virtual network over the blockchain could bring better performance, but, losing a token between parties could deliver inconsistency and unreliable services. Additionally, Un honest party can try to cheat by not forwarding the service or could change the timestamp of the current transaction [15]. Finally, a malicious user or node can learn the pattern of the communication and figured out the encryption keys.

4. Blockchains to improve network control and management

4.1 Wireless mesh network

Developing a network that utilizes fewer expenses and provides community services are essential. These idea or concept suggested by researchers and companies for the last two decades. Developing such an environment requires more financial support. It also requires a system that generates the transaction, and a controller that manages the network traffic usage of each region. One of the best ways to have such community services is to develop a wireless mesh network. The network will have a property to divide the nodes based on geo-location. Each different subnetworks need to find a way to trust each other's activities. These activities include transactions, the number of nodes they support, and the amount of traffic generated or used. A wireless mesh network considered as one of the future community services. It will connect many sub-networks to achieve cost reduction. However, building trust between different sub-networks could be a difficult task. Including blockchain, implementation could bring confidence between the participating sub-networks. AKabbinale et al. [1] Proposed blockchain for economically sustainable wireless mesh networks. There is one of the works offered to enable complete transparency and accountability for investment and revenue. It also helps other forms of economic enjoy sharing of network traffic, content, and services. The system keeps the records of each sub-networks on deployed blockchain technologies. Blockchain technologies deployed on the access network layer. These enable blockchains to have enough information about several links, nodes, maintenance, and consumption of the network resources. This information helps in determining the amount of budget, implementation of resource use, and to keep records of transactions.

The main disadvantages of integrating blockchains in wireless mesh-networks are network congestion. In a wireless mesh network, the amount of system generated by the subnetworks increases by the number of nodes. These will cause spectrum limitation, bandwidth and CPU consumption, and lack of interoperability [32]. In such implementation, wireless gateway routers will have more responsibility to perform. These duties include adding a transaction, mining blocks, and time-stamping everything. It could cause traffic congestion and overload. For instance, if the battery of one of the gateway routers failed or shutdown, this creates an overhead to the network. Additionally, users data travels through different wireless hops that cause privacy concern. With high capital and maintenance capacity, such deployment will remove intermediary providers — for instance, Wi-fi, phone carriers, and middleman between organization.

4.2 Internet of Things

Internet of things is the network of Interconnected devices. The connection of devices either in heterogeneous or homogeneous environment faces some challenges. These challenges include transparency, audibility, conflict of identity, and forks [5]. Several ways of managing devices considered by companies centralized, decentralized, and distributed. It is very challenging to reach all the available nodes from the centralized system [3]. The main difficulties can be a failure from the server-side or client-side; either way, it is hard to manage it centrally. However, decentralized means of controlling the devices face performance issues. By including blockchains and smart contract [18], these issues can be removed. Then, activating the smart-contract to update the firmware any time it detects the latest version. Blockchain technologies included as middleware between the network and application layer. By using blockchain, it is possible to control and manage devices inside in the same ecosystem. Given that IoT devices are connected fully or partial, they are susceptible to an attacker. It is vital to secure update patches and communications. Blockchains, on the other hand, bring security through public key stored in the blockchain platform and private key stored in IoT devices [12].

Blockchains implementations in the internet of things are maintaining the balance as a middleman. They provide services between the network and the application layer. As proposed in Figure 6, these technologies should consider the capacities of end layer devices. The devices supported by the internet of things throughput capacity is different in each layer. The leading development of blockchain technologies is to act as a distributed ledger. This ledger includes security through a cryptographic hash of previous blocks. It will also result in a low susceptibility to manipulation and forgery by malicious participants [21]. Implementing such technology in monitoring and managing the network traffic need research works from academic and industry. Most works of blockchain in the internet of things are acting as a middleware between application and network layer. These tasks include hiding heterogeneity of hardware, operating systems, and protocols [34].

