Blockchain Incentivized Data Forwarding in MANETs: Strategies and Challenges

Caciano Machado*, Carla Merkle Westphall

Departamento de Informática e Estatística – Universidade Federal de Santa Catarina

Abstract

Recently, blockchain trustless properties started to be investigated to design cooperation enforcement mechanisms in many systems. This paper presents a comprehensive and detailed review of works on blockchain-enabled data forwarding incentives for multi-hop MANETs. We contextualize the problem of selfish misbehavior in networks composed of routers that are property of different participants: community, D2D, and vehicular networks, including DTN alternatives. We discuss how uncooperative behavior from multiple device owners leads to unreliable communication affecting trust in MANETs. We summarize pre-blockchain incentive mechanisms for data forwarding, classified as credit-based and reputation-based, and outline game-theoretic approaches. We discuss blockchain features useful for data forwarding incentives in multi-hop MANETs, detailing off-chain mechanisms that have been applied in the state-of-the-art. We describe the critical points in the state-of-the-art based on research papers, patents, and products. Finally, we discuss and summarize existing strategies and challenges for further research.

Keywords: manet, free-riding, blockchain, incentive mechanisms, community networks

1. Introduction

Specific mobile ad hoc networks (MANET) have been proposed to expand network coverage to regions that conventional networks cannot reach. Some examples of MANETs are community networks, device-to-device (D2D) networks, and vehicular networks (VANET). The main goal of community networks [1, 2, 3] is to provide Internet access to low-income and remote areas, where commercial service providers and public policies do not reach. D2D networks [4] enable wireless communication among personal devices and the Internet of Things (IoT) as a complement to infrastructured networks. VANETs [5] allow communication along roads using vehicles as relays. D2D and VANET could also be designed as Delay-Tolerant Networks (DTN) [6] that admit long communication delays.

Those MANETs require cooperative sharing of resources to enable reliable data forwarding. However, misbehaved nodes could undermine network reliability by acting selfishly, taking advantage of cooperation from other devices, and avoiding making their resources available. This behavior is also known as *free-riding*.

There is plenty of research in mechanisms that aim to prevent free-riding as shown in the survey from Jedari *et al.* [7]. Most of them adopt credit-based incentives or trust-building reputation mechanisms. Game-theoretic modeling has also been investigated in order to maximize data delivery ratio among participants. Credit-based mechanisms require tamper-resistant hardware modules or trusted third-parties. Reputation-based mechanisms are prone to second-order free-riding [8], which consists of devices that avoid contributing to the reputation mechanism.

Recently, blockchains started to be adopted to provide financial compensation for collaborative participants in MANETs. Blockchains have trustless properties (i.e., they achieve dependable and secure properties without the need for trusted third-parties) [9] that apply to incentive mechanisms in MANETs. These properties could allow collaborative nodes to join and leave MANETs without prior trust assumptions and to be rewarded according to their cooperation. This work aims to gather the state-of-the-art in multi-hop incentivized MANETs that adopt blockchains for incentives in data forwarding, outline their strategies, and discuss their challenges. Our contributions are: an overview of the state-of-the-art in blockchain-based mechanisms for incentives in data forwarding in multi-hop MANETs; outline their strategies and challenges; discuss directions for further research to advance in this topic.

After this introduction, we organize this paper as shown in the roadmap of Figure 1. Section 2 contextualizes reliability and trust issues due to the free-riding problem in data forwarding in multi-hop MANETs. Section 3 shows pre-blockchain incentive mechanisms for this problem proposed in the literature. Section 4 presents an overview of blockchain concepts. Section 5 is a review of the state-

*Corresponding author.

Email addresses: caciano.machado@ufrgs.br (Caciano Machado), carla.merkle.westphall@ufsc.br (Carla Merkle Westphall)

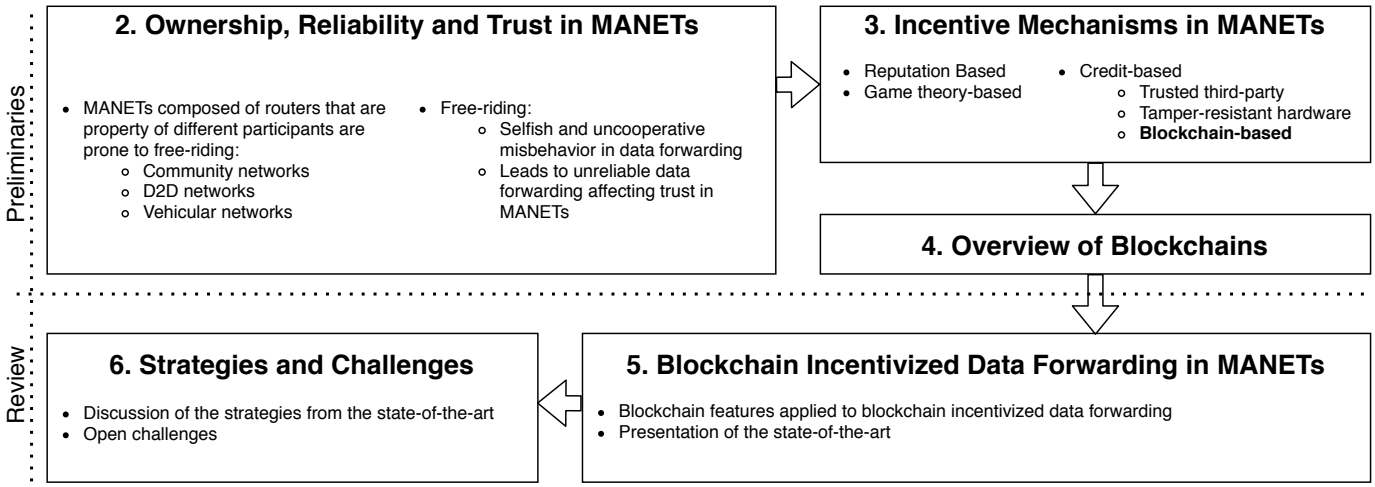

Figure 1: Roadmap of this paper

of-the-art consisting of research papers, products, and patents. Section 6 is a discussion of the incentive strategies found in the state-of-the-art and open challenges. Finally, Section 7 presents our conclusion.

2. Ownership, Reliability and Trust in MANETs

Other works review the problem of cooperation in MANETs in a user-centric (or human-centric) perspective [10, 7]. We consider the ownership of devices and their relationship with reliability in a more general and precise viewpoint. We analyze the selfish misbehavior in MANETs according to how participants (economic agents as individuals or organizations) allocate their network resources to cooperate ith other participants.

This section characterizes network elements that present selfish misbehavior and how their conduct compromises reliable communication. First, we present a misbehavior classification for MANETs to distinguish selfish misbehavior from malicious activity. Later, in order to contextualize the problem of network router's selfish misbehavior in multi-hop MANETs, we describe the expected consequences of selfish misbehavior in MANETs network elements. Moreover, we discuss how router ownership affects data forwarding reliability and, consequently, their trustworthiness. Finally, we describe well-known types of MANETs that are prone to such selfish misbehavior.

2.1. Misbehavior in MANETs

Misbehavior in MANETs can be classified according to the intention of the participants, as shown in Figure 2. Unintentional misbehavior appears independently of a participant's will, such as node mobility and transmission errors. Intentional misbehavior can be subdivided into malicious and selfish. Malicious misbehavior consists of attacks such as vandalism, denial of service, and exploration of protocol vulnerabilities. Selfish misbehavior consists in refusal to cooperate in the network operation providing computational, network and energetic resources because this implies an opportunity cost.

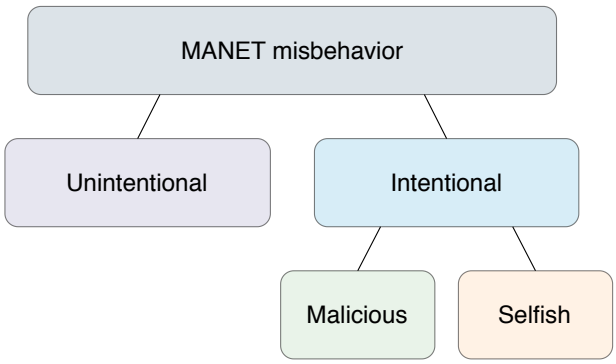

Figure 2: MANET misbehavior

A MANET assumed to be cooperative in order to guarantee its sustainability may have its resources depleted by a lack of cooperation and excessive or uncoordinated demand. The most direct effects of selfish misbehavior in the reliability of packet-switched MANETs are packet loss and delivery delays. These effects are due to selfish routers that drop or delay packets, and avoid to cooperate, overloading other cooperative routers. Applications that rely on protocols with confirmation, such as those over TCP/IP, could be affected by packet loss. Real-time applications such as voice calls, videoconferences, or control loops, could be affected by high latency and jitter. To better contextualize the problem that this survey focuses, we illustrate examples of selfish misbehavior in the lower network OSI layers: physical layer, link layer, and network layer.

2.1.1. Physical Layer

Disputes for channel allocation in unlicensed radio frequencies is an example of selfish misbehavior in the physical layer [11]. Nodes competing for selfishly using a non-

regulated radio spectrum in the same area could lead to inefficient spectrum allocation and interference. Cognitive radios [12, 13] deal with this problem sensing environment spectrum usage and dynamically changing signal frequency, bandwidth, waveform, and power.

Figure 2 illustrates access points disputing channel allocation over time in IEEE 802.11 unlicensed spectrum. In this example, access points A, B, C, and D have radio signals in overlapping areas, as shown in Figure 2a. Thus, they need to cooperate to avoid interference, adjusting radio frequency, bandwidth, and power. Figure 2b shows channel allocation changes of each access point over time. In case of interference, node B does not cooperate because it never changes channels or decreases power to reduce coverage. Also, node B allocates channels 3 and 4 simultaneously, and it does not reduce its bandwidth when nodes C and D try to use channel 3.

2.1.2. Link Layer

IEEE 802.11 CSMA/CA MAC protocol design relies on random contention times for the wireless channel shared among multiple active nodes. The protocol assumes cooperative behavior and operates efficiently if nodes follow random times strictly [14]. However, with the emergence of programmable network adapters, firmware can be overwritten to maximize individual nodes' performance selfishly [15].

In this situation, instead of respecting the protocol binary exponential backoff process before starting a transmission to avoid traffic congestion in the network, selfish nodes could reduce contention window sizes to increase their chance of gaining media access to communicate. Figure 4 illustrates the backoff slots from the contention window that could be reduced to increase the chance of gaining media access. If this behavior is widespread in the local link, then the number of collisions would deplete its capacity.

2.1.3. Network Layer

Multi-hop networks composed of routers that are property of different owners are prone to the free-riding problem. In this context, a free-rider is a router that consumes more than contributes to the network, i.e., produces messages that are rightly forwarded by other routers, but do not relay messages from other devices reciprocally. In other words, a free-rider router takes advantage of cooperation from other routers and selectively avoids using its resources (energy, processor, memory, storage, and bandwidth) to contribute with the routing protocol and to forward messages from other devices. From an individual perspective, discarding messages may be advantageous to a router than relaying them to the next-hop. This allows the router to prioritize its own traffic, tasks and to preserve battery lifetime. However, when free-riding behavior is widespread, it degrades network dependability and performance. This survey focuses on the problem of free-riding applied to multi-hop MANETs [16] [17].

Figure 5 illustrates a MANET with messages represented by M_{SD}, where S is the source node and D is the destination node. Each message M_{SD} has only one source and one destination, though this problem description can easily be extended to the cases that the message has one source and multiple destinations. The path of message M_{AF} includes node B, which is a selfish node that characterizes a free-rider. Node B discards message M_{AF} to prioritize its own traffic. Though, node B still takes advantage of the cooperation of other nodes and keeps producing messages that are relayed rightly by them.

2.2. Reliability affects Trust

In a general definition derived from social sciences, trust is the degree of subjective belief about a particular entity's behavior. In this context, the reputation of an entity is established from its previously performed actions. Due to the unique characteristics of MANET environments and the inherent unreliability of wireless channels, particularly collaborative MANETs, composed of routers that are property of distinct owners, the concept of trust in MANETs should be carefully defined [18]. We adopt the trust definition from Li and Singhal [19], who states that trust is the belief that an entity is capable of performing reliably, dependably, and securely in a particular case. The particular case here is the data forwarding in MANETs.

Trust management systems intend to improve network reliability and usually are based on monitoring, directly and indirectly, nodes' behavior. The rationale is to trust on the most reliable nodes, i.e., nodes with a higher probability of forwarding packets or contributing to the routing protocol. A series of works use reputation mechanisms to evaluate nodes' trustworthiness for reliable and secure packet forwarding [20, 21, 22, 23].

2.3. Ownership affects Reliability

This subsection describes how ownership affects nodes' reliability and, in consequence (Section 2.2), trust in MANETs. Multi-hop MANETs composed of devices that are property of distinct participants are prone to the free-riding problem illustrated in Figure 5. In such scenarios, selfish users tend to give preference to their own traffic in detriment of others' traffic [16] [17]. Selfish users avoid sharing capital expenditure (CAPEX: routers, antennas, cabling, and licensing) and operational expenditure (OPEX: backhaul contracts, electric energy, working hours, and maintenance) to forward traffic that is not useful to them. From a selfish perspective, traffic from other users is not useful. Selfish nodes tend to lower others' traffic preference or even to reject forwarding because allocating resources to forward others' traffic is an opportunity cost. This selfish behavior affects MANET nodes' reliability and, thus, their trustworthiness (Section 2.2).

