Future Generation Computer Systems 112 (2020) 283–296

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems

Jérémy Robert [b,*], Sylvain Kubler [a], Sankalp Ghatpande [b]

[a] Université de Lorraine, CNRS, CRAN, UMR 7039, France
[b] University of Luxembourg, Interdisciplinary Center for Security, Reliability and Trust, Luxembourg

ARTICLE INFO

Article history:
Received 27 August 2019
Received in revised form 19 February 2020
Accepted 20 May 2020
Available online 27 May 2020

Keywords:
Blockchain
Lightning Network
Cryptocurrency
Internet of Things
Micropayment

ABSTRACT

Information is being seen as the new "oil" for companies. Trading and negotiating personal data, which includes data generated by owned smart devices, is gaining attention and acceptance in the Internet of Things (IoT) era. There is a global trend to move towards open innovation ecosystems that allow data owners to have better control over their data and privacy, choosing if/what and with whom to share/trade specific data streams. Nonetheless, this requires the design of IoT ecosystems that integrate automatic enforcing mechanisms to guarantee the delivery of the negotiated data, or still the capability of making near-instantaneous payments for the data (in the form of micro-units). This paper discusses the requirements that need to be fulfilled to properly support (micro)-payment in IoT, and further the extent to which different blockchain technologies can fulfill those requirements. Based on this analysis, our paper progresses the current state-of-the-art in three-respect: (i) by carrying out a benchmark performance analysis between LN and other-like solutions; (ii) by integrating the Lightning Network (LN) off-chain technology within an existing IoT ecosystem, developed as part of the bIoTope H2020 project, and (iii) by designing a novel algorithm for payment channel fee reduction. Experiments carried out in this paper show that LN outperforms traditional blockchain solutions under IoT-specific constraints and objectives, and that an optimal parameter setting of the proposed algorithm can be identified.

1. Introduction

The development of the Internet has brought forth a rapid change in the society, from the introduction of *e*-commerce to social media, it has become part of everyday life. The Internet of Things (IoT) is an evolution of how the Internet can be used and leveraged, providing smart connected things with the ability to communicate over the World Wide Web with other things, people, processes, which is also referred to as the Web of Things (WoT) [1]. However, the reality is not as rosy as it may sound, as today's IoT is essentially a collection of isolated "Intranets of Things", also referred to as "vertical silos" [2,3] where data is siloed in a unique system, cloud, domain, and stay there, thus preventing market growth [4]. Contrary to vertically-oriented closed systems, several organizations and standardization fora understood the need to move towards open innovation ecosystems [5–7], which should allow Things' owners to have full end-to-end control over their data and privacy; for example choosing to share/trade (or not) Thing-related data with a specific peer; deciding for which purpose personal data could be used, and so forth. Nonetheless, this requires the design and adoption of large-scale IoT ecosystems that should facilitate the seamless discovery, access and integration of heterogeneous, sensor-originated data through the WoT, integrate automatic enforcing mechanisms to guarantee the delivery of the negotiated data, or still the capability of making near-instantaneous payments for the data (i.e., in the form of micro-units). The emerging blockchain movement brings interesting solutions to meet those requirements [3,8], including distributed ledger and smart contract capabilities, encryption mechanisms, *etc.* [9–13].

Blockchain is a technology that has found applications in various areas such as transaction processing, crowdfunding, or government cash management [15,16]. To date, a new use of that technology and a complete new range of applications are made possible with the introduction of the so-called "smart contracts" (payments becoming conditional on the state of variables) [17], which is increasingly used in all sectors of our society for industrial, telecommunications, medical, or still consumer applications [18–20]. However, besides legal, cultural and organizational challenges, technical limitations of traditional blockchains (e.g., bitcoin and Ethereum to name the most well known) cannot scale for wide-spread use. To overcome this issue, a new range of blockchain solutions called "off-chain" protocols has

* Corresponding author.
E-mail address: jeremy.robert@uni.lu (J. Robert).