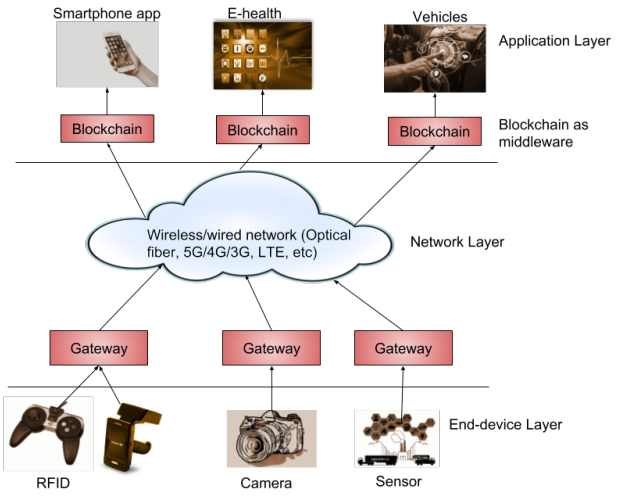

Figure 4. Three-layer of internet of things architecture with blockchain as middleware

Adding such a job in blockchain application over low power and computation devices is not adequate. Blockchains in the internet of things take part in providing uniform, and high-level interfaces, reusable, and portable applications. These requirements need a set of standard services that cut duplication of efforts. Merging all the properties of middleware into either public or private blockchain must consider the deployment environments. Implementation of blockchains in the Internet of things faces challenges from storage, computation capacity. As illustrated in

Figure 3, the end-device layer comprises sensors and low-power embedded platforms. In such devices, blockchain demands synchronization between participating devices. These will need enough bandwidth and computations power, which is very hard to guarantee. In low-power devices, the size of the memory is close to the 10kb and storage capacity of 100kb, but blockchain platforms demand GBs of memory. Other than this, the heterogeneity of devices also plays critical impacts on the performance. Because all the tools not manufactured to perform computation power, it is challenging to integrate devices.

In this part, we only tried to address a high-level limitation of considering blockchain in the internet of things since the consideration of blockchain in this area is increasing so we believe an independent work would satisfy the reader.

4.3 Road Traffic Support

Vehicle to vehicles communication reduces traffic incidents, jams, and pathways blocks. These properties improve day to day activities. However, making the information exchange between vehicle to vehicles raises privacy and security. The communication between cars managed by the centralized system. This system not only has a weakness of vulnerability for a single point of failure. However, it has scalability and performance limitation on reaching all the vehicles that are on mobility. It is also difficult to support a different kind of vehicular networks. Blockchains are considered to remove such challenges. Some of the contributions include trust management in Vehicle to vehicle communication. Smart Vehicles communication and cars to charge stations connection.

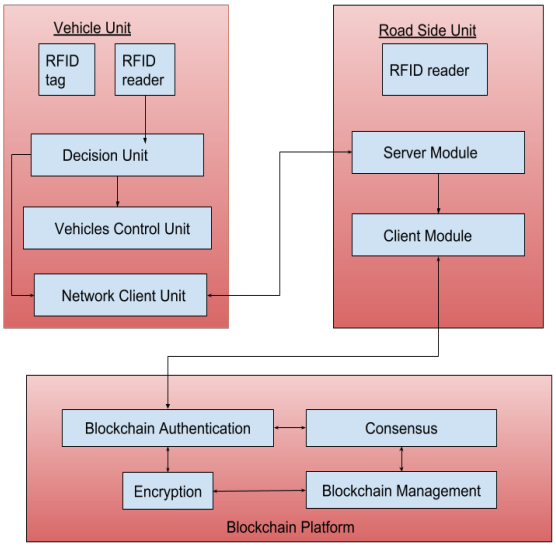

Figure 5. Road Traffic Support relationship between vehicles to roadside unit

4.3.1 Trust Management in Vehicles Network

In the centralized trust management system, the cars and roadside unit (RSU) connected to the central server. The central server provides the rating information. Based on the current progress, it calculates and stores trust values of vehicles to vehicles communication. The centralized system faces a high amount of request and high latency. The main factors the number of intelligent vehicles are increasing very fast.

In contrast, a decentralized system can cope up with the growth rate of intelligent vehicles; however, since the collected information stored on RSU, which will make it less consistent and incomplete. Yang et al. [39] proposed private blockchain-based decentralized trust management system. It provides a distributed ledger that is hard to temper (malicious vehicles could easily be discarded from the system). The RSU is responsible for collecting rating information and trust value management. The cars, at the same time, will manage traffic-related events. They send a warning message to other vehicles. The communication protocol can be using vehicles to vehicles communication standards (Long-term Evolution Vehicles to Vehicles (LTE-V2V), Dedicated short-range Communication (DSRC), and Vehicle Ad Hoc network (VANET)).