Some works [24] also argue that in networks without a central authority, nodes tend to act selfishly. In contrast, selfish misbehavior does not affect networks composed of routers that are property of institutions such as

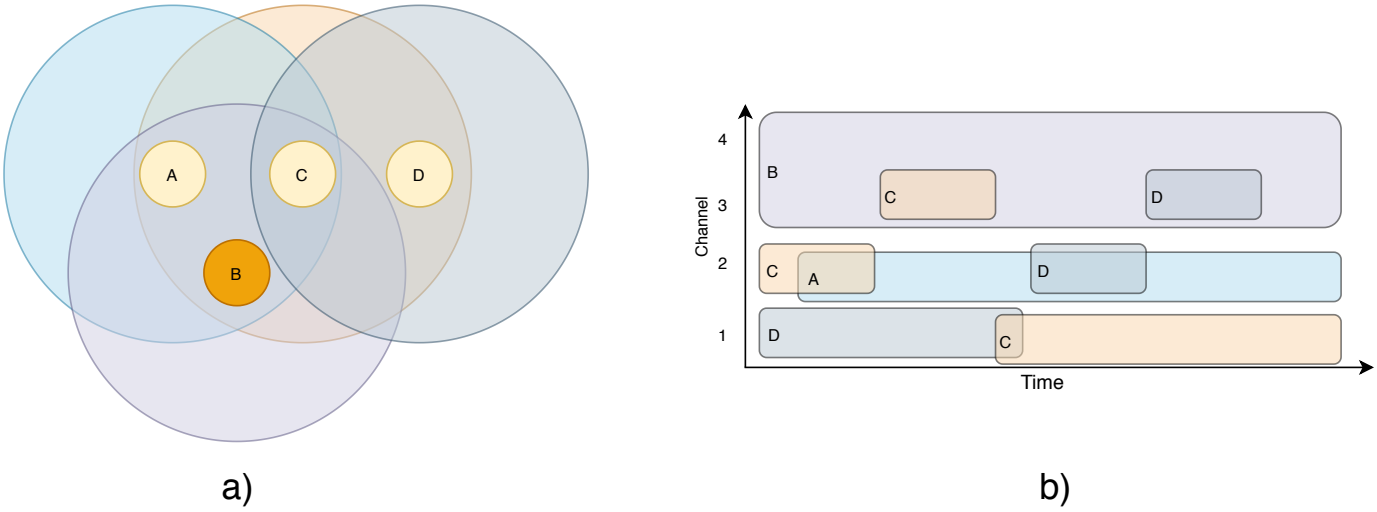

Figure 3: Dispute over frequency channel allocation over time in IEEE 802.11 access points

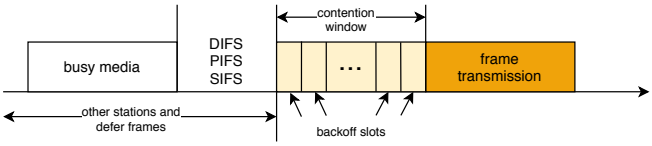

Figure 4: Selfish CSMA/CA contention times

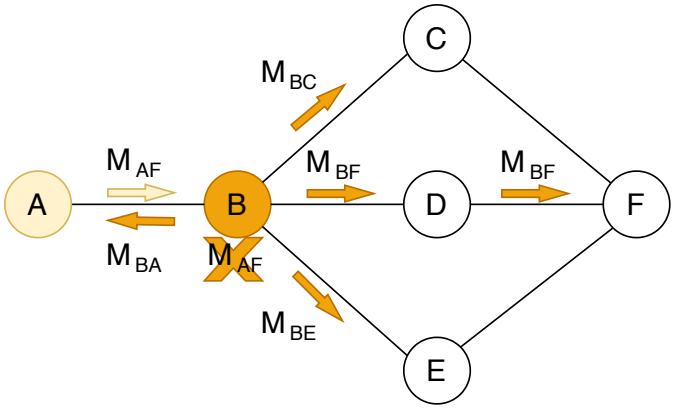

Figure 5: Free-riding behavior in node B

universities, companies, and government offices. In such situations, network devices are configured by the same authority and do not present the free-riding behavior in data forwarding and routing protocols. Similarly, in networks for military or rescue operations, nodes cooperate for the critical purpose of the network because they are generally under the control of a single authority, even when composed of devices of different owners. Categorically, owners of devices concede authority for central coordinators that operate the network to manage devices for a common goal, so that conflicts of interest related to the property of resources cease. Thus, ownership, instead of authority, is the determining factor for selfish behavior.

2.4. MANETs prone to free-riding

This work focuses on blockchain solutions that could found incentive mechanisms to expand and support multi-hop MANETs. The systems of interest cope primarily with the free-riding problem in data forwarding for multi-hop networks complementary to the Internet that could attend underserved areas. Figure 6 illustrates the types of MANETs with routers that are property of different participants and prone to selfish and uncooperative misbehavior: community networks, device-to-device networks, and vehicular networks, including corresponding delay-tolerant variations.

Due to the extensive research on methods for mitigating selfish misbehavior in systems, we outline examples of systems that also have advancements on this issue but are outside of the scope of our study: incentivized overlay and P2P networks; protocols of OSI layers that are not specific for multi-hop networks, such as physical and link layers; network access services such as paid hotspots; crowdsensing systems; data trading systems. This separation is essential to contextualize our focus on incentives for data forwarding discussed in Section 3. Furthermore, Section 4.3 presents a series of works to contextualize how

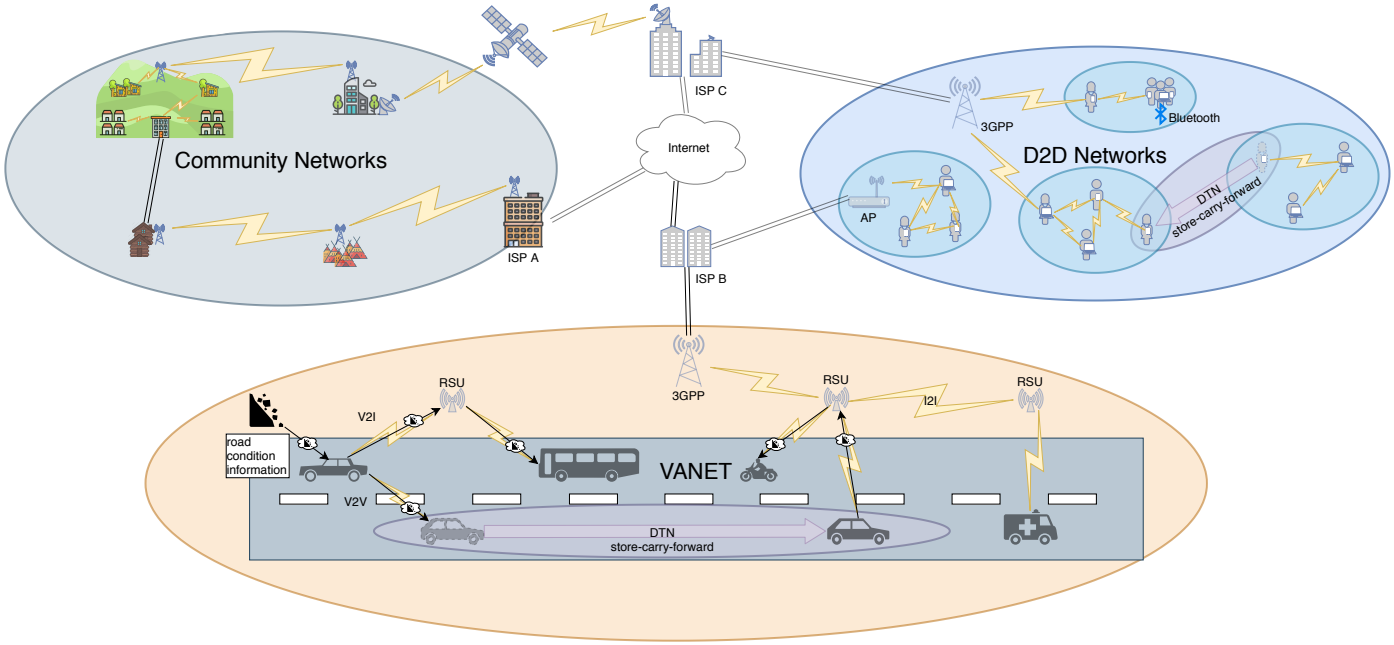

Figure 6: MANETs composed of routers that are property of different participants.

blockchains have been applied for incentives in services other than data forwarding. The following subsections detail the types of networks illustrated in Figure 6, prone to the free-riding problem in data forwarding.

2.4.1. Community networks

Community networks [1, 2, 3] are a type of wireless mesh network [25] that aims to provide last-mile infrastructure for Internet access in underserved or underdeveloped areas. They are typically deployed in areas where market or public policies failed to deliver service, such as rural areas, shantytowns, including indigenous and nomadic populations. Community networks are composed of shared low-cost off-the-shelf routers that form a cooperative multi-hop network that interconnects user devices to an ISP. These networks are more static than typical MANETs and can also adopt wired communication between hops. Compared to other MANETs, trust in community networks is easier to achieve due to more fixed and stable nodes. However, they still are more *ad hoc* than well-established Internet autonomous systems. Additionally, these networks allow deploying local services for communities to save ISP bandwidth and enable more efficient, dependable, and secure services. Many economic sustainability models have been proposed for community networks, including new blockchain-enabled incentive mechanisms.

2.4.2. D2D networks

In contrast to community networks, device-to-device (D2D) networks [26] (or even client wireless mesh networks) [27] are inherently more dynamic and ephemeral than community networks. Routers are personal mobile devices such as notebooks, smartphones, tablets, and other devices with WiFi, Bluetooth, NFC, or other short-range wireless technology. Nodes can join and leave the network using and contributing to the operation of the network while active. Additionally, some devices can share Internet access through 3GPP connectivity or WiFi Access Points (AP). It is harder to establish trust between nodes because the neighborhood is constantly changing, and reputation information becomes obsolete quickly. There is a challenge in managing trust for identifying misbehavior when nodes migrate from one network to another. Routing protocols should address those trust and dynamicity characteristics in their path discovery. It is essential to notice the difference between this category of network from the Internet of Things (IoT). In D2D networks, we address only devices from different owners. The IoT could also comprise whole networks from the same owner (individual or institutional) that do not present conflicts of interest in the network operation. Moreover, D2D networks could serve as infrastructure for IoT devices.

2.4.3. Vehicular ad hoc networks

A vehicular ad hoc network (VANET) [5] is a MANET type that vehicles work as routers that relay data. Usually, they serve for vehicle coordination, traffic information, and road services (emergency, gas stations, restaurants), but they can also provide last-mile Internet access as in other wireless mesh networks. VANETs have specific protocol stacks over radio and infrared technologies [28] that consider mobility patterns and vehicle orientation along roads. Communication is typically classified as V2V (between vehicles) or V2I (between vehicles and infrastructure devices). Roadside units (RSU) are arranged along the road to enable V2I communication. VANETs also present simi-

lar challenges for managing trust as in D2D networks [29]. Flying ad hoc networks (FANET) [30] is a particular case of vehicular network specific for unmanned aerial vehicles (UAV) that present distinct requirements.

2.4.4. Delay-Tolerant Networks

Delay-tolerant networks (DTN) [6] are also known as disruption-tolerant networks or opportunistic networks. The objective of DTNs is to enable communication in MANETs that are constantly partitioned. This type of network follows the *store-carry-forward* paradigm that consists of extending the store-and-forward principle with the physical mobility of devices. Instead of immediately forwarding received data, routers carry data until they find an opportunity to forward them to another router toward the destination. This process increases latency and jitter significantly but enables communication for classes of applications that are not sensitive to such delays.

D2D networks [31] and VANETs [32] can also be designed as DTNs, as illustrated in Figure 6. In the example of the D2D networks, a participant (icon with dashed contour lines) migrates from a D2D network with no Internet connectivity and opportunistically carries data from that network to another D2D network with Internet access through a participant's 3GPP connection. In the VANET example, a car (icon with dashed contour lines) detects a landslide on the road and sends road condition information to a car crossing nearby in the opposite direction using V2V communication. This car is able to opportunistically disseminate this information to other cars directly (V2V) or indirectly (V2I and I2I), distributing it to RSUs alongside the road.

Typical MANETs trust and reputation mechanisms cannot be readily applied to DTNs because behavior monitoring is not straightforward since such deployments are prone to frequent partitions and exhibit high mobility [33]. Moreover, there is a particular class of DTN that merges social awareness in routing decisions [34] [35]. The rationale behind social-aware networks (SAN) is to increase data delivery reliability by trusting devices from owners who have more interaction with other participants or engage in specific communities. Generally, they gather information from social networks to find relations between participants that could serve as metrics for routing decisions.

3. Incentive mechanisms in MANETs

An incentive mechanism can be defined as a system rule whose goal is to induce participants to act in a specific way. Collaboration could be achieved with rewards to stimulate cooperation or punishments to discourage misbehavior. For instance, in a market, a payment could serve as an incentive, working as a reward, whenever a participant offers a service or sells a good, and as a punishment, every time a participant consumes a good or service.

In order to mitigate selfish misbehavior in MANETs, many works have been proposed in an incentive perspective [10, 36, 7]. On the one hand, a trust-based viewpoint relies on past interactions between nodes to establish their trustworthiness, classifying nodes accordingly to their reliability. On the other hand, incentives focus on consequences from cooperative or uncooperative behavior. Some of these mechanisms are classified predominantly as trust management-based by some works [20] and as incentive-based by others [37]. The classification depends on the author's viewpoint. For example, a selfish node marked as untrusted could be incentivized to change its behavior by sanctions such as traffic shaping or isolation. For the sake of clarity, we understand that pre-blockchain incentive mechanisms are a manner of building trust among participants. Additionally, we use the term incentive indistinctly from cooperation enforcement [38].

Incentive mechanisms assume that participants act rationally, from an economic perspective. In fact, there are cases that participants contribute without economic incentives, such as in altruistic and community spirit-driven behavior that motivates volunteering [39]. Those subtler and subjective motivations, such as social status, influence, and affection, are beyond this work scope. We believe that depending on participants' subjective characteristics is not enough for sustaining MANETs because even volunteering requires economic investment for CAPEX and OPEX [40, 41]. In other words, volunteering tends to cease when volunteer resources are scarce or get depleted.

Furthermore, Félegyházi *et al.* [24] indicated that cooperation solely based on nodes' self-interest could exist in theory. Although, their simulation results indicate that, in practice, the conditions of cooperation is unlikely to happen in the absence of incentive mechanisms.

Nevertheless, incentive mechanisms do not necessarily provide strong authentication of entities. Instead, they contribute to identifying the trustworthiness of peers and enforce cooperation using mutual incentives [42].

3.1. Classification of Incentive Mechanisms

There is a large amount of literature on incentive mechanisms for data forwarding in MANETs. Reported mechanisms fall into two categories illustrated in Figure 7: reputation-based and credit-based mechanisms. Most of these mechanisms adopt security protocols schemes with cryptographic tools to punish misbehaved nodes or enforce payment to contributing nodes. Other classifications include game-theoretic approaches that could even result in reputation-based or credit-based mechanisms [43].

Credit-based mechanisms. Credit-based mechanisms, illustrated in Figure 8, model the data-forwarding task as a service that can be valuated and charged. These models incorporate a form of virtual currency to regulate the dealings between the various nodes for data forwarding in multi-hop networks. Virtual currency is used by source

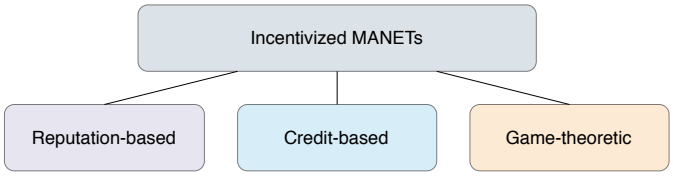

Figure 7: MANET Incentive Mechanisms Classification

and destination nodes to pay forwarder nodes. Also, forwarder nodes are incentivized to relay messages to earn credit because they need credit when they assume the role of source or destination of messages to pay other forwarder nodes. Those mechanisms deploy different distributed algorithms and cryptographic techniques for secure payment and traffic accounting to ensure fair rewards. Two approaches have been widely adopted for secure credit-based mechanisms: tamper-resistant hardware that secures credit accounting with dedicated hardware modules attached to the network interfaces; virtual banks that depend on a trusted third-party service responsible for centralized accounting. SMART [44] is a virtual bank example for DTNs, and FRAME [45] is a tamper-resistant hardware example to incentivized VANETs.

Furthermore, credit-based mechanisms present reciprocity limitation, i.e., a participant credit is bound to its contribution in data forwarding. Consequently, if there is no traffic demand to be forwarded by other participants, a high demanding node cannot acquire enough credits to pay other nodes to forward its data. Some credit-based mechanisms solve this issue by introducing an external currency [46]. Moreover, conventional payment methods for wireless and mobile applications [47] also require trust in third-parties and are not network protocol-aware, such as credit-based incentives solutions.

Bogliolo *et al.* [10] were the first to suggest using blockchains for credit-based incentives in MANETs in order to eliminate the need for trusted third-parties or tamper-resistant hardware. Figure 8 also illustrates a hypothetical incentive mechanism that relies on a blockchain for distributed secure methods for traffic accounting and respective payments. This figure depicts a typical P2P overlay network that distributes blockchain transactions. Blockchain-based approaches are described in Section 5.