https://doi.org/10.1016/j.future.2020.05.033
0167-739X/

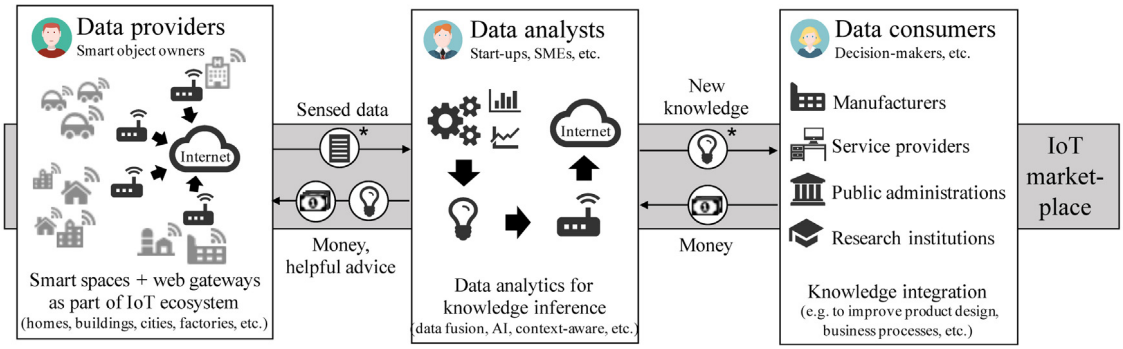


Fig. 1. Stakeholders and possible interactions in large-scale IoT ecosystem [14].

emerged, consisting in temporarily moving some transactions off-chain for computation elsewhere, and then returning a summary to the main chain. This approach is promising to better meet IoT requirements in terms of privacy, security, throughput, and latency [21], as argued by Ron Resnick (EEA Executive Director of the Enterprise Ethereum Alliance[1].). A number of off-chain solutions have emerged in the recent years [22], the most well-known today being the "Lightning Network (LN)" [23]. LN allows micropayments to be securely and bi-directionally routed across multiple peer-to-peer payment channels, resulting in enhanced scalability, throughput and latencies. Micropayments in IoT applications could span from trading sensor-originated data (e.g., temperature, humidity, home appliance or car-related sensor data) to aggregated or processed data (e.g., historical maintenance datasets, prediction web service, etc.). At the time of writing this article, we are not aware of any research initiative that has focused on (i) investigating how to integrate the LN technology into large-scale IoT ecosystems; neither on (ii) evaluating the extent to which LN outperforms traditional blockchain technologies. This paper tackles these two research and engineering gaps with a threefold contribution:

1. a benchmark performance analysis between LN and other-like solutions is carried out;
2. a framework for integrating LN with an existing IoT ecosystem is presented;
3. a novel algorithm for payment channel management and fee reduction is designed.

While the first and second contribution are unique, to the best of our knowledge, one may wonder to what extent the third one differs from state-of-the-art studies focusing on the integration of blockchain with IoT infrastructures. As will be further discussed and analyzed in Section 2, the current literature mainly focuses on the definition of smart contracts for various IoT application purposes, but a very few focus on the integration of micro-billing solutions in open IoT ecosystems, and even fewer on improving existing micro-billing solutions. This makes our research different.

The paper structure is as follows: Section 2 discusses requirements that need to be fulfilled when dealing with micropayments in large IoT ecosystems, along with the extent to which off-chain solutions could meet those requirements. Section 3 presents both the proposed integration framework and algorithm for fee reduction. Section 4 presents the implemented framework and experimental results; the conclusion follows.

2. Blockchain-enabled micropayments

Section 2.1 discusses the importance of supporting data trading and micropayment in large-scale IoT ecosystems. Section 2.2 provides a more-in-depth discussion about the building blocks underlying any blockchain technology, and the extent to which they impact on the overall system performance. Section 2.3 provides first experimental evidence that off-chain solutions outperform on-chain ones from a throughput, speed and fee transaction perspective.