The main setbacks of the previous approaches come from RSU server and decision unit of vehicles. The RSU server module becomes overloaded by collecting traffic-related events. The decision unit of the cars will be responsible for sending warning messages and guaranteeing the arrival. Additionally, the decision unit of the vehicle will be to overload in the case a large amount of traffic propagation. The processing capacity of the server module and decision unit must be considered as a critical point in the implementation.

4.3.2 Communication of Smart Vehicles

Vehicle Ad Hoc network (VANET) is one of the vehicles to a vehicle's communication standard [27]. The transferring or sending a message to another vehicle requires identifying the source, plate number, and the identity of the owner. On such occasions, vehicles owner loses interest to broadcast any incidents, jams or congestions. To solve privacy and motivation to publicize the different event mechanisms proposed: Threshold Authentication [14], Credit Network with Blockchain, and a privacy-preserving blockchain based incentive announcement network. Threshold Authentication, if the number of vehicles that confirmed the message is higher than the threshold value, then the message considered honest and valid. This methodology has two limitations if the number of malicious nodes or vehicles are higher than the number of correct nodes then the news tempered, the privacy of the event broadcaster including the owner identity is not secured. In Credit network with blockchain, each node has a point regarding there reputation so that to find the dishonest node is very easy. The only disadvantage is that it is simple to trace the coins through the public key. However, it is tough to trace the transactions that make it less reliable.

However, L. Li [22] designed privacy-preserving vehicles announcement protocol on a blockchain network. It maintains the reliability and anonymity of the messages. To increase the motives of the users have accounts at different addresses. Where they collect the coin, they gained for providing or announcing the events to the neighbors who need it.

4.3.3 Electric Vehicles and Charging Stations

The international energy agency forecasted the number of electric vehicles would reach 125 million by 2030 and increased by 57 percent in 2017. The domination of electric cars also brought another attention, which is charging stations. The main problem arises from the amount of time the vehicles owners need to recharge. If electric cars want to reload from the charge station, the owner needs to reload more often than oil gas, which means the owner needs to pay for the transaction each time. Such demands make the Bitcoin community to developed the off-chain transaction. In the off-chain operation, the transaction fee is charged only to open and close the channel. To even reduce the

cost of the transaction bitcoin-based payment network proposed. E Erdin et al. [6] created a virtual topology payment channel network. They managed to cut the transaction fee by allowing vehicles to recharge from any one of the stations. The stations are connected to the virtual interface on the top of the blockchain. The channel is open between the two participating parties may bring inconsistency. To overcome the limitation, the new method evolved. The lightning network is an overlay network between peer to peer communication. It works on the top of the blockchain and has similar properties like off-chain blockchain. For two nodes in the system to exchange message, they open a channel to transfer the transaction like off-chain blockchain. However, the main difference arises when the number of nodes to communicate is more than two nodes. In such cases, the sending node sends the message through the intermediate node by appending a secret password that is well known by the receiver since all the participating parties must gain a benefit so that they proposed routing payment on the lightning network.

The implementation of blockchains in roadside traffic management brings advantages to transport management. It will reduce traffic jams, incidents, and enhance road management system. The deployment of blockchains should consider power consumption, latency, maintenance, and security. The RSU server and client modules take part in performing blockchains tasks. The tasks to mining block, time-stamping, and adding transactions. Such responsibilities help the road management system but add more overload to RSU unit. For example, in the case of the public blockchain, the consensus protocol is POW, which consumes too much power. The number of transactions per seconds is less than the amount of throughput needed by a traffic management system. Besides that, by implementing Etherium or Bitcoin on the roadside traffic management system will affect the cost of maintenance. The battery life of RSU, and network instability, while the removal of the RSU unit that holds the longest chain, another limitations to be addressed before implementations.