Reputation-based mechanisms. Reputation-based mechanisms [20, 21, 22, 23] evaluate the reputation of nodes to forward packets through the most reliable nodes. The reputation of a node increases when it carries out rightly the task of forwarding data sent by its neighbors. Mechanisms in this category measure the reputation of other network nodes and incorporate techniques that isolate or shape traffic of misbehaving nodes, that is, those that show a low reputation value. Likewise, reputation mechanisms can prioritize the traffic of well-behaved nodes. CONFIDANT protocol [20] is an example of a reputation-based mechanism for MANETs. ICARUS [48] is an example of a hybrid incentive mechanism that combines reputation and credit techniques.

A well-known challenge of reputation mechanisms is the second-order free-riding problem [8], i.e., participants who do not spend resources detecting and punishing free-riders. Nodes with such behavior take advantage of other's efforts in reputation management similarly to simple free-riding. Efforts to mitigate higher-order free-riders still present the dilemma in the next order. For instance, a reputation mechanism that prevents up to second-order free-riders still suffers from misbehavior from third-order free-riders.

Furthermore, a series of works also implement reputation mechanisms on top of blockchains to handle misbehavior in MANETs [49, 50, 51, 52, 53]. They adapt existing pre-blockchain mechanisms to store reputation information on-chain to detect malicious misbehavior. However, they are outside of the scope of this survey because they are prone to the second-order free-riding and cannot handle selfish misbehavior efficiently.

Game-theoretic approaches. Game theory [54] models situations in which multiple participants select strategies that have mutual consequences. A game consists of a set of n players, $1, 2, \ldots, n$. Each player i has its own set of strategies S_i. To play the game, each player i chooses a strategy $s_i \in S_i$. Let $s = (s_1, \ldots, s_n)$ denote the vector of strategies selected by the players and $S = S_1 \times S_2 \times \ldots \times S_n$ represents the set of all possible ways in which players can pick strategies. The vector of strategies $s \in S$ selected by players determines the outcome for each player. Suppose a player always achieves a better outcome by using a unique strategy than using other strategies, independent of the strategies the other participants played. In that case, we say that the strategy is the player's dominant strategy. If players select strategies such that no one can unilaterally change its strategy to gain more payoff, we say that the game reaches a Nash equilibrium. The game theory subareas can be classified into cooperative/non-cooperative games, dynamic/static games, repeated/one-interaction games, finite/infinite games, and n-person/two-person games.

Algorithmic game theory design [55] is a subarea of game theory that deals with the design of games. It studies optimization problems where the underlying data is *a priori* unknown to the algorithm designer and must be, implicitly or explicitly, extracted from selfish participants, e.g., via a bid. The high-level goal is to design a protocol, i.e., an incentive or cooperation enforcement mechanism, that interacts with participants so that even selfish non-cooperative behavior yields a desirable outcome. Notably, when truth-telling is the dominant strategy of all participants, we say the mechanism is incentive compatible.

The book *Game Theory in Wireless and Communication Networks* [56] presents a comprehensive compilation of game-theoretic works for multi-hop MANETs, including games to incentivize data forwarding. For example, data forwarding in a non-cooperative MANET can be modeled

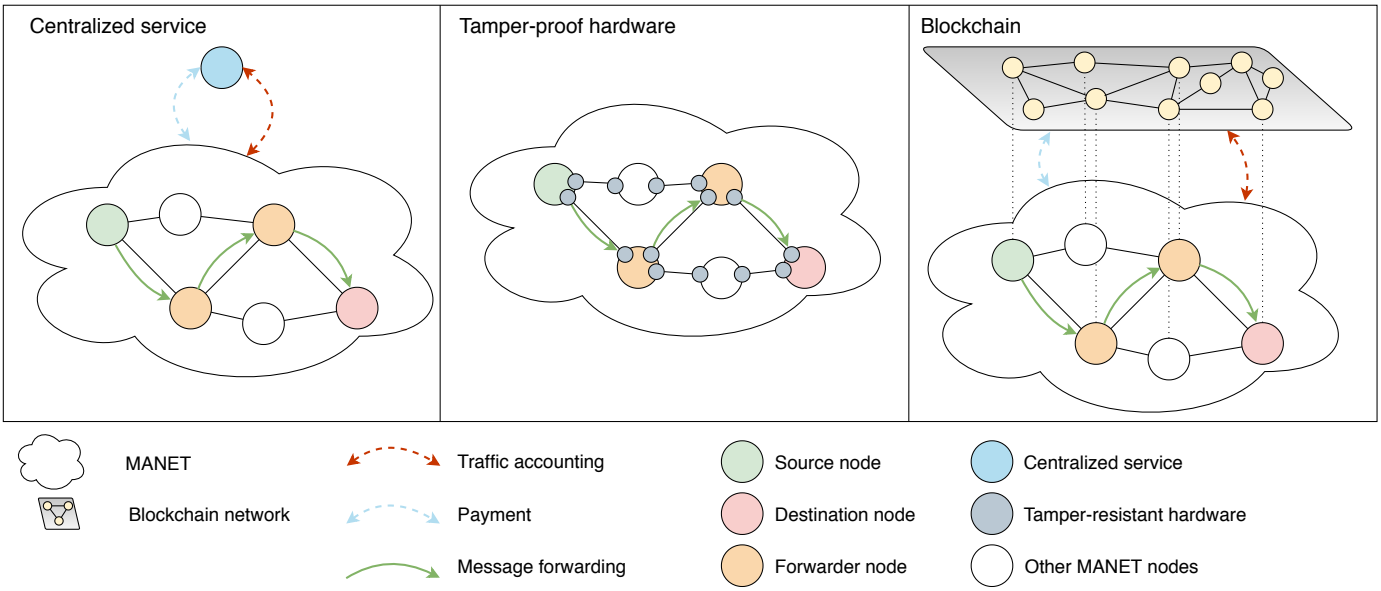

Figure 8: Credit-based incentive mechanisms.

as a repeated-game that consists in the same game repeated over time. Players (nodes) become aware of other players' past behaviors and change their strategies accordingly, allowing reputation evaluation, punishment, and retribution. Han *et al.* [57] model a self-learning repeated-game that each node iteratively adjusts its forwarding probability to avoid being punished by other nodes. DARWIN [58] is another example of a game theory-based reputation mechanism for MANET data forwarding. Stackelberg games involve a hierarchical decision-making process and divide players into *leaders* and *followers*. Leaders are players that hold stronger positions and could impose their strategies upon the others. Followers are limited to react to leaders' strategies. Ileri et al. [59] model a credit-based incentive for multi-hop MANETs as a Stackelberg game in which leaders are Access Points (AP) and followers are devices that forward data toward the AP. Evolutionary game theory (EGT) is a biological-inspired approach that models the evolution of strategies through pairwise interactions between individuals. In EGT, the payoff of a strategy can be interpreted as its fitness, and strategies with higher fitness have more chances to reproduce. Tang *et al.* [60] proposed an EGT game MANETs based on indirect reciprocity and incomplete information.

3.2. Indirect effects of incentivized MANETs

Besides the potential of deploying sustainable networks in areas not covered by conventional services, incentivized MANETs could also minimize nonessential and undesired traffic. For instance, in a credit-based incentive mechanism, mitigation of DDoS from IoT botnets [61] can be achieved allocating credits enough for no more than regular operation of this class of devices. Any attempt to execute a DDoS attack would consume credits and deter it [62, 63]. Similarly, spammers could be hampered, requiring payment for traffic in order to send messages. Furthermore, from an Internet-wide perspective, the addition of credits could also reduce spurious and unwarranted traffic, including malicious traffic [64], that consumes network resources [65, 66].

4. Overview of blockchains

Blockchains are distributed databases organized as sequential chains of blocks that store transactions, as illustrated in Figure 9. The figure exemplifies transactions secured by a Merkle tree in each block. Nodes achieve consensus for new block contents in a trustless approach [9], eliminating the need to trust in third-parties. Once a new block of transactions is appended to the blockchain, it has a very low probability of being invalidated.

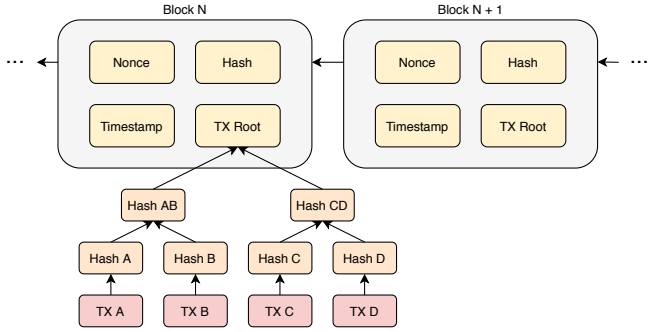

Figure 9: Typical blockchain structure, with transactions (TX) secured by a Merkle tree in each block.

Bitcoin was the pioneer blockchain that proposed a secure and trustless P2P system for payments over the Internet [67]. It secures the most used and valuable cryp-

tocurrency (BTC) today and inspired many other systems for innovations other than financial transactions over the Internet.

Scripts and Smart Contracts. Blockchains such as Bitcoin also allow encoding rules and scripts for processing transactions. This feature evolved to the point that supports programs called smart contracts [68, 69]. The consensus protocol automatically enforces the trusted execution of these programs in a traceable and irreversible way. Ethereum [70], for example, transforms blockchains in finite state machines, which state transitions are equivalent to cryptocurrency transactions, and enable secure and decentralized applications.

Transactions. Each transaction in Bitcoin, say Alice paying Bob 10 BTC, has one or more transaction outputs (TXO), which serve as sums of spendable BTC. These unspent sums are called *unspent transaction outputs* (UTXO). They remain UTXOs until the owner (Bob, for example) redeems them to pay someone else. After that, they are referred to as spent TXOs. In a UTXO based blockchain, there are no accounts or wallets at the protocol layer. Instead, coins are stored as a list of unspent transaction outputs or UTXOs. Transactions are created by consuming existing UTXOs and producing new UTXOs in their place. Rather than following in Bitcoin's principles, smart contract-based blockchains have chosen to employ an account strategy. Instead of having each coin uniquely referenced, coins are represented as a balance within an account. Accounts can either be controlled by a private key or a smart contract.

Consensus. Consensus algorithms are the core of blockchains and serve to establish agreement of the content and ordering of transactions among nodes [71]. Initial systems adopted CPU-bound [67] and memory-bound [72] algorithms known as Proof-of-Work (PoW). In such consensus algorithms, nodes are incentivized to calculate time-consuming challenges based on the data of new transaction blocks. The challenges results are verifiable hashes that chain the previous block with the new one. Nodes that execute such tasks are known as miners and are rewarded with cryptocurrency when they successfully create a new secure block. The reward could be a fee for transactions stored in the new block or even the creation of new cryptocurrency, also called mining. The trustless property comes from the possibility of any node validating the integrity of blocks independently, eliminating the need for prior trust establishment with third-parties. The mining reward is also an incentive for potential attackers to contribute to the reliability of the system instead of using their resources to attack it. In Bitcoin, for example, the condition for trust in the network is that most of the computational power from participants execute honest mining [67].

Permissionless and permissioned blockchains. Blockchain can be classified according to the participation of nodes. Zheng *et al.* [71] taxonomy characterizes blockchains as public when they are permissionless, i.e., they allow any node in the world to participate in the consensus protocol. In opposition, consortium or private blockchains are permissioned, i.e., they require authentication of nodes. Typically, public blockchains present trustless properties, i.e., they do not need to establish trust among nodes to provide dependable properties such as data integrity and availability.

Scalability solutions. Blockchains systems present scalability issues that limit their practical use for many applications: low throughput, that can be expressed in transactions per second (tps) capacity; high financial costs, that involves the amount of cryptocurrency spent in transaction fees; and high storage costs, that relates to the size of the blockchain file. Transaction confirmation time is another issue related to the frequency that new blocks are created. Several works have been proposed to mitigate these limitations [73, 74]. They can be classified as on-chain (layer-1) or off-chain (layer-2) scalability solutions.

On-chain approaches try to change aspects from consensus algorithms to achieve slightly better scalability: MAST [75] allows a Merkle tree to encode mutually exclusive branches in a script reducing the size of a block; in Sharding techniques [76], nodes are grouped forming a shard, and each shard processes different blocks, improving throughput by parallel processing; SegWit [77] is a technique that solves transaction malleability and allows Bitcoin to process 1.7 times to 4 times more transactions; in IOTA [78], there is no block, miner or transaction fee involved, and every node can create transactions freely after solving a specific computational task and choose two previous transactions to validate and approve them if valid; Bitcoin-NG [79] consists in the election of a leader that is allowed to create multiple consecutive blocks, increasing tps.

Off-chain mechanisms are decoupled from the main chain consensus protocol and could achieve high scalability improvements. In Sections 4.1 and 4.2, we highlight off-chain mechanisms for scalability known as channels and childchains that have been explored in many incentivized MANETs systems for data forwarding presented in Section 5.

Furthermore, there are specific scalability solutions in the context of fog and edge computing systems to enable the participation of resource-constrained devices in blockchains. The paper from Xiong *et al.* [80] introduces mobile devices that buy edge computing services for mining tasks, and the equilibrium of reward sharing is achieved using a Stackelberg game. Chen *et al.* [81] formulate an offloading problem in a multi-hop perspective so that intermediate nodes are incentivized to forward mining tasks from mobile devices to edge servers. A similar offloading scheme was proposed [82] for cloud/fog computing using

auction mechanisms. Wu and Ansari [83] described a fog computing system that uses a simplified blockchain with size limited to a fixed number of blocks and a cooperative heuristic algorithm to reduce mining time.

4.1. Micropayment Channels

Blockchain channels have been proposed to enable the secure exchange of transactions among parties outside of the blockchain (named off-chain). These transactions act as an escrow or promissory notes and are settled later on the blockchain. A channel represents the relationship among parties, outside of the blockchain, and can be classified as micropayment channels and state channels. The former represents mechanisms that serve only for cryptocurrency transfer transactions [84, 85], and the latter is a generalization that intends to support state transitions for smart contracts [86]. In this survey, we focus on micropayment channels that can support credit-based incentives.

Micropayment channels exchange transactions, i. e., the altered balance of cryptocurrency. To set up the micropayment channel between two parties, they should establish a 2-of-2 multi-signature address, with each of them holding one of the keys. Multi-signature addresses require signatures of at least n of a total of m participants (e.g., 2 of 2) to complete transactions and are typically implemented using aggregated signatures [87] to minimize overhead.

The creation of a micropayment channel requires a blockchain transaction, called funding transaction, and involves regular transaction times and cryptocurrency fees costs (Figure 10). The funding transaction represents the deposit of an amount of cryptocurrency in the multi-signature address of the channel. In this case, the funding transaction sets the maximum amount that can be transmitted on this channel.

Parties exchange signed transactions, called commitment transactions, that alter the initial balance value (Figure 10). These transactions are valid transactions in that they could be submitted for settlement by either party but instead are held off-chain by each party pending the channel closure. Off-chain transactions enable minimal costs and delays. The settlement transaction represents the final state of the channel and is settled on the blockchain by any of the parties (Figure 10).

In the end, only two transactions are recorded on the blockchain: the funding transaction that established the channel and a settlement transaction that allocated the final balance correctly between the participants. The settlement transaction must be signed among parties (for example, multi-signature 2-of-2 address). The end of the channel can be cooperatively agreed or closed unilaterally by broadcasting a commitment transaction on the blockchain.