2.1. Need for micropayment in ecosystem-wide marketplaces

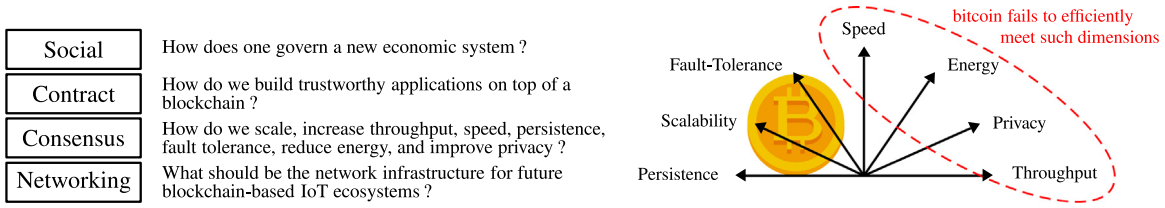
Several organisms and standardization fora understood the need to work against the "vertical silos" model that shape today's IoT [3,4] and to move towards the creation of open[2] IoT ecosystems [5] that offer efficient identification, discovery and interoperation of data and services across platforms [24]. Among other standardization fora and initiatives, let us cite the Alliance for Internet of Things Innovation (AIOTI) launched by the EU [25], the Open Platform 3.0™ at The Open Group, the OneM2M global standards initiative [26], the IEEE Internet of Things (IoT) initiative [27], or still the International Technical Working Group on IoT-Enabled Smart City Framework developed at NIST [28].

In the vision of a sustainable IoT ecosystem, it should be possible to create a new value chain through establishing an environment for data trading between different stakeholders, as depicted in Fig. 1, namely between (i) end-users who own smart objects (e.g., a smart fridge); (ii) data analysts (startups, SMEs…) who may be interested in accessing smart object-related data to deliver new services that fulfill untapped needs, whether end-user needs (e.g., offering a new service that proposes recipes with food items that are going to exceed the best before date) and/or business needs (e.g., generating some knowledge such as usage patterns, failure prediction, which could benefit the (iii) fridge manufacturer to improve the fridge design). As emphasized in Fig. 1, various types of incentives between these stakeholders could be imagined such as money returns, vouchers or even "helpful tip" transactions [29]. Digital marketplaces could be considered to help supporting such incentives schemes, acting as IoT search engines for multimodal registration, discovery and trading of data and services, as described in [5,14]. From a data/service trading perspective, a key challenge is to step back from the widely adopted centralized cloud approach that poses security and privacy concerns [30,31], and move towards decentralized and distributed systems [3,8,32,33].

The emergence of blockchain-based innovations have led to a large number of consortia working on the design and implementation of decentralized digital marketplaces in the IoT era.

[1] https://entethalliance.org, last access Aug. 2019

[2] Within the meaning of "open" standards.



(a) Blockchain Stack and Trade-Off problem

(b) Blockchain Stack and Trade-Off problem

Fig. 2. Blockchain Stack and Trade-Off problem.

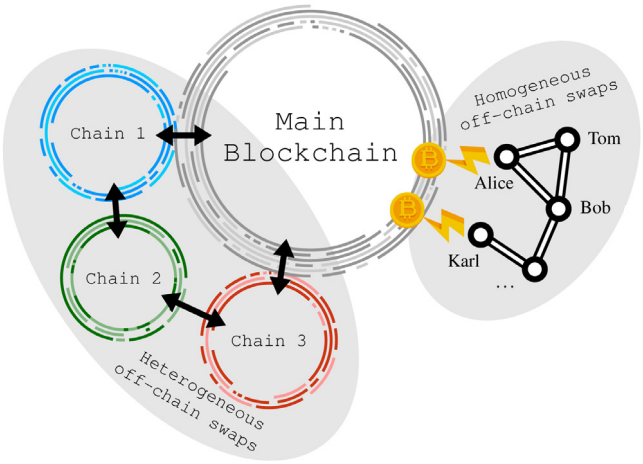


Fig. 3. Overview of the different "off-chain" families/technologies (i.e., atomic cross-chain swaps and payment channels).

Among well-known initiatives, let us mention the Trusted IoT Alliance[3] and IoTA foundation,[4] the Enterprise Ethereum Alliance (EEA), or still Flowchain.[5] All these initiatives promote and/or investigate different, but also common architectural design principles and best practices to meet IoT requirements at different blockchain levels, which can be declined into [15]: (i) Networking; (ii) Consensus; (iii) Contract and (iv) Social, as depicted in Fig. 2(a).