5. Blockchains to enhance security in network protocol

5.1 Border Gateway Protocol

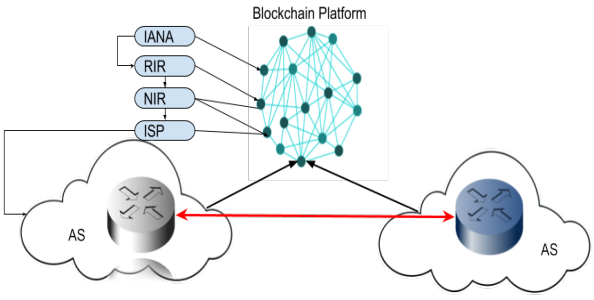

Figure 6. Architecture of BGP with blockchain resource management.

BGP is the only implemented protocol to exchange routing information between two different autonomous systems. It designed without the intention of possible attackers like prefix/sub prefix hijacks. The Internet Engineering Task Force (IETF) Secure inter-domain routing (SIDR) proposed Resource Public Key Infrastructure (RPKI). It works on centralized authorities. This system has a high chance of miss-configuration and compromised RPKI authorities. So other techniques proposed by the researchers on how to handle such limitation on RPKI. Appending the transparency log to alarm the changes on RPKI and adding inanimate objects to realize the revocation. However, even adding such a method will not guarantee if the malicious authorities delete or modify objects. Besides that, to respond to such activities based on the alarm system takes time.

Moreover, revocation in RPKI requires complicated collaboration with resource certificate issuers. Jun et al. [17] present an Expectation Exchange and Enforcement mechanism. It defines policies between autonomous systems such that any independent system may enforce such policies. Kumar and Crowcroft [2] proposed security of distance-vector related routing protocol through digital signature. They performed loop detection in pathfinding to verify the selected route's path information is correct. Xing, Q. Wang, B. Wang [31] propose public blockchain-based internet number resource authority and BGP security, which implemented a blockchain application that provides temper-resilence and transparent internet routing registry plus origin repository and governance infrastructure for BGP security. Additionally, they developed a lightweight framework on blockchain to replace RPKI authentication based on origin.

Blockchains considerations in BGP has enhanced the security of prefix and subfix hijacks. The implementation of blockchains in BGP needs to consider performance and latency. Blockchains are designed to acts as a distributed ledger between participating parties IANA, RIR, ISP, and NIR. In such deployment, security must be given a higher priority since a single break can cause global attacks. For instance, based on the current state of the art, public blockchains have route announcement capacity of 10 to 20, which is less throughput for BGP.

Furthermore, public blockchains like Bitcoin ability to generate new route blocks takes 10 minutes that is not enough. If we prefer to put in place either private or consortium blockchains, the autonomous node gets responsible for management. These tasks include organizing, access control, and resource management. The current BGP protocols take 30 minutes to propagate new routes, but if blockchains considered, then it may go beyond. Adding a new independent system needs to download whole records in which cases may take weeks and more depending on bandwidth.

5.2 Named Data Networking

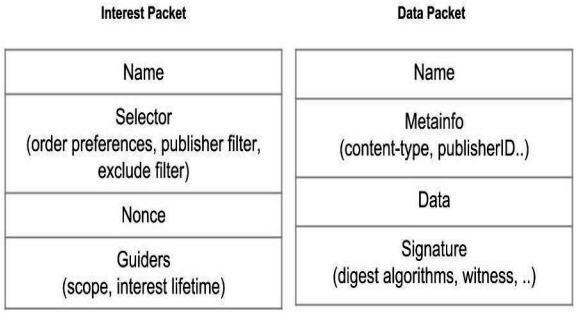

Figure 7. Named Data Networking architecture

The Internet is as the massive interconnection of computers or nodes. The information exchange between participating nodes is done using TCP/IP. It provides reliable and delivery guarantee

services. Although some would agree that TCP/IP has some limitation on securing network flow, it has no particular way to broadcast messages to some specified group. So implementing blockchain on it considered not adequate. Mohammad et al. [24] proposed policy-based security module in TCP/IP stack and policies include security policy in the application layer. Security control and data security layer in the transport layer. Hao-yu et al. [34] addressed the issues related to TCP/IP agreement has some specific security bugs. They analyzed the limitation of the protocol in performing an agreement. The parameters are unreliable identity authentication, information divulging not prevented, and weak protection against data integrity. The proposed possible counter solutions. Jin et al. [33] suggested another protocol to exchange message between different parties on the Internet Named Data Networking (NDN) [33]. It is different from the defacto protocol TCP/IP in architecture and concept-wise. NDN architecture has two communication unit: interest packet and the data packet, as illustrated in Figure 6. Interest packet is the named representative or description string of the data packet, the relationship between the interest packet and data packet is always one to one. If a requester wants to get the data packet needs to send the request by presenting the interest packet. As each of the packet transition can be traced and no IP addressing, then malicious nodes or system could be easily traced out.