Micropayment channel operation. Figure 10 illustrates a simplified version of Bitcoin Lightning [88] micropayments with two participants. Alice and Bob establish a micropayment channel with an escrow that holds 4 Bitcoin from each party while the channel is active. Thus, transactions are limited to a value up to the escrow. The first transaction setups the channel on-chain. The following transactions are exchanged between Alice and Bob and held off-chain. Each commitment transaction represents an agreement for a new balance. Even though the figure shows each commitment transaction with the signatures of both parties, each party actually needs to keep the transaction off-chain only with the other's party signature. Each party adds its signature in the commitment transaction only to send the transaction on-chain. Once the commitment transaction goes on-chain, the balance cannot be repudiated because it has signatures from both parties. For example, in commitment transaction 1, Alice pays 1 Bitcoin to Bob sending a new signed balance of 3 to Alice and 5 to Bob. Bob does not need to sign and send the commitment transaction back to Alice because it is only in Bob's interest to maintain the new transaction that gives him 1 Bitcoin more. If Alice tries to cheat, Bob can sign the received commitment transaction signed by Alice and send it on-chain to redeem the balance. The correct finalization of the channel should use an on-chain settlement transaction that must be signed by both parties to redeem the balance.

There are many problems to maintain micropayment channels correct operation. If one party disappears before establishing at least one commitment transaction, the other party will lose the funds, since there is no commitment performed. Besides, if one party broadcasts a commitment transaction in his/her favor, the other party could be wrongly paid for a service provided. For example, suppose one malicious party should pay a value of 6 Bitcoins to the other party for the whole service provided for 30 minutes. In that case, he/she could try to broadcast a commitment transaction created in the first 15 minutes and try to pay only 3 Bitcoins. Several strategies, not detailed here, are used to prevent these malicious behaviors in micropayment channels [88]: time-locks, revocation keys, and Hashed Time Lock Contracts (HTLC).

4.2. Childchains

Childchains are an off-chain mechanism that builds a hierarchical tree of blockchains with a parent-child relationship, as illustrated in Figure 11. Transactions are processed within childchains faster than consensus used in the main chain, enabling more transactions per second.

Sidechains. At the higher level, a childchain operates similarly to a sidechain [89]. A sidechain is a blockchain with its own independently secured consensus algorithm and is pegged to another blockchain. Value can be transferred from one blockchain to another by relaying simple payment verification (SPV) [67] proofs. An SVP proof allows us to verify that an event in blockchain A has indeed occurred in blockchain B. The purpose of sidechains is to add new functionalities, improve privacy, and secure conventional blockchains.

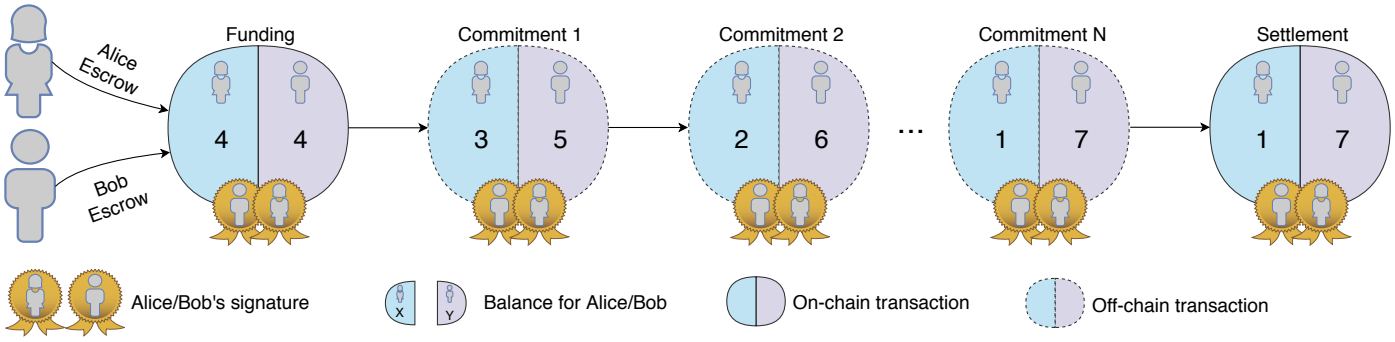

Figure 10: Micropayments channel: funding, commitment and settlement transactions

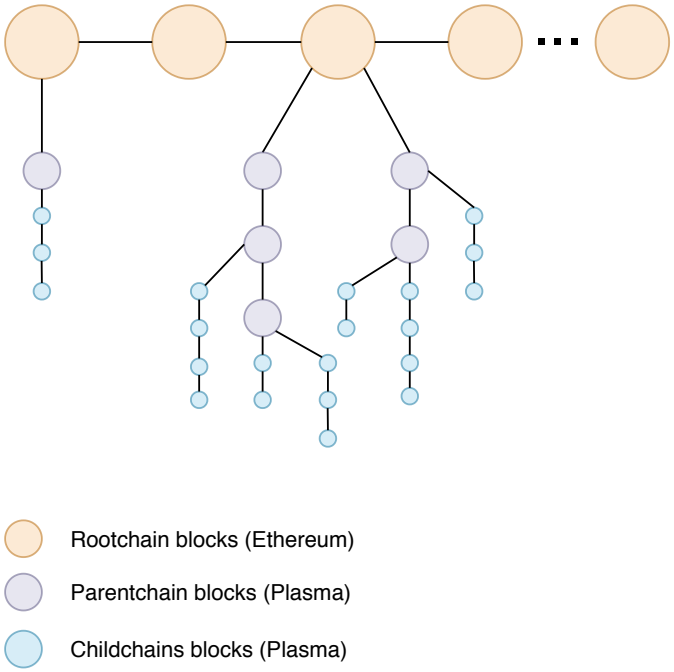

Figure 11: Childchain tree hierarchy

Plasma. An example of childchain can be found in Ethereum Plasma [90]. The first Plasma describes a mechanism that enables connecting blockchains to a base blockchain, often referred to as the *rootchain* or the *mainchain*. Disputes that happen due to fraud in the leaves are escalated to parentchains towards the mainchain. Thus, the mainchain acts as the final arbitrator in the case of unresolved disputes. In this system, childchains are funded in the mainchain (Figure 11), and for each of them, a smart contract locks a cryptocurrency deposit pegged with tokens valid in the new childchains. These childchains can create other childchains, becoming parent chains.

The created childchains behave like ordinary blockchains, and the proofs of the transactions processed there are stored in the parentchains with Merkle root hashes of the plasma blocks. The responsible for inserting the hashes in parentchains is known as the *operator*. The operator could be a random node chosen by an agreement protocol such as Proof-of-Stake or just a centralized node. Authors argue that Plasma hierarchic structure can be used not only for payments but also for computation of smart contracts through MapReduce operations. Furthermore, several variations of Plasma have been proposed [91] [92], using different data models, though all of them still present significant unresolved issues for safety or liveness. Most issues are related to the management of fraudulent users or operators, and require onerous monitoring and challenge mechanisms.

4.3. Blockchain-incentivized services

Besides data forwarding for communication purposes, blockchain features have been investigated to encourage cooperative support for a variety of other services. Before presenting data forwarding incentives in Section 5, we outline here a series of works that propose blockchain-enabled incentives for other services. Incentives adopted by those works could present common characteristics with the state-of-the-art that deserve to be investigated in the future.

Useful mining. PoW consensus algorithms use resource-intensive tasks as challenges that should be solved by

independent participants to receive financial compensation. Despite scalability concerns, PoW consensus algorithms still efficiently support cryptocurrencies with financially incentivized volunteers and without the need for trusted third-parties. Nevertheless, some efforts [93] proposed to combine useful calculations in resource-intensive PoW challenges. Miners that solve those challenges implicitly provide a service and are rewarded similarly to traditional PoW. Preliminary groundwork has been proposed in: Primecoin [94], which calculates prime numbers using Cunningan chains; NooShare [95], that executes Monte Carlo simulations; Proof-of-eXercise [96], which solves matrices for scientific problems.

Data storage. Alternatives have been proposed to provide blockchain-incentivized distributed storage services [97]. For example, Permacoin [98] and Retricoin [99] have consensus algorithms that reward nodes that contribute with storage space using *Proofs-of-Retrievability* (PoR). Filecoin is a blockchain-based digital payment system, which supports digital storage and data retrieval for IPFS users [100]. It proposes the *Expected Consensus*, which includes *Proofs-of-Replication* (PoRep) and *Proofs-of-Space-Time* (PoSt) from nodes that store users' data. In each round of the consensus process, those proofs produce data that randomly chooses a node that defines the next block of the blockchain.

Data trading. Data trading platforms [101] facilitate the exchange of datasets, bridging sellers and buyers. Upon receiving the buyer's payment, the data exchange platform will transmit the purchased data to the buyer and pay the seller (after deducting the management fees or commission). Chen *et al.* [102] proposed a blockchain-based data trading framework for IoV that implements a double auction mechanism to achieve the desired economic benefit and protect the privacy of buyers and sellers. Dai *et al.* [103] also propose a data trading platform where both data exchange and buyers cannot obtain access to the seller's raw data, i.e., they get access only to the data analysis findings.

Energy trading. Advances in renewable energy such as solar panels and wind turbines enabled energy production in end-consumers, often called *prosumers*, that can sell surplus energy. In this context, blockchains can coordinate local energy markets and incentivize the participation of prosumers [104, 105]. Also, *energy coins* have been proposed in PETCON [106] and BEST [107] for energy trading transactions among electric vehicles and microgrids in blockchain consortiums.

Cloud/fog and edge computing. Many works have been proposed in the context of cloud/fog and edge computing to rent unused processing capacity and to offload tasks from resourced-constrained devices. The work from Taghavi *et al.* [108] present a collaborative federation of cloud providers that trade processing capacity among them and deploy a blockchain-based monitoring to detect service level agreement violations. Xiong *et al.* [80] conceive resource-constrained mobile devices that buy processing capacity from edge servers for mining tasks and the equilibrium of reward sharing is achieved using a Stackelberg game. A similar scheme was proposed for cloud/fog computing using auction mechanisms [82]. Liu et al. [109] proposed rewards for mobile edge computing nodes that perform transcoding jobs in distributed video streaming services. Lin *et al.* [110] designed a permissioned blockchain system for secure offloading of bilinear pairings from IoT nodes to edge servers.

5. Blockchain Incentivized Data Forwarding in MANETs

MANETs are also starting to adopt cryptocurrencies to improve network connectivity trust without the need for trust in third-parties (trustless). Blockchain features are suitable for scenarios that trust is difficult to establish or maintain, such as multi-hop MANETs with routers that are property of different participants. In Section 3.1, we outlined conventional reputation-based, credit-based, and game theory-based incentive mechanisms for cooperation in multi-hop MANETs and their limitations. In Section 4, we presented an overview of blockchain concepts, highlighting those more relevant for blockchain-incentivized services. This section is organized as follows: first, we discuss blockchain features that are specifically useful for incentives in multi-hop MANETs; finally, we present the state-of-the-art key points, including research papers, products, and patents. Even though we found many other works that combine blockchains with MANETs, we excluded those works that do not relate to reward incentive mechanisms for data forwarding and, thus, are outside of the scope of this survey.

A series of blockchain features and concepts are useful to incentivize data forwarding in multi-hop MANETs. For instance, the elimination of trusted third-parties could enable decentralized and trustless MANET infrastructure. Unlike the Internet, where autonomous systems (AS) usually have the bureaucratic and legal framework to establish long-standing trust between them, MANETs are formed by participant's infrastructure with more loose and short-lived relationships. In this context, blockchains allow participating in MANETs without the need for trust in authorities that could abuse of information asymmetry to take economic and political advantages [111].

Credit-based incentives and blockchain. Most works in the state-of-the-art are similar to credit-based incentives such as those shown in Section 3.1 that cope with the free-riding problem. Typically, credit-based incentives are limited by reciprocity, i.e., a participant cannot use network services beyond its contribution. This limitation does not exist

with financially incentivized MANETs with cryptocurrencies. Any participant can use network services, given that they have enough cryptocurrency to pay for it. Additionally, secure blockchain payment methods can eliminate or reduce the need for full trust in third-parties and tamper-resistant hardware used by previous credit-based approaches (Figure 8). Actually, trustless payment confirmation is trivial with blockchain-based cryptocurrencies.

Blockchain systems adopted. Table 1 classifies the state-of-the-art accordingly to the blockchain adopted in incentive mechanisms: Bitcoin, Ethereum, or Other. Part of the Ethereum based systems, instead of using ether (Ethereum coin), implement their ERC-20 tokens [113, 119, 121, 126]. ERC-20 [127] is a protocol standard that defines smart contract rules for issuing tokens on Ethereum. Moreover, as shown in Table 2, public blockchains based on Proof-of-Work present performance for transactions per second, transaction fees, and ledger size requirements that are challenging for MANET devices and their incentive mechanisms. For example, transaction fees could be prohibitive for community networks that intend to provide affordable connectivity. Besides, full ledger file size requirements are unfeasible for resource-constrained personal mobile devices. Permissioned blockchains, adopted by some systems [125, 128], allow better performance, though they are not trustless.

Channels and childchains. Due to scalability limitations (Section 4) to confirm on-chain transactions, many MANET systems adopted off-chain mechanisms, such as channels and childchains, to enable faster and cheaper transactions. Table 3 classifies the state-of-the-art in on-chain or off-chain mechanisms. Micropayments channels (Section 4.1) have been widely applied in incentivized MANETs for implementing ideas similar to conventional escrows and checks. For instance, establishing a channel needs an escrow that the parties should deposit as collateral for transactions. Likewise, micropayments can be compared as checks, because the transaction information is kept off-chain by the parties until settlement in the main chain. Childchains (Section 4.2) have a few proposals for payments in incentivized MANETS but no public implementation yet. For instance, AMMBR [116] proposes using childchains in which members are nodes within a local MANET to enable faster transactions.

Smart contracts. Both channels and childchains are deployed over smart contracts (or simplified scripting, such as in Bitcoin). Furthermore, there are other subsystems implemented in smart contracts to support incentivized MANETs. For instance, MeshDapp [125] deploys smart contracts to estimate demand and supply of network forwarding services, and define prices based on estimations. Another example is Althea [113] that implements subnetworking addressing and management over smart contracts.

State-of-the-art. In the next subsections, we present blockchain-enabled data forwarding incentive mechanisms for multi-hop MANETs found in research papers, patents, and products. We outline the key points of each work and classify them according to blockchain features that they adopt in their incentive mechanism.

5.1. Kadupul

Kadupul [115] is a system that aims to incentivize data forwarding in low-latency links for D2D DTNs. Nodes create alternative local routes to allow low-latency communication, avoiding using slow or unreliable ISP's uplinks. The forwarding with low latency is incentivized with Bitcoin time-locked puzzles [129].

Time-locked puzzles are mechanisms that hide information in the blockchain for a specific time or until certain conditions are satisfied. Bitcoin's time-locked puzzle implementation allows us to retain a reward until one of three conditions is met: until a specific time passes; until a node solves the puzzle; or until the solution is revealed. Kadupul incentivizes nodes to forward data as soon as possible so they can receive a key to decrypt the time-locked puzzle and reward the forwarding nodes. Kadupul is routing protocol agnostic and suggests using P2P neighbor discovery protocols to determine the forwarding path. The authors propose five time-locked puzzle strategies from which we highlight three: double incentive, all or nothing, and contract forwarding. Kadupul involves high overhead setting up puzzles and has no implementations for any strategy.