Over the past few years, an increasing number of scientific studies have proposed blockchain-based IoT applications, as reported in Table 1. Even though the list is not exhaustive, it shows that most of the papers focus on presenting a given architecture/application and associated smart contracts (*cf.*, columns respectively denoted by "Architecture" and "Smart Contr". in Table 1), along with performance analyses (*cf.*, column denoted by "Performance"). Despite the importance of integrating blockchain technologies in (large-scale) IoT ecosystems [34], too little work has been done in this regard (*cf.*, column denoted by "IoT Ecosys".). Similarly, much remains to be done to support micro-billing in large-scale IoT settings (*cf.*, column denoted by "Micro-billing"). An interesting work for supporting scalable micropayments using LN is proposed in [23], in which architectural designs and possible use cases are described, however no experimental evidence of the system performance are provided. In [35], the authors propose an alternative solution to LN and Raiden Network, called FastPay, which aims at overcoming the hidden transactions problem (i.e., the fact that payments are batched and the blockchain only records the combined payments, losing information about the raw payments). Although the approach is interesting, the FastPay platform is designed for edge-IoT platforms and not for large-scale IoT ecosystems. Green et al. [36] introduce techniques for constructing anonymous payment channels, which is not possible with LN-like solutions. Despite a few limitations of their approach, discussed by the authors themselves, performance of the proposed approach is not evaluated. [37] is, to the best of our knowledge, one of the few studies that focus on horizontally integrated IoT systems, which is what we refer to as "open IoT ecosystem", in which the authors design a new protocol for lightweight payments.

The next section discusses the requirements for micropayment in IoT environments, along with why traditional blockchain cryptocurrencies fail to meet those requirements.

2.2. Requirements and challenges

Despite the fact that micropayment is a hot topic in the literature [52,53], there is no coherent definition of what (or how small) a micropayment should be. Popular commercial providers dealing with digital transactions (e.g., PayPal) classify a micropayment as a payment of less than 5 USD[6], while other scholars or studies consider it as low as a *"fraction of a penny"* [54], or still as 1.10^{-6} USD [55]. While traditional blockchain-based cryptocurrencies (e.g., bitcoin, Ether) can be beneficially used for the former definition, they turn to be inappropriate for the latter due to the incurred transaction (or processing) fees. Indeed, cryptocurrency exchanges impose transaction fees that may become higher than the cost to sell or buy sensor IoT data. For example, bitcoin transaction fees reached ≈38 USD in 2017, while a pay-as-you-go API call should not exceed a couple of cents.

In addition to the transaction fee concern, other requirements make traditional blockchain solutions inappropriate to support micropayment in large-scale IoT ecosystems, in which billions of API calls – *and thus transactions* – need to be performed on a daily basis [56]. Those requirements are mainly related to the "Consensus" layer (*cf.*, Fig. 2(a)), and particularly the fact that traditional blockchain consensus protocols fail to meet key performance dimensions. For example, bitcoin technology is very efficient to make systems persistent, scalable and highly tolerant to faults, but it offers very poor performance in terms of transaction speed, throughput, energy and privacy [57], as emphasized in Fig. 2(b). To overcome those limitations, the "Off-chain Atomic Swaps" paradigm has been introduced, which consists in offloading selected transactions from the main blockchain to a trusted compute environment. This approach is gaining attention and investment worldwide. The next section further discuss the "Off-chain Atomic Swaps" paradigm.

3 https://www.trusted-iot.org, last access Aug. 2019.

4 https://www.iota.org, last access Aug. 2019.

5 https://flowchain.co, last access Aug. 2019.

6 https://www.paypal.com/us/smarthelp/article/what-are-micropayments-faq664, last access Aug. 2019.

Table 1
Overview of state-of-the-art integration framework regarding IoT & Blockchain.