NDN has two essential properties: it works on the content of the data and allows multicasting. This system behavior makes it more appropriate for data transmission. Jin et al. [33] proposed a bitcoin blockchain decentralized system over NDN. For a new node to take part in the network needs to download the whole record. While the miner continues working on the current transaction. After that, the miners broadcast the new update to the system. In the end, the listeners check the correctness of the block then update their local blockchain up to date. Since the nodes in NDN can send the message to a collection of groups at a time will increase the performance of the network. Some researchers suggest that implementing blockchain technology in the current internet protocol TCP/IP is wrong decisions even so deploying it on Named data networking (NDN) could bring better performance and provide less latency service [33]. However, changing TCP/IP prefixes to named URLs will take a considerable amount of times. Besides that, NDN has unsolved problems: how to manage naming, routing, security, and application development.

6. Conclusion

The main aims of including blockchains in the networking infrastructure are to enhance security, to increase performance, to reduce latency, and to build trust between participating parties. In this paper, we presented the nine different areas where blockchain claimed to solve the challenges. Blockchains are making an impact in various domains, including networking. Table II demonstrates the contribution of blockchain as an element of network function in networking. As we can see from Table II, most of the contributions are to guarantee security and performance. Although there are contributions to support the performance of the network environment, most of them lack considering the limitations. The development phase requires the considerations of power consumption by the miners. The time it takes for the miners to finish and propagate the update is also another factor. The underlying network infrastructure complexity differs in different conditions and environment. Performing a test case only in simulation and modeling reduces the contributions. The proposed architecture and deployment in mobile and cellular network lack more research works. In mobile and cellular network, the main challenges come from resource use. The nodes in the mobile and cellular network have small capacity comparing to what needed in the blockchain. Finally, time-critical matters are vital in networking. So in such an environment considering blockchain to provide network function delay the services. Besides, if the development of the lightweight framework that considers all the limitation introduced by Table II, then realizing blockchains as a network function brings more advantages to the current network infrastructure.

7. REFERENCES

[1] Aniruddh Rao Kabbinale, Emmanouil Dimogerontakis, Mennan Selimi, Anwaar Ali, Leandro Navarro, Arjuna Sathiaseelan, "Blockchain for Economically Sustainable Wireless Mesh Networks," 2018.

[2] B. Kumar, and J. Crowcroft. "Integrating Security in Inter-Domain Routing Protocols" ACM Computer Commun. Review], pages 36 51, 1993.

[3] Boudguiga Aymen, Bouzerna Nabil, Granboulan Louis, Olivereau Alexis, Quesnel Flavien, Roger Anthony, and Sirdey Renaud, "Towards Better Availability and Accountability for IoT Updates by means of a Blockchain," 2017

[4] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)], Banff, AB, 2017, pp. 2567-2572.

[5] Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing and Internet Technology, 2015.

[6] E Erdin, M Cebe, K Akkaya, S Solak, E Bulut, S Uluagac, "Building a Private Bitcoin-based Payment Network among Electric Vehicles and Charging Stations," 2018

[7] Giovanni Di Stasi, Stefano Alallone, Roberto Canonico, Giorgio Ventre, Routing Payments on the Lightning Network], Napoli, 2018.

[8] Gudgeon, Lewis et al. "SoK: Off The Chain Transactions," IACR Cryptology ePrint Archive 2019

[9] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)," 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, 2017, pp. 253-255.

[10] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee and Y. Ji, "Blockchain-based trusted authentication in cloud radio over fiber network for 5G," 2017 16th International Conference on Optical Communications and Networks (ICOCN)], Wuzhen, 2017, pp. 1-3

[11] Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D. and Wagner, D., "Smart locks: Lessons for securing commodity internet of things devices.," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security

[12] Huh Seyoung, Cho Sangrae, and Kim Soohyung, "Managing IoT devices using blockchain platform," 2017

[13] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in a factory of the future use case," 2017 Internet of Things

Business Models, Users, and Networks], Copenhagen, 2017, pp. 1-8

[14] J. Shao, R. Lu, X. Lin and C. Zuo, "New threshold anonymous authentication for VANETs," 2015 IEEE/CIC International Conference on Communications in China (ICCC), Shenzhen], 2015, pp. 1-6.