The *double incentive* forwarding makes the forwarders lose their reward unless they forward the data intact to the next-hop as soon as possible and creates an incentive for assisting other forwarders. The sender must negotiate the forwarding fees with forwarders. It then generates and makes public a chain of rewards using time-locked encryption. The next step distributes the time-locked puzzle secrets and nonces to all forwarding nodes in the path. Each forwarder n keeps the nonce, and each node $n+1$ keeps the secret. When the node $n+1$ receives the data, it sends back an acknowledgment to the forwarder n containing the respective secret needed to receive the payment.

The *all or nothing* strategy pays the reward to all nodes only after the data is delivered to the destination. Instead of distributing secrets in advance, the final receiver acknowledges the data delivery to the sender, and the sender then unlocks the puzzles for all the forwarders. This scheme requires more coordination between senders and receivers but makes it difficult for the forwarders to collude maliciously. It also increases the forwarding risk as none of the nodes will receive their reward if the packet is lost or delayed along the way.

The *Contract forwarding* works without prior establishment of the forwarding path as the two previous strategies. The sender negotiates a forwarding contract with another node to bring the data to the recipient. It is then up to the node that accepted the forwarding contract to deliver the data as fast as possible. This node may use any number

Table 1: Blockchain Incentivized MANET Systems

Bitcoin	Ethereum	Other/Undefined
RouteBazzar [112]	Althea [113]	Routing Based Blockchain [114]
Kadupul [115]	AMMBR [116]	Skywire [117]
LOT49 [118]	Rightmesh [119]	
Post-disaster DTN [120]	Blockmesh [121]	
VDTN – RSU-to-RSU [122]	VDTN – RSU-to-vehicle [123]	
Truthful Incentive [124]	MeshDapp [125]	
	Smartmesh [126]	

Table 2: Public Proof-of-Work blockchain performance

	Bitcoin	Ethereum
Transaction time (s)	600	30
Price per transaction (US$)	1.00	0.10
Full ledger size	270GB	350GB

of subcontractors for the packet until the path reaches its final destination.

5.2. Truthful Incentive

He *et al.* [124] proposed a credit-based incentive mechanism for DTNs that uses Bitcoin for secure transactions. Message source nodes pay back intermediate collaborative nodes when they figure out that the messages are successfully delivered to the destination.

Basically, the source node produces two random numbers R1 and R2, where R1 is used to prove that the next-hop node received the data correctly, and R2 is used to prove that the destination got the data successfully. Every hop of the data forwarding involves an on-chain payment commitment from the sender to the receiver at this hop. The first hop receiver forwards the data to the next-hop and uses commutative encryption to validate that it received R1 from the source node and that it received a confirmation ACK from the subsequent hop. Subsequent hops validate their contribution in data forwarding with the ACK sent backward and the ACK received from the next-hop.

The authors provided experimental results to evaluate the overhead of their mechanism, calculating the impact of processing the commutative encryption used in message delivery verification. They also evaluate the bandwidth and storage requirements necessary for piggybacked data introduced in messages and on-chain transactions. Finally, authors simulate: a) the impact of the number of positive cooperative nodes and the playing strategies on the utility of a positive cooperative node; b) the impact of the encounter probability and the playing strategies on the utility of the receiver. Both simulations are calculated with 1 to 10 cooperative nodes and different node collusion configurations.

5.3. RouteBazaar

RouteBazaar [112] uses blockchains to build trust between Internet autonomous systems (AS). Provides ASes with automatic means to form, establish, and verify end-to-end connectivity agreements. Even though RouteBazaar uses BGP, which is not a mesh specific routing protocol, we describe their solution here because it could also be applied in community networks.

In RouteBazaar, a provider is an AS that advertises connectivity over a *pathlet* that describes path fragments with cost and quality of service information (e.g., a pathlet with identifier 0xf48d4c4, from AS234 to AS343, with 5ms of latency and 3Gbps of throughput, and costing $50). A path is formed by composing pathlets leading from a source to a destination. A customer in RouteBazaar is an entity paying for the end-to-end connectivity provided by a path. Agreements are registered in the blockchain and identified by an anonymous tag created by parties.

The forwarding proof for a specific pathlet is also written in the blockchain. It contains an anonymous tag, a hash of a traffic sample (e.g., every 50^{th} packets), a timestamp, and the throughput average since the last traffic sample capture. Clients register payment proof directly in the blockchain too.

The system allows us to estimate the quality of service using the forwarding proofs timestamps. It also allows ISPs to check whether clients are good payers with payment proofs registered in the blockchain. RouteBazaar has no implementations, and the need to write in the blockchain so often would cause considerable overhead.

5.4. Post-disaster DTN

Chakrabarti and Basu's [120] work is a D2D DTN for post-disaster communication that uses Bitcoin to incentivize data forwarding. In their proposed scheme, the entire disaster-affected area is virtually divided into several non-intersecting zones, consisting of several shelters.

The network architecture is composed of four types of nodes: shelter-nodes for the disaster area shelters that generate situational messages and broadcasts them to the forwarder-nodes; control-nodes that represents the emergency operation centers of disaster areas where situational information from remote shelters are collected, and the rewards are distributed; forwarder-nodes from volunteers that carry smartphones and move around the disas-

Table 3: On-chain and Off-chain Blockchain Incentivized MANETs

On-chain	Off-chain		Unknown/Not applicable
Kadupul [115]	Micropayment channels	Childchains	Routing Based Blockchain [114]
RouteBazaar [112]	Althea [113]	AMMBR [116]	Blockmesh [121]
MeshDapp [125]	LOT49 [118]		Skywire [117]
Post-disaster DTN-[120]	Rightmesh [119]		
VDTN – RSU-to-RSU [122]	Smartmesh [126]		
VDTN – RSY-to-vehicle [123]			
Truthful Incentive [124]			

ter area opportunistically collecting and forwarding situational messages towards the control-node; observer-nodes that collect reward transactions generated by forwarder nodes and send them to the Bitcoin network. Forwarder-nodes are assumed not to have Internet connectivity in the disaster area and depend on observer-nodes to send on-chain transactions.

A shelter-node belonging to a particular zone sends a message to the control-node through one or more forwarder-nodes and gives an equal amount of Bitcoin incentive to all cooperative forwarder-nodes that help in forwarding the message and a fixed amount α for the observer-node. Additionally, every intermediate forwarder-node pays a certain amount of incentive to the next-hop forwarder and collects a digitally signed acknowledgment from the next-hop forwarder to which it forwards the message as a sign of cooperation. A forwarder-node is considered cooperative if and only if it has a digitally signed acknowledgment from its successor. It is to be noted that every reward is actually a commitment, and incentives could be redeemed by the forwarder-nodes only after the shelter-node comprehends that the message is successfully delivered to the control-node. This mechanism prevents the forwarder-nodes from indulging in dine and dash behavior.

5.5. VDTN – RSU-to-RSU

Two works proposed on-chain incentive mechanisms for VDTNs (VANET DTNs – Sections 2.4.3 and 2.4.4). Both works aim to incentivize disseminating alerts and advertisements for vehicles on roads with insufficient network coverage. These proposals limit multi-hop data forwarding to two hops. The first hop between the message source S and an incentivized vehicle V_c responsible for the store-carry-forward. The second hop between the vehicle V_c and the message destination D. Both systems also deal with privacy issues due to sensitive location history of vehicles.

Park *et al.* [122] propose a Bitcoin-based incentive mechanism for communication from a source RSU_s to a destination RSU_d opportunistically through a vehicle V_c in a strategy similar to Kadupul [115]. The goal is to enable traffic information produced in the area of RSU_s to be sent to RSU_d that, in turn, disseminate that information to vehicles crossing RSU_d. Each vehicle V_c and RSU participate in the Bitcoin network and have their keys issued by a trusted authority in the system called *Service Manager*. These keys generate Bitcoin addresses that enable RSUs to pay vehicles when messages are forwarded. The incentive is done through a multi-signature Bitcoin transaction that requires signatures from both RSU_s and RSU_d. When RSU_s creates the message and sends it to V_c it signs a payment transaction that will be time-locked until RSU_d signs it. Also, V_c's reward is time-locked, i.e., is if V_c does not forward the message to RSU_d or not redeem its payment until a deadline, then RSU_s can withdraw the payment.

5.6. VDTN – RSU-to-vehicle

Distinctly from Park et al approach (Section 5.5), which destination of the incentivized forwarding is an RSU that further disseminates messages locally, Li *et al.* [123] strategy incentivizes vehicles to opportunistically forward data to the final destination vehicles. Moreover, they use Ethereum cryptocurrency for incentives instead of Bitcoin. In their proposal, an advertiser A delegates to an RSU the task of distributing a message M to V_c vehicles crossing RSU's area. Those vehicles are incentivized to opportunistically forward data to other vehicles out of the RSU range. The number of vehicles that message M can reach depends on the reward for each successful delivery and the total deposit placed on-chain by A. An Ethereum smart contract secures the time-locked deposit and the reward management. Anonymous tokens serve as receipts to secure against repudiation attacks from malicious advertisers that could refuse to pay. Privacy is achieved using vehicle's blind signatures. Similarly to Park et al [122] proposal, this work also has a trusted authority responsible for key generation and management called *Register authority*. V2V and V2I communication among vehicles and nearby RSUs are achieved with the DSRC protocol. The authors performed simulations in VANETSim to evaluate the off-chain computational costs. They also evaluated the performance of transactions using a Proof-of-Authority (PoA) private blockchain with Parity Ethereum.

5.7. Althea

Althea [113] aims to incentivize communities to deploy last-mile connectivity to the ISP. It uses the Babel protocol [130] to determine the routes of infrastructured mesh networks. The routing protocol also incorporates price metrics that consider how much each router owner wants

to receive as payment for data forwarded and mechanisms to verify announced metrics. Thus, routes are determined according to traditional cost metrics and the proposed price metrics. The weight of price metrics is adjustable so that users can define their link preference between price and quality.

The forwarding incentive scheme relies on payment for forwarded data using micropayment channels. The current version of Althea uses the Ethereum blockchain with a low-overhead micropayment channel mechanism called Guac [131]. Each node that wants to have data forwarded establishes Guac micropayment channels and VPN tunnels with its neighbors for payment. VPN tunnels serve as an accounting mechanism to control data delivery with neighbors. Moreover, nodes pay neighbors only after their data is forwarded, and forwarders can block or shape the traffic of bad payers. VPN accounting also serves as a reputation mechanism to avoid nodes that provide low-quality service. Additionally, Althea nodes also create VPN tunnels with exit nodes (servers that provide access to the Internet), which traffic accounting could serve to audit the traffic accounting from neighbor tunnels.

5.8. Rightmesh

Rightmesh [119] proposes to incentivize D2D DTNs with Ethereum micropayments. It has an Android API to build applications using a proprietary protocol stack that operates over Bluetooth and WiFi technology.

Data forwarding is incentivized using μRaiden [132] micropayment channels with their ERC-20 tokens (RMESH). In Rightmesh's viewpoint, establishing pairwise micropayment channels between neighbors would be very sensitive due to frequent changes in topology in MANETs. Thus, off-chain payments are intermediated by proxy nodes called *superpeers* located in cloud service providers and have stable access to the Internet and the Ethereum network. Also, superpeers intermediate traffic to enable accounting and, consequently, should be trusted by MANET nodes. Micropayments commitment transactions are piggybacked in data packets and acknowledge packets so that nodes could forward them toward superpeers with guarantees of payment upon delivery.

Rightmesh identifies devices using their Ethereum public address both for routing and payment. Its routing protocol is based on hop count metric and peer-defined prices for packet forwarding propagated through a discovery protocol to all nearby nodes. Rightmesh discovery protocol has a mechanism to guarantee that sellers charge the correct prices. Every buyer data packet carries a commitment indicating how much is being paid for the data wanted to be forwarded. If the buyer has not received the updated price yet, the forwarder will drop the packet, waiting for retransmission with the updated price. Additionally, buyers define the maximum price they are willing to pay in route selection.

5.9. LOT49

LOT49 [118] proposes D2D networks incentivized with Bitcoin payments using the Lightning Protocol for channel micropayments. They also propose a new scheme for aggregated signatures [133] [87] in micropayment channels to minimize the incentive protocol overhead and increase the bandwidth available for data delivery. A prototype was evaluated using the AODV routing protocol [134] to estimate the delivery ratio with different node densities.

If a source node wants to send data to a destination node through a multi-hop path, then every node in the path should have a micropayment channel established with its next-hop. Sending data requires an off-chain commitment transaction with a reward from the source node to the next-hop that can only be completed with a receipt from the destination node. Every next-hop should make another commitment transaction with its next-hop, under the same delivery conditions, to complete the data forwarding. Each node in the path reduces the reward for the next forwarder. The difference represents the value they earn for forwarding the data.

Once the data has been delivered, the destination node transmits back a payment receipt with a secret value that has been encrypted in the message delivered. The forwarder nodes use this payment receipt to update the state of their payment channels with each other. Any node that receives the secret can settle their update transaction on-chain even if their channel partner disappears or becomes uncooperative. Nodes can observe transactions settled by other relay nodes involved with the same message delivery to learn the secret they need to settle their channel updates.

When a payment channel does not already exist between two nodes, it must be set up and funded. A transaction that funds a new channel cannot be confirmed locally between mesh nodes because it involves a payment that could have been committed to funding a different channel. Thus, these transactions must be confirmed directly by the Bitcoin network to be considered reliable. However, staying synchronized with the state of the blockchain is impractical over a low bandwidth network. Thus, LOT49 defines a witness node that is persistently connected to the Internet, such as a gateway. The witness node monitors and reports the current state of transactions of interest to nodes within the mesh.

5.10. AMMBR

Like Althea, AMMBR [128] aims to disseminate the Internet with blockchain incentivized community networks in the last mile to the ISP. AMMBR supports the mesh routing protocol BATMAN-Adv [135] and proposes the development of a new one based on BMX7 [136]. AMMBR launched its cryptocurrency (AMR) and designed its router hardware. The proposed router is modular and extensible, supporting modules for blockchain mining, multiple radio technologies, and IoT-related features.

In their first white paper [128], they proposed a payment method for the forwarding services directly in the blockchain using dedicated hardware that combines Proof-of-Elapsed-Time [137] with a new algorithm called Proof-of-Velocity (PoV). The authors described PoV as a variation of Proof-of-Work with memory-hard [72] characteristics and designed to be calculated efficiently with proprietary silicon-germanium ASICs with a clock above 20GHz. In the second white paper [116], AMMBR omits discussions about PoV and proposes using Plasma child-chains [90] to enable feasible consensus between routers within local wireless meshes as a means to enable payments between routers.

5.11. Routing Based Blockchain

Trautmann and Burnell's patent [114] describes a system that introduces a Proof-of-Routing scheme that can securely implement a blockchain network and provide useful consensus. Their blockchain-based router idea includes different nodes that process data packets between endpoints. Nodes can include router nodes, which analyze and route data packets, and block nodes that manage collections of specially labeled packets and generate new blocks in the blockchain.

When a router node receives a packet, it signs the packet using a signature aggregation scheme. The router then evaluates the packet to determine whether it is a *root packet*. Root packets satisfy predetermined criteria (e.g., a hash from the packet that is smaller than a given number, similarly to PoW schemes). The root packet criteria ensure that only a small amount of the packets in a given network are root packets. If a packet node is identified, a copy of that packet is forwarded to a block node.

Block nodes collect root packets from one or more router nodes and combine them to produce new blockchain blocks. The block should satisfy criteria such as: a) collect at least 1000 root packets; and b) each root packet must have been signed and routed by 100 different routers.

If a block node successfully discovers a group of root packets that allows it to generate the next block in the blockchain, that block node and any routers contributing to that group of root packets is issued cryptocurrency. Upstream or downstream routers from a root packet at a given router are also issued cryptocurrency for handling the packet. This mechanism incentivizes data packets to be signed and forwarded to their respective destinations and stimulates router nodes to not adhere to free-riding behavior.

5.12. MeshDapp

MeshDapp [125, 138] focuses on balancing mesh network service costs (CAPEX and OPEX) and respective payments to enable sustainable network infrastructure. Their approach uses Ethereum smart contracts to automate fair accounting and money transfers for the network service provided.

The authors compare the networking service to an electricity market, assuming the need for a *mediator* that finds the optimal retail service prices and optimal connectivity allocation to balance the infrastructure. In their analogy, they compare the kWh unit from electricity with the MBh from forwarding services. They also assume that forwarding demand is close to supply. Each mesh network is called a mesh island with its own local Ethereum Proof-of-Authority (PoA) consensus [139]. Each mesh island's mediator executes over smart contracts fed by a monitoring system that accounts network traffic. This accounting should be reliable to serve as criteria to estimate demand and supply and define prices. Although, the authors do not describe how to ensure accounting reliability of the monitoring system. Additionally, preliminary works provided experimental results for PoA consensus feasibility in wireless mesh networks [140].

5.13. Other systems

Here we show systems that advertise themselves as incentivized meshes but do not provide minimal public documentation about incentive mechanisms. Like other examples, all of them have a cryptocurrency associated.

Blockmesh. Blockmesh [121] aims to introduce their ERC-20 token (BMH) to serve as reward for the network supporters to incentivize the deployment of community networks in underdeveloped and disaster areas. It inherits a mesh network protocol called Mesh Datagram Protocol (MDP) [141] from the Serval Project [142]. In this protocol, host identifiers are ECDH keys that serve to cipher, sign, and validate transmitted packets. Blockmesh also proposes dedicated hardware called Mesh Extender (MeshEx), which serves as an access point and integrates with the mesh network and blockchain. Blockmesh is limited to a few applications that execute over MDP protocol and currently comprise messaging, voice calls, and file transfer. Additionally, MDP is a network protocol that does not provide ordering and confirmation.

Smartmesh. Smartmesh [126] proposal is similar to Rightmesh using its ERC-20 token (SMT). They advertise that their system incentives will operate with off-chain transactions using Raiden [85] micropayment channels and Plasma. Documentation also mentions a Smartmesh Raiden extension that enables high speed and secure payment. Moreover, they intend to deploy Android and iOS mobile devices as MANET routers. Those devices are expected to run Light Ethereum Subprotocol (LES) [143] that do not need to keep a full blockchain file.

Skywire. Skywire [117] is the blockchain incentivized network proposed to be part of a blockchain system called Skycoin. The system aims to develop a smart contract language called CX, a blockchain structure called Fiber, and a consensus algorithm called Obelisk. They advertise that

Skywire will become an alternative to conventional connectivity to the Internet to circumvent censorship and vigilance and prevent ISP monopolies. The promoted strategy to achieve such goals is to disseminate the infrastructure of community networks with mesh routers called Skyminers that are incentivized to operate the network receiving Skycoin as a reward. However, since their first announcement, there is no specification or public code describing how consensus protocols, routing algorithms, and incentive mechanisms will work.

6. Strategies and Challenges

In the previous section, we outlined key points of the state-of-the-art and blockchain features that could be readily be applied to their forwarding incentive mechanisms. This section analyzes and compares strategies from the works in the state-of-the-art, their advantages, limitations, and challenges. Figure 12 classifies the state-of-the-art works designed to specific MANETs, including DTN alternatives, as shown in Section 2.3.

Figure 13 illustrates the discussion of this section with an example of a tree-based routing protocol that forms a loop-free connectivity tree among nodes within a MANET. In this example, node S has a routing path with node D to transmit data. Routing protocols could use a series of metrics to define routes. For instance, latency, bandwidth, jitter, expected transmission ratio (ETX), and data transfer prices. In an incentivized MANET, forwarder nodes, such as F_1 and F_2, should have a method to prove that they forwarded data. A MANET could also include a malicious node Y that eavesdrops traffic and blockchain accounting information from other nodes.

6.1. Payment and forwarding proofs

Most of the works in the state-of-the-art deal with the free-riding problem similarly to pre-blockchain credit-based incentive mechanisms. In this context, packet forwarding is a service rewarded with cryptocurrency. The method for assuring that a party (e.g., source node S and/or destination node D, in Figure 13) paid and the other party (e.g., forwarding nodes F_1 and F_2, in Figure 13) performed packet forwarding correctly differs from one mechanism to another. We separate the system's components into payment and forwarding proofs to cope with these two problems. However, we understand that some mechanisms unify them, i.e., the same mechanism provides both payment and forwarding proofs.

Payment proofs. Secure payment accounting is an inherent feature of blockchains. In Section 4, we discussed blockchain performance limitations and respective mechanisms that intend to improve scalability. Here we summary strategies from the state-of-the-art that adapt blockchain payment accounting mechanisms to the limitations and requirements specific to incentivized MANETs.

Intermittent and low-bandwidth connectivity can affect MANETs, mainly DTNs. Consequently, devices could stay out of sync with the blockchain for long periods and unable to perform on-chain transactions. Off-chain mechanisms enable transactions to be performed securely between nodes in a MANET, even when the network is partitioned and without Internet connectivity. For instance, a micropayment channel allows payments up to a value equal to the deposit placed in the channel establishment. Each transaction is secure if devices can connect to the blockchain before commitment transaction time-locks expire, to manage potential malicious transactions from other parties (Section 4.1).

Resource-constrained devices in some MANETs (e.g., D2D networks) cannot store full blockchain information. Full blockchain is a requirement for trustless security in public blockchains. An alternative is to adopt proxy-based communication to the blockchain via trusted nodes that have more storage resources [118, 119, 120]. Moreover, both VDTN proposals [122, 123] require a central authority that issues participants' keys implying that participants should trust in third-parties for payments. Both proxy-based and key issuer approaches characterize dependence on trusted third-parties that eliminate the trustless property.

Forwarding proofs. Besides payment proofs, blockchain incentivized MANETs need forwarding proofs that confirm that nodes contributed to data forwarding to enable fair payments and prevent undue billing. This element is interesting for infrastructured networks, such as community networks. However, they can operate similarly to conventional ISPs, i.e., consumers can change their ISP if it is not working according to contracted service when there is available a set of competing neighbors offering networking services, such as in GUIFI.net [144]. Furthermore, this approach is not suitable for more dynamic MANETs with ephemeral connectivity such as VANET and D2D networks. Thus, they need a mechanism incorporated into the system to securely account node contributions and enable fair payment. We divide forwarding proofs from the state-of-the-art according to two criteria: mechanisms (Table 4) and trust (Table 5).

Mechanisms define how forwarding proofs are implemented. On the one hand, monitoring mechanisms implement traffic metering in the MANET with proxies and tunnels. RouteBazaar suggests using GRE (Generic Routing Encapsulation) tunnels to enable accounting of traffic samples in intermediate ASs [112] and storing information on-chain. Althea [113] uses Wireguard VPN tunnels to account traffic among neighbors. Rightmesh [119] uses proxy servers called superpeers that intermediate traffic. On the other hand, receipt mechanisms consist of packet delivery acknowledgments with piggybacked receipts. Those receipts consist of signatures from the destination of the original packet or cryptographic information about nodes in the forwarding path that can be used to redeem their

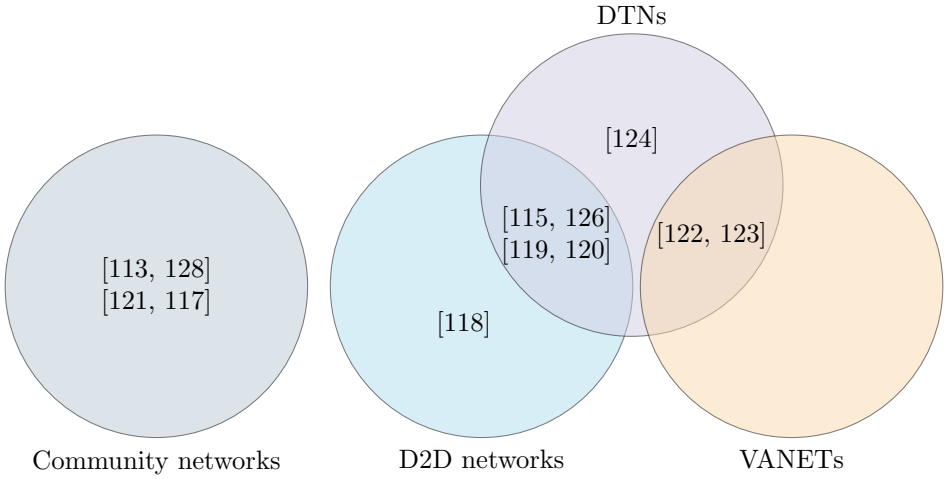

Figure 12: State-of-the-art classified accordingly to their application.

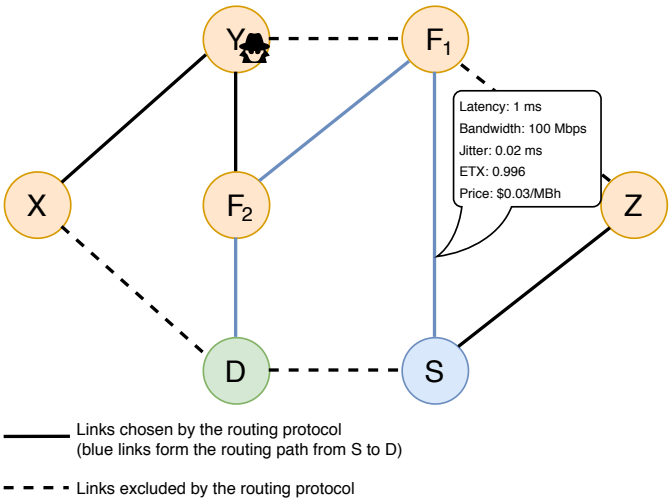

Figure 13: Example of a tree-based routing protocol, a routing path betweeen two nodes, and link metrics for the routing protocol.

rewards. The ownership of receipts is enough for forwarding proofs because the destination already acknowledged the packet's delivery. This strategy could be associated with off-chain channel micropayments [118, 119], confirmation of on-chain payment commitments [115, 124], or other mechanisms, such as anonymous tokens [123].

Table 4: Forwarding proof mechanisms

Traffic monitoring	Receipts
Althea [113]	LOT49 [118]
RouteBazaar [112]	Rightmesh [119]
	Kadupul [115]
	VDTN – RSU-to-vehicle [123]
	Truthful Incentive [124]

In the trust criteria, we divide forwarding proofs in trusted third-parties and trustless approaches. Trusted third-parties approaches assume trust in specific elements of the network architecture to ensure forwarding proofs, despite trustless payment mechanisms. Althea [113] needs to trust on neighbor's tunnel accounting. RouteBazaar [112] should rely on intermediate ASs traffic accounting. Rightmesh [119] depends on superpeers. Both VDTN works [122, 123] should trust on centralized certificate authorities. Post-disaster DTN [120] should trust on Control-nodes.

We can consider both cryptocurrency and packet forwarding as commodities that can be exchanged. There is plenty of blockchain-enabled trustless mechanisms to transfer cryptocurrency among parties securely. However, MANET credit-based incentives cannot be considered trustless unless they implement forwarding proofs that do not need to trust in third-parties in the same way that public blockchains. Up to now, it is an open challenge for incentivized MANETs. Moreover, distributed and collaborative accounting techniques to enable forwarding proofs could fall into the second-order free-riding problem that affects reputation mechanisms. In other words, nodes could act selfishly, avoid performing distributed accounting tasks, and taking advantage of other cooperative nodes' work. We believe that efficient solutions for trustless forwarding proofs should rely on algorithmic game theory design to model incentives for distributed accounting. The idea presented in the patent from Trautmann and Burnell [114] seems to follow this approach, though it needs further investigation.

6.2. Routing protocols

Most systems from the state-of-the-art implement forwarding incentives on top of existing routing paths. Different routing protocols define those paths as those shown in Table 6. Additionally, some systems are routing protocol agnostic [115, 125, 114]. In the case of DTNs, those

Table 5: Forwarding proof trust

Trusted third-party	Trustless
Althea [113]	Routing Based Blockchain [114]
RouteBazaar [112]	
Rightmesh [119]	
LOT49 [118]	
VDTN – RSU-to-RSU [122]	
VDTN – RSU-to-vehicle [123]	
Post-disaster DTN [120]	

paths are unknown beforehand but created opportunistically hop-by-hop.

Besides forwarding incentives, price-aware routing protocols have been explored in some works [113, 112]. For example, Althea [113] incorporates price costs in link metrics in addition to typical costs such as link speed and quality of service, as illustrated in Figure 13. As a result, paths are determined on a market basis where the price of the links is taken into account. Similarly, RouteBazaar [112] implements an on-chain catalog of AS routing paths with price and quality of service that can be contracted by interested ASs.

Table 6: Routing protocols

Routing protocol	Systems
BGP	RouteBazaar [112]
Babel	Althea [113]
Batman-Adv	AMMBR [116]
AODV	LOT49 [118]

6.3. Proof-of-Networking

Some works suggest using network service provided as a basis for proofs in blockchain consensus to produce (mine) new cryptocurrency [128, 121, 117, 114]. For example, a router that proves that it contributed to traffic forwarding or the convergence of a routing protocol could receive cryptocurrency as a Proof-of-Networking (PoN) [145] reward likewise Bitcoin's Proof-of-Work. The idea that is closer to PoN has been proposed by Trautmann and Burnell [114] in their Proof-of-Routing scheme.

6.4. Quality of Service

One problem that is barely discussed in the state-of-the-art is how to deal with different network quality of service (QoS) requirements. Real-time audio and video communication, online services, and delay-tolerant applications have distinct network requirements in terms of bandwidth, latency, and jitter. Systems should deploy some sort of network resource reservation and queueing policies to accomplish strict network requirements. At least, the system should allow clients to detect whether services are being provided as advertised or not. These features would require more complex forwarding proof mechanisms.

Even though RouteBazaar [112] pathlets provide on-chain path announcements with QoS information, there is no system enforcement or efficient mechanism to detect whether the intermediate ASs provide service accordingly. We found two works in this direction, though they are outside of the scope of forwarding incentives: PayFlow [146], which enables end devices to make pre-paid bandwidth reservations in a software-defined (SDN) network using cryptocurrency; the other work proposes an automatized smart contract SLA compensation system [147].

6.5. Privacy and Anonymity

Incentive mechanisms in MANETs could leak information about localization and trajectory of nodes and users when they create public on-chain transactions for payments. This security issue could also inhibit users from using MANET incentivized services. Some works support privacy mechanisms in order to avoid sensitive information from being exposed. Park *et al.* [122] propose zero-knowledge proof techniques for payments, and Li et al. [123] supports anonymous payments. RouteBazaar [112] proposes anonymized forwarding and payment proofs. Kadupul [115] *all or nothing* strategy can hide forwarder's identities. To achieve this, Kadupul assumes using anonymous broadcast and that the final receiver sends an acknowledge message directly to the sender. Then, the sender unlocks the puzzles for all the forwarders.