[15] Jordi Herrera-Joancomartí et al. “On the Difficulty of Hiding the Balanceof Lightning Network Channels,” IACR ePrint Archive 2019

[16] Jourenko Maxim, Larangeira Mario, Kurazumi Kanta, and Tanaka Keisuke, "SoK: A Taxonomy for Layer-2 Scalability Related Protocols for Cryptocurrencies," 2019

[17] Jun Li, J. Stein, Mingwei Zhang, and O. Maennel, "An expectation-based approach to policy-based security of the Border Gateway Protocol," 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA], 2016, pp. 340-345.

[18] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

[19] K. Kotobi and Sven G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," 2017 Wireless Telecommunications Symposium (WTS)], Chicago, IL, 2017, pp. 1-6.

[20] K. Valtanen, J. Backman and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case," 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)], Barcelona, 2018, pp. 185-190.

[21] Kshetri Nir, "Can Blockchain Strengthen the Internet of Things?," IT Professional, 2017

[22] L. Li et al., "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," in IEEE Transactions on Intelligent Transportation Systems], vol. 19, no. 7, pp. 2204-2220, July 2018

[23] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-5.

[24] M. Al-Jarrah and A. R. Tamimi, "A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement," 2006 Innovations in Information Technology, Dubai], 2006, pp. 1-5.

[25] N. Bozic, G. Pujolle and S. Secci, "A tutorial on blockchain and applications to secure network control-plane," 2016 3rd Smart Cloud Networks \& Systems (SCNS), Dubai, 2016, pp. 1-8.

[26] Omar Dib, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, Elyes Ben Hamida, "Consortium Blockchains: Overview, Applications, and Challenges," International Conference on Wireless and Mobile Communications, ICWMC, Nice, June 2017.

[27] S. Harrabi, W. Chainbi, and K. Ghedira, "A multi-agent proactive routing protocol for Vehicular Ad-Hoc Networks," The 2014 International Symposium on Networks, Computers, and Communications,] Hammamet, 2014, pp. 1-6.

[28] S. Kiyomoto, A. Basu, S. Rahman, and S. Ruj, "On blockchain-based authorization architecture for beyond-5G mobile services," 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, 2017, pp. 136-141.

[29] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[30] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017

[31] S. Raju, S. Boddepalli, S. Gampa, Q. Yan and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," 2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6.

[32] Selimi Mennan, Rao Aniruddh, Ali Anwaar, Navarro Leandro, Sathiaseelan Arjuna, "Towards Blockchain-enabled Wireless Mesh Networks," 2018

[33] Tong Jin, Xiang Zhang, Yirui Liu, Kai Lei, "BlockNDN: A bitcoin blockchain decentralized system over named data networking," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)], pp. 75-80, 2017

[34] W. Hao-yu, C. Hui-Zhi, Z. Xu, J. Chao-jun and J. Xiao-Juan, "The Security and Promotion Method of Transport Layer of TCP/IP Agreement," 2010 Second International Conference on Information Technology and Computer Science, Kiev], 2010, pp. 513-517.

[35] W. Y. Maung Maung Thin, N. Dong, G. Bai, and J. S. Dong, "Formal Analysis of a Proof-of-Stake Blockchain," 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS), Melbourne, Australia, 2018, pp. 197-200.

[36] Wang Xu, Zha Xuan, Ni Wei, Liu Ren, Guo Y, Niu Xinxin, and Zheng Kangfeng, "Survey on Blockchain for Internet of Things," Computer Communications, 2019]

[37] Xing, Q.; Wang, B.; Wang, X. "BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution," Symmetry 2018, 10, 408.

[38] Y. Zhao and X. Zhang, "New media identity authentication and traffic optimization in a 5G network," 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing], 2017, pp. 1331-1334.

[39] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, Blockchain-based Decentralized Trust Management in Vehicular Networks, in IEEE Internet of Things Journal \& 10.11.2018.

[40] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin, "Blockchain challenges and opportunities: A survey" International Journal of Web and Grid Services,] 2018.