6.6. Common washing and frauds

Netcommons project [148] advocates community networks as commons and raises concerns regarding conflicts of interest in deploying cryptocurrencies for community networks incentives. They question whether commercial projects for blockchain-enabled community networks act legitimately toward a commons network infrastructure or mostly by for-profit motivations. Furthermore, they coin the term *common washing* that means the appropriation of the concept and the values of the common in the dominant discourse by private actors. Furthermore, the history of frauds regarding cryptocurrencies, such as ICO scams [149], intensifies these concerns.

Table 7: Summary of Blockchain Incentivized Data Forwarding in MANETs

System	Blockchain	MANET	Rout. Prot.	Payment proof	Forwarding proof	Privacy	Trusted third-party
Kadupul [115]	Bitcoin	D2D DTN	-	On-chain	Receipts	Hide forwarder's id	-
Truthful Inc. [124]	Bitcoin	DTN	-	On-chain	Receipts	-	-
RouteBazaar [112]	Bitcoin	-	BGP	On-chain	GRE tunnel acct.	Anon. fw. and pay.	Interm. AS traffic acct.
Post-disaster DTN [120]	Bitcoin	D2D DTN	-	On-chain	Receipts	-	Control-node
VDTN – to-RSU [122]	Ethereum	VDTN	-	On-chain	-	-	Service manager
VDTN – to-vehicle [123]	Ethereum	VDTN	-	On-chain	Receipts	Zero-knowl. proofs	Register authority
Althea [113]	Ethereum	Com. Net.	Babel	Off-chain Guac μpay.	VPN tunnel acct.	-	Peers' traffic acct.
Rightmesh [119]	Ethereum	D2D DTN	-	Off-chain μRaiden μpay.	Receipts	-	Superpeers
LOT49 [118]	Bitcoin	D2D	AODV	Off-chain Lightning μpay.	Receipts	-	Witness nodes
AMMBR [116]	Ethereum	Com. Net.	Batman-Adv	Off-chain Plasma childc.	-	-	-
Rout. Based Blockc. [114]	-	-	-	Proof-of-Routing	Proof-of-Routing	-	Trustless
MeshDapp [125]	Ethereum	-	-	On-chain	-	-	-
Blockmesh [121]	Ethereum	Com. Net.	-	-	-	-	-
Smartmesh [126]	Ethereum	D2D DTN	-	Off-chain Raiden μpay.	-	-	-
Skywire [117]	-	Com. Net.	-	-	-	-	-

7. Conclusion

This paper presented a comprehensive and detailed review of recent works on blockchain-enabled data forwarding incentives for multi-hop MANETs, summarized in Table 7. First, we contextualized selfish misbehavior in specific types of MANETs and why it affects data delivery reliability. We also summarized pre-blockchain incentive mechanisms that stimulate cooperative behavior and presented an overview of blockchain features that could support incentive mechanisms. In the state-of-the-art review, we described the key points of each work found. The works in the state-of-the-art consist of research papers, patents, and products. Finally, we discussed strategies adopted in the state-of-the-art and challenges for further research. Blockchains trustless features are in constant evolution and can potentially foster new forms of connectivity for future networks. We hope that this survey could be useful for other researchers and network protocol engineers to encourage them to explore blockchain concepts and systems to design efficient data forwarding incentive mechanisms. Our future works will focus on simulations and experiments to evaluate the best strategies for blockchain-enabled incentive mechanisms in data forwarding.

References

[1] P. Antoniadis, B. L. Grand, A. Satsiou, L. Tassiulas, R. L. Aguiar, J. P. Barraca, S. Sargento, Community Building over Neighborhood Wireless Mesh Networks, IEEE Technology and Society Magazine 27 (1) (2008) 48–56.

[2] D. Schuler, Community networks and the evolution of civic intelligence, AI & SOCIETY 25 (3) (2010) 291–307.

[3] P. Micholia, M. Karaliopoulos, I. Koutsopoulos, L. Navarro, R. B. Vias, D. Boucas, M. Michalis, P. Antoniadis, Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions, IEEE Communications Surveys Tutorials 20 (4) (2018) 3581–3606.

[4] A. Asadi, Q. Wang, V. Mancuso, A Survey on Device-to-Device Communication in Cellular Networks, IEEE Communications Surveys Tutorials 16 (4) (2014) 1801–1819.

[5] H. Hartenstein, K. Laberteaux, VANET: vehicular applications and inter-networking technologies, Vol. 1, John Wiley & Sons, 2009.

[6] A. Vasilakos, Y. Zhang, T. Spyropoulos, Delay Tolerant Networks: Protocols and Applications, 1st Edition, Wireless Networks and Mobile Communications (Book 19), CRC Press, 2011.

[7] B. Jedari, F. Xia, Z. Ning, A Survey on Human-Centric Communications in Non-Cooperative Wireless Relay Networks, IEEE Communications Surveys Tutorials 20 (2) (2018) 914–944.

[8] K. Panchanathan, R. Boyd, Indirect reciprocity can stabilize cooperation without the second-order free rider problem, Nature 432 (2004) 499–502.

[9] K. Werbach, The Blockchain and the New Architecture of Trust, Information Policy, The MIT Press, 2018.

[10] A. Bogliolo, P. Polidori, A. Aldini, W. Moreira, P. Mendes, M. Yildiz, C. Ballester, J. . Seigneur, Virtual currency and reputation-based cooperation incentives in user-centric networks, in: 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 2012, pp. 895–900.

[11] W. Lehr, J. Crowcroft, Managing shared access to a spectrum commons, in: First IEEE International Symposium on New

Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005., 2005, pp. 420–444.
[12] Y. L. Mischa Dohler, Cooperative Communications: Hardware, Channel and PHY, 1st Edition, Wiley, 2010.
[13] B. Wang, K. J. R. Liu, Advances in cognitive radio networks: A survey, IEEE Journal of Selected Topics in Signal Processing 5 (1) (2011) 5–23.
[14] M. Sami, N. K. Noordin, M. Khabazian, F. Hashim, S. Subramaniam, A Survey and Taxonomy on Medium Access Control Strategies for Cooperative Communication in Wireless Networks: Research Issues and Challenges, IEEE Communications Surveys Tutorials 18 (4) (2016) 2493–2521.
[15] M. Raya, J.-P. Hubaux, I. Aad, Domino: A system to detect greedy behavior in ieee 802.11 hotspots, in: Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, MobiSys '04, Association for Computing Machinery, New York, USA, 2004, p. 84–97.
[16] S. Buchegger, J. . L. Boudec, Self-policing mobile ad hoc networks by reputation systems, IEEE Communications Magazine 43 (7) (2005) 101–107.
[17] E. C. Efstathiou, P. A. Frangoudis, G. C. Polyzos, Stimulating Participation in Wireless Community Networks, in: Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, 2006, pp. 1–13.
[18] J. Cho, A. Swami, I. Chen, A survey on trust management for mobile ad hoc networks, IEEE Communications Surveys Tutorials 13 (4) (2011) 562–583.
[19] H. Li, M. Singhal, Trust management in distributed systems, Computer 40 (2) (2007) 45–53.
[20] S. Buchegger, J.-Y. Le Boudec, Performance Analysis of the CONFIDANT Protocol, in: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, MobiHoc '02, ACM, New York, USA, 2002, pp. 226–236.
[21] Q. He, D. Wu, P. Khosla, Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks, in: 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No.04TH8733), Vol. 2, 2004, pp. 825–830 Vol.2.
[22] R. Menaka, V. Ranganathan, B. Sowmya, Improving performance through reputation based routing protocol for manet, Wirel. Pers. Commun. 94 (4) (2017) 2275–2290.
[23] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, A. Kannan, QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks, Wireless Personal Communications 110 (4) (2019) 1637–1658.
[24] M. Felegyhazi, J.-P. Hubaux, L. Buttyan, Nash equilibria of packet forwarding strategies in wireless ad hoc networks, IEEE Transactions on Mobile Computing 5 (5) (2006) 463–476.
[25] P. H. Pathak, R. Dutta, A Survey of Network Design Problems and Joint Design Approaches in Wireless Mesh Networks, IEEE Communications Surveys Tutorials 13 (3) (2011) 396–428.
[26] H. Nishiyama, M. Ito, N. Kato, Relay-by-smartphone: realizing multihop device-to-device communications, IEEE Communications Magazine 52 (4) (2014) 56–65.
[27] I. F. Akyildiz, X. Wang, A survey on wireless mesh networks, IEEE Communications Magazine 43 (9) (2005) S23–S30.
[28] F. Domingos Da Cunha, L. Villas, A. Boukerche, G. Maia, A. Carneiro Viana, R. A. F. Mini, A. A. F. Loureiro, Data communication in vanets: Survey, applications and challenges, Ad Hoc Networks 44 (C) (2016) 90–103.
[29] J. Zhang, A Survey on Trust Management for VANETs, in: 2011 IEEE International Conference on Advanced Information Networking and Applications, 2011, pp. 105–112.
[30] F. Mohammed, I. Jawhar, N. Mohamed, A. Idries, Towards Trusted and Efficient UAV-Based Communication, in: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, USA, 2016, pp. 388–393.
[31] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, C. Diot, Pocket Switched Networks and Human Mobility in Conference Environments, in: Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking, WDTN '05, Association for Computing Machinery, New York, USA, 2005, p. 244–251.
[32] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, C. Cervello-Pastor, From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks, IEEE Communications Surveys Tutorials 14 (4) (2012) 1166–1182.
[33] N. Mantas, M. Louta, E. Karapistol, G. T. Karetsos, S. Kraounakis, M. S. Obaidat, Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey, IET Networks 6 (2017) 169–178(9).
[34] F. Xia, L. Liu, J. Li, J. Ma, A. V. Vasilakos, Socially Aware Networking: A Survey, IEEE Systems Journal 9 (3) (2015) 904–921.
[35] K. Wei, X. Liang, K. Xu, A Survey of Social-Aware Routing Protocols in Delay Tolerant Networks: Applications, Taxonomy and Design-Related Issues, IEEE Communications Surveys Tutorials 16 (1) (2014) 556–578.
[36] B. M. C. Silva, J. J. P. C. Rodrigues, N. Kumar, G. Han, Cooperative Strategies for Challenged Networks and Applications: A Survey, IEEE Systems Journal 11 (4) (2017) 2749–2760.
[37] Y. Zhang, W. Lou, W. Liu, Y. Fang, A Secure Incentive Protocol for Mobile Ad Hoc Networks, Wirel. Netw. 13 (5) (2007) 569–582.
[38] G. F. Marias, P. Georgiadis, D. Flitzanis, K. Mandalas, Cooperation enforcement schemes for MANETs: a survey, Wireless Communications and Mobile Computing 6 (3) (2006) 319–332.
[39] P. Antoniadis, B. L. Grand, A. Satsiou, L. Tassiulas, R. L. Aguiar, J. P. Barraca, S. Sargento, Community Building over Neighborhood Wireless Mesh Networks, IEEE Technology and Society Magazine 27 (1) (2008) 48–56.
[40] P. Micholia, M. Karaliopoulos, I. Koutsopoulos, L. Navarro, R. B. Vias, D. Boucas, M. Michalis, P. Antoniadis, Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions, IEEE Communications Surveys Tutorials 20 (4) (2018) 3581–3606.
[41] L. Cerdà-Alabern, R. Baig, L. Navarro, On the Guifi.net community network economics, Computer Networks 168 (2020) 107067.
[42] N. Samian, Z. A. Zukarnain, W. K. Seah, A. Abdullah, Z. M. Hanapi, Cooperation stimulation mechanisms for wireless multihop networks: A survey, Journal of Network and Computer Applications 54 (2015) 88–106.
[43] D. Yang, X. Fang, G. Xue, Game theory in cooperative communications, IEEE Wireless Communications 19 (2) (2012) 44–49.
[44] H. Zhu, X. Lin, R. Lu, Y. Fan, X. Shen, SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks, IEEE Transactions on Vehicular Technology 58 (8) (2009) 4628–4639.
[45] F. Li, J. Wu, FRAME: An Innovative Incentive Scheme in Vehicular Networks, in: 2009 IEEE International Conference on Communications, Dresden, Germany, 2009, pp. 1–6.
[46] M. E. Mahmoud, X. Shen, PIS: A Practical Incentive System for Multihop Wireless Networks, IEEE Transactions on Vehicular Technology 59 (8) (2010) 4012–4025.
[47] S. Téllez, Jesús; Zeadally, Mobile Payment Systems: Secure Network Architectures and Protocols, Springer Science and Business Media : Springer, 2017.
[48] D. E. Charilas, K. D. Georgilakis, A. D. Panagopoulos, Icarus: hybrid incentive mechanism for cooperation stimulation in ad hoc networks, Ad Hoc Networks 10 (6) (2012) 976–989.
[49] S. Goka, H. Shigeno, Distributed management system for trust and reward in mobile ad hoc networks, in: 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018, pp. 1–6.

[50] B. David, R. Dowsley, M. Larangeira, MARS: Monetized Ad-hoc Routing System (A Position Paper), in: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, CryBlock'18, ACM, New York, USA, 2018, pp. 82–86.

[51] M. Li, H. Tang, X. Wang, Mitigating Routing Misbehavior using Blockchain-Based Distributed Reputation Management System for IoT Networks, in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1–6.

[52] M. A. A. Careem, A. Dutta, Reputation based Routing in MANET using Blockchain, in: 2020 International Conference on COMmunication Systems NETworkS (COMSNETS), 2020, pp. 1–6.

[53] M. T. Lwin, J. Yim, Y.-B. Ko, Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks, Sensors 20 (3) (2020) 698.

[54] R. B. Myerson, Game Theory: Analysis of Conflict, Harvard University Press, Cambridge, USA, 1997.

[55] T. Roughgarden, Algorithmic game theory, Commun. ACM 53 (7) (2010) 78–86.

[56] Z. H. et al, Game theory in wireless and communication networks : theory, models, and applications, 1st Edition, Cambridge University Press, Cambridge, UK, 2012.

[57] Z. Han, C. Pandana, K. J. R. Liu, A self-learning repeated game framework for optimizing packet forwarding networks, in: IEEE Wireless Communications and Networking Conference, 2005, Vol. 4, 2005, pp. 2131–2136.

[58] J. J. Jaramillo, R. Srikant, A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks, Ad Hoc Networks 8 (4) (2010) 416–429.

[59] O. Ileri, S.-C. Mau, N. B. Mandayam, Pricing for enabling forwarding in self-configuring ad hoc networks, IEEE Journal on Selected Areas in Communications 23 (1) (2005) 151–162.

[60] C. Tang, A. Li, X. Li, When Reputation Enforces Evolutionary Cooperation in Unreliable MANETs, IEEE Transactions on Cybernetics 45 (10) (2015) 2190–2201.

[61] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Y. Zhou, Understanding the mirai botnet, in: 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, Canada, 2017, pp. 1093–1110.

[62] D. Mankins, R. Krishnan, C. Boyd, J. Zao, M. Frentz, Mitigating distributed denial of service attacks with dynamic resource pricing, in: Seventeenth Annual Computer Security Applications Conference, New Orleans, USA, 2001, pp. 411–421.

[63] Y. Huang, X. Geng, A. B. Whinston, Defeating DDoS Attacks by Fixing the Incentive Chain, ACM Trans. Internet Technol. 7 (1) (2007) 5–es.

[64] I. Zeifman, Bot Traffic Report 2016, Available at: `https://www.imperva.com/blog/bot-traffic-report-2016/` (2016).

[65] A. Gupta, D. O. Stahl, A. B. Whinston, The Economics of Network Management, Commun. ACM 42 (9) (1999) 57–63.

[66] M. Thelwall, D. Stuart, Web crawling ethics revisited: Cost, privacy, and denial of service, Journal of the American Society for Information Science and Technology 57 (13) (2006) 1771–1779.

[67] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Tech. rep., Bitcoin.org (2008).

[68] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, Association for Computing Machinery, New York, NY, USA, 2016, p. 254–269.

[69] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: Architecture, applications, and future trends, IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 (11) (2019) 2266–2277.

[70] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, Tech. rep., Ethereum project (2014).

[71] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE Computer Society, Honolulu, USA, 2017, pp. 557–564.

[72] Z. Feng, Q. Luo, Evaluating memory-hard proof-of-work algorithms on three processors, Proc. VLDB Endow. 13 (6) (2020) 898–911.

[73] S. Kim, Y. Kwon, S. Cho, A Survey of Scalability Solutions on Blockchain, in: 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, South Korea, 2018, pp. 1204–1207.

[74] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to Scalability of Blockchain: A Survey, IEEE Access 8 (2020) 16440–16455.

[75] J. Lau, Merkelized Abstract Syntax Tree, Available at: `https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki` (2016).

[76] M. Zamani, M. Movahedi, M. Raykova, RapidChain: Scaling Blockchain via Full Sharding, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 931–948.

[77] E. Lombrozo, J. Lau, P. Wuille, Segregated Witness (Consensus layer), Available at: `https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki` (2015).

[78] W. F. Silvano, R. Marcelino, Iota Tangle: A cryptocurrency to communicate Internet-of-Things data, Future Generation Computer Systems 112 (2020) 307 – 319.

[79] I. Eyal, A. E. Gencer, E. G. Sirer, R. Van Renesse, Bitcoin-NG: A Scalable Blockchain Protocol, in: Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation, NSDI'16, USENIX Association, USA, 2016, p. 45–59.

[80] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When Mobile Blockchain Meets Edge Computing, IEEE Communications Magazine 56 (8) (2018) 33–39.

[81] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, Y. Zhang, Cooperative and Distributed Computation Offloading for Blockchain-Empowered Industrial Internet of Things, IEEE Internet of Things Journal 6 (5) (2019) 8433–8446.

[82] Y. Jiao, P. Wang, D. Niyato, K. Suankaewmanee, Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks, IEEE Transactions on Parallel and Distributed Systems 30 (9) (2019) 1975–1989.

[83] D. Wu, N. Ansari, A Cooperative Computing Strategy for Blockchain-Secured Fog Computing, IEEE Internet of Things Journal 7 (7) (2020) 6603–6609.

[84] J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments, Available at: `http://lightning.network/docs` (January 2016).

[85] R. Network, Raiden network, Available at: `https://docs.raiden.network/` (2019).

[86] S. Dziembowski, S. Faust, K. Hostáková, General State Channel Networks, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 949–966.

[87] G. Maxwell, A. Poelstra, Y. Seurin, P. Wuille, Simple Schnorr multi-signatures with applications to Bitcoin, Designs, Codes and Cryptography 87 (9) (2019) 2139–2164.

[88] A. M. Antonopoulos, Mastering bitcoin: Programming the open blockchain, O'Reilly Media, Inc., Sebastopol, USA, 2017.

[89] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, K.-K. R. Choo, Sidechain technologies in blockchain networks: An examination and state-of-the-art review, Journal of Network and Computer Applications 149 (2020) 102471.

[90] J. Poon, V. Buterin, Plasma: Scalable autonomous smart contracts, Tech. rep., plasma.io (2017).

[91] V. Buterin, Minimal viable plasma, Available at: `https://et`

hresear.ch/t/minimal-viable-plasma/426 (2018).
[92] G. Konstantopoulos, Plasma Cash: Towards more efficient Plasma constructions, in: Stanford Blockchain Conference 2019, Stanford, USA, 2019, pp. 1–17.
[93] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D. I. Kim, A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks, IEEE Access 7 (2019) 22328–22370.
[94] S. King, Primecoin, Available at: https://primecoin.io (2013).
[95] A. Coventry, Nooshare: A decentralized ledger of shared computational resources, Available at: http://web.mit.edu/alexc/www/nooshare.pdf (2012).
[96] A. Shoker, Sustainable blockchain through proof of exercise, in: 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), IEEE Computer Society, Cambridge, USA, 2017, pp. 1–9.
[97] H. Huang, J. Lin, B. Zheng, Z. Zheng, J. Bian, When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues, IEEE Access 8 (2020) 50574–50586.
[98] A. Miller, A. Juels, E. Shi, B. Parno, J. Katz, Permacoin: Repurposing Bitcoin Work for Data Preservation, in: Proceedings of the 2014 IEEE Symposium on Security and Privacy, IEEE Computer Society, San Jose, USA, 2014, pp. 475–490.
[99] B. Sengupta, S. Bag, S. Ruj, K. Sakurai, Retricoin: Bitcoin Based on Compact Proofs of Retrievability, in: Proceedings of the 17th ACM International Conference on Distributed Computing and Networking (ICDCN), ACM, Singapore, Singapore, 2016, pp. 14:1–14:10.
[100] J. Benet, N. Greco, Filecoin: A decentralized storage network (2017).
[101] F. Liang, W. Yu, D. An, Q. Yang, X. Fu, W. Zhao, A survey on big data market: Pricing, trading and protection, IEEE Access 6 (2018) 15132–15154.
[102] C. Chen, J. Wu, H. Lin, W. Chen, Z. Zheng, A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles, IEEE Transactions on Vehicular Technology 68 (9) (2019) 9110–9121.
[103] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou, H. Jin, SDTE: A Secure Blockchain-Based Data Trading Ecosystem, IEEE Transactions on Information Forensics and Security 15 (2020) 725–737.
[104] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing microgrid energy markets: A case study: The Brooklyn Microgrid, Applied Energy 210 (2018) 870 – 880.
[105] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews 100 (2019) 143 – 174.
[106] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains, IEEE Transactions on Industrial Informatics 13 (6) (2017) 3154–3164.
[107] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, K.-K. R. Choo, BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system, Computers & Security 85 (2019) 288 – 299.
[108] M. Taghavi, J. Bentahar, H. Otrok, K. Bakhtiyari, A Blockchain-Based Model for Cloud Service Quality Monitoring, IEEE Transactions on Services Computing 13 (2) (2020) 276–288.
[109] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, M. Song, Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing, IEEE Transactions on Wireless Communications 18 (1) (2019) 695–708.
[110] C. Lin, D. He, X. Huang, X. Xie, K.-K. R. Choo, Blockchain-based system for secure outsourcing of bilinear pairings, Information Sciences 527 (2020) 590 – 601.
[111] H. Asghari, M. Van Eeten, A. Arnbak, N. A. van Eijk, Security economics in the HTTPS value chain, in: Twelfth Workshop on the Economics of Information Security (WEIS 2013), Elsevier, Washington,DC,USA, 2013, pp. 1–36.
[112] I. Castro, A. Panda, B. Raghavan, S. Shenker, S. Gorinsky, Route Bazaar: Automatic Interdomain Contract Negotiation, in: 15th Workshop on Hot Topics in Operating Systems (HotOS XV), USENIX Association, Kartause Ittingen, Switzerland, 2015, pp. 1–7.
[113] J. Tremback, J. Kilpatrick, D. Simpier, B. Wang, Althea white paper, Available at: https://althea.net/whitepaper (Apr. 2019).
[114] T. Trautmann, A. Burnell, Routing Based Blockchain (U.S. Patent 16/104,849 430, Feb. 2020).
[115] M. Skjegstad, A. Madhavapeddy, J. Crowcroft, Kadupul: Livin' on the Edge with Virtual Currencies and Time-Locked Puzzles, in: Proceedings of the 2015 Workshop on Do-it-yourself Networking: An Interdisciplinary Approach, DIYNetworking '15, ACM, New York, USA, 2015, pp. 21–26.
[116] AMMBR Foundation, AMMBR: white paper v2, Available at: https://ammbr.com/docs/2018/11/Ammbr_Whitepaper.pdf (2018).
[117] Skycoin, Skycoin - Edition 1.2, Available at: https://www.skycoin.com/whitepapers (Oct. 2017).
[118] R. Myers, A lightweight protocol to incentivize mobile peer-to-peer communication, Available at: https://global-mesh-labs.gitbook.io/lot49/ (Jun. 2019).
[119] J. Ernst, Z. Wang, S. Abraham, J. Lyotier, C. Jensen, M. Quinn, D. Harvey, The Power of Connectivity in the Hands of the People – Decentralized Mobile Mesh Networking Platform Powered by Blockchain Technology and Tokenization, Available at: https://www.rightmesh.io/whitepapers (Mar. 2018).
[120] C. Chakrabarti, S. Basu, A Blockchain Based Incentive Scheme for Post Disaster Opportunistic Communication over DTN, in: Proceedings of the 20th International Conference on Distributed Computing and Networking, ICDCN '19, Association for Computing Machinery, New York, USA, 2019, p. 385–388.
[121] Prometeus Industries Pty, Blockmesh, Available at: https://www.blockmesh.io/pdf/BlockMesh-White_Paper-1.pdf (2017).
[122] Y. Park, C. Sur, K.-H. Rhee, A Secure Incentive Scheme for Vehicular Delay Tolerant Networks Using Cryptocurrency, Security and Communication Networks (2018) 73–85.
[123] M. Li, J. Weng, A. Yang, J. Liu, X. Lin, Toward blockchain-based fair and anonymous ad dissemination in vehicular networks, IEEE Transactions on Vehicular Technology 68 (11) (2019) 11248–11259.
[124] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, L. Sun, A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications, IEEE Access 6 (2018) 27324–27335.
[125] E. Dimogerontakis, L. Navarro, M. Selimi, S. Mosquera, F. Freitag, Meshdapp – blockchain-enabled sustainable business models for networks, in: K. Djemame, J. Altmann, J. Á. Bañares, O. Agmon Ben-Yehuda, M. Naldi (Eds.), Economics of Grids, Clouds, Systems, and Services - GECON 2019, Vol. 11819, Springer International Publishing, Cham, 2019, pp. 286–290.
[126] Smartmesh Foundation, SmartMesh Tokenized Mobile Mesh Network, Available at: https://smartmesh.io/SmartMeshWhitePaperEN.pdf (2017).
[127] F. Vogelsteller, V. Buterin, Eip 20: Erc-20 token standard, Available at: https://eips.ethereum.org/EIPS/eip-20 (2015).
[128] AMMBR Foundation, AMMBR: white paper v1, Available at: https://ammbr.com/docs/201708/Ammbr_Whitepaper_v1.1_15Aug2017.pdf (2017).
[129] Gwern.net, Time-Locked Encryption, Available at: https://www.gwern.net/Self-decrypting-files (2019).

[130] J. Chroboczek, The Babel Routing Protocol, RFC 6126, RFC Editor (Apr. 2011).
[131] J. Tremback, Althea's multihop payment channels, Available at: https://blog.althea.net/altheas-multihop-payment-channels/ (2017).
[132] Brainbot Labs, μRaiden, Available at: https://microraiden.readthedocs.io/ (2018).
[133] C. Decker, R. Russell, O. Osuntokun, eltoo: A simple layer 2 protocol for bitcoin, Available at: https://blockstream.com/eltoo.pdf (2018).
[134] I. D. Chakeres, E. M. Belding-Royer, AODV routing protocol implementation design, in: 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings., IEEE Computer Society, Tokyo, Japan, 2004, pp. 698–703.
[135] D. Seither, A. König, M. Hollick, Routing performance of Wireless Mesh Networks: A practical evaluation of BATMAN advanced, in: 2011 IEEE 36th Conference on Local Computer Networks, IEEE Computer Society, Osnabrück, Germany, 2011, pp. 897–904.
[136] A. Neumann, L. Navarro, L. Cerdà-Alabern, Enabling individually entrusted routing security for open and decentralized community networks, Ad Hoc Networks 79 (2018) 20–42.
[137] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, On Security Analysis of Proof-of-Elapsed-Time (PoET), in: P. Spirakis, P. Tsigas (Eds.), Stabilization, Safety, and Security of Distributed Systems, Springer International Publishing, Cham, 2017, pp. 282–297.
[138] E. San Miguel, R. Timmerman, S. Mosquera, E. Dimogerontakis, F. Freitag, L. Navarro, Blockchain-Enabled Participatory Incentives for Crowdsourced Mesh Networks, in: K. Djemame, J. Altmann, J. Á. Bañares, O. Agmon Ben-Yehuda, M. Naldi (Eds.), Economics of Grids, Clouds, Systems, and Services, Springer International Publishing, Cham, 2019, pp. 178–187.
[139] S. D. Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain, in: Italian Conference on Cyber Security, Milan, Italy, 2018, pp. 1–11.
[140] A. R. Kabbinale, E. Dimogerontakis, M. Selimi, A. Ali, L. Navarro, A. Sathiaseelan, J. Crowcroft, Blockchain for economically sustainable wireless mesh networks, Concurrency and Computation: Practice and Experience 32 (12) (2020) e5349, e5349 cpe.5349.
[141] L. Baumgärtner, P. Gardner-Stephen, P. Graubner, J. Lakeman, J. Höchst, P. Lampe, N. Schmidt, S. Schulz, A. Sterz, B. Freisleben, An experimental evaluation of delay-tolerant networking with serval, in: 2016 IEEE Global Humanitarian Technology Conference (GHTC), IEEE Computer Society, Seatle, USA, 2016, pp. 70–79.
[142] S. P. Gardner, Serval Project, Available at: http://servalproject.org (2019).
[143] P. T. Documentation, Light Ethereum Subprotocol, Available at: https://openethereum.github.io/wiki/Light-Ethereum-Subprotocol-(LES) (2020).
[144] D. Vega, R. Baig, L. Cerdà-Alabern, E. Medina, R. Meseguer, L. Navarro, A technological overview of the guifi.net community network, Computer Networks 93 (2015) 260–278, community Networks.
[145] L. Ghiro, L. Maccari, R. L. Cigno, Proof of networking: Can blockchains boost the next generation of distributed networks?, in: 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), IEEE Computer Society, Isola, France, 2018, pp. 29–32.
[146] D. Chen, Z. Zhang, A. Krishnan, B. Krishnamachari, PayFlow: Micropayments for Bandwidth Reservations in Software Defined Networks, in: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019, pp. 26–31.
[147] E. J. Scheid, B. B. Rodrigues, L. Z. Granville, B. Stiller, Enabling Dynamic SLA Compensation Using Blockchain-based Smart Contracts, in: 2019 IFIP/IEEE Symposium on Integrated Network and Service Management, 2019, pp. 53–61.
[148] netCommons, Network Infrastructure as Commons, Available at: https://www.netcommons.eu/ (2019).
[149] C. C. University, The list of scam & fraud crypto websites, Available at: https://cryptochainuni.com/scam-list/ (2020).