Ref.	Platform/protocol	Architecture	Performance	Smart Contr.	Micro-billing	IoT Ecosys.	Description
[38]	PoS-like	✓	✓	✓	✗	✓	Design of a blockchain-based framework for food traceability
[39]	Ethereum	✓	✓	✓	✗	✓	Design of a blockchain based monitoring system for healthcare application by using smartphones
[34]	Ethereum	✓	✓	✓	✗	✍	Change dynamically the hash function to improve performance
[40]	PoW	✓	✓	✓	✗	✗	Improvement of the mining process efficiency by controlling block number between IoT devices and blockchain
[41]	Ethereum	✓	✓	✓	✗	✗	Design of a novel decentralized auditing smart contract in Ethereum
[42]	N/A	✓	✓	✓	✗	✗	Design of an blockchain-based IoT architecture supporting effective big data analysis in the cloud
[43]	Fast BFT	✓	✍	✓	✗	✗	Design of a secure and lightweight architecture based on a new software-defined blockchain model and a BFT algorithm
[44]	Ethereum	✓	✓	✗	✗	✗	Design of a new scheme for aggregating blockchain data in periodic updates to reduce the communication cost of wireless IoT devices
[45]	Po(Stability)	✓	✓	✗	✗	✗	Design of a secure clock synchronization scheme for blockchain-enabled IoT based on a new Proof of Stability consensus
[46]	PoW	✓	✗	✓	✗	✍	Access control framework based on blockchain enabling to distribute access tokens using smart contracts
[47]	FlowChain	✓	✗	✗	✗	✍	Design of a new distributed ledger system for peer-to-peer networks and real-time data transactions
[48]	Ethereum	✓	✗	✗	✗	✍	Design of a light client for Smart Cities
[37]	Ethereum	✗	✓	✓	✓	✍	Design of a Ticket-Based Verification Protocol minimizing the number of accounts needed for an organization
[35]	Ethereum	✗	✓	✗	✓	✗	Design of a secure fast payment protocol for blockchain-based IoT
[49]	TumbleBit	✗	✓	✗	✓	✗	Design of a new fully bitcoin compatible payment hub acting as intermediary for off-chain payment
[50]	PBFT	✗	✓	✗	✗	✗	Design of a lightweight IoT information sharing security framework preventing local malicious behavior
[51]	N/A	✗	✗	✍	✍	✍	Survey the privacy preservation in blockchain-based IoT applications
[23]	LN	✗	✗	✗	✓	✗	Design of a new technology for improving bitcoin transactions rate
[36]	Bolt	✗	✗	✗	✓	✗	Design of a new technique to build anonymous payment channels

✓ addressed or considered ✗ not addressed or considered ✍ Partial, on-going or future work.

2.3. Towards the use of off-chain solutions in IoT ecosystems

Section 2.3.1 briefly introduces existing off-chain atomic swaps mechanisms, which can be divided into two categories: heterogeneous and homogeneous off-chain swaps [22]. Section 2.3.2 provides a first benchmark analysis between technologies falling within these two categories as well as with the most known on-chain solutions: bitcoin.

2.3.1. Categories of off-chain atomic swaps

A well-known approach to conduct off-chain transactions consists in using a broker-like system (or cryptocurrency exchange point) that maintains end-user accounts. To put it another way, the transactions are offloaded to a custodian, whereby users require trusting third party custodians to hold the tokens, update user balances, and allow withdrawal/deposits [58]. However, this approach requires to trust a third party to hold users' fund, leading to counterparty risk, as evidenced by the *Mt. Gox event* (largest bitcoin exchange point) that lost bitcoins worth half a million USD [59]. To enable interchangeability of digital assets across different blockchains without involving any broker or centralized intermediary, atomic swaps mechanisms have been introduced, also known as atomic cross-chain swaps. Two distinct mechanisms can be distinguished, as described in [22] and depicted in Fig. 3, namely:

- *heterogeneous off-chain swaps:* they support interchangeability of assets at a predetermined rate between the parent blockchain, which is usually referred to as the "main chain", and all additional blockchains referred to as "side chains". Examples of heterogeneous off-chain swaps are weiDex[7] (between Ethereum, Aeternity, bitcoin, LockTrip) and Elements by Blockstream [60];
- *homogeneous off-chain swaps:* Unlike heterogeneous off-chain swaps that deal with different cryptocurrencies, homogeneous ones only deal with one cryptocurrency, where some transactions are offloaded from the main chain to a trusted compute environment. An example of homogeneous off-chain swaps is Lightning Network (LN) [23], which relies on bitcoin.

[7] https://www.stateofthedapps.com/dapps/weidex, last access Aug 2019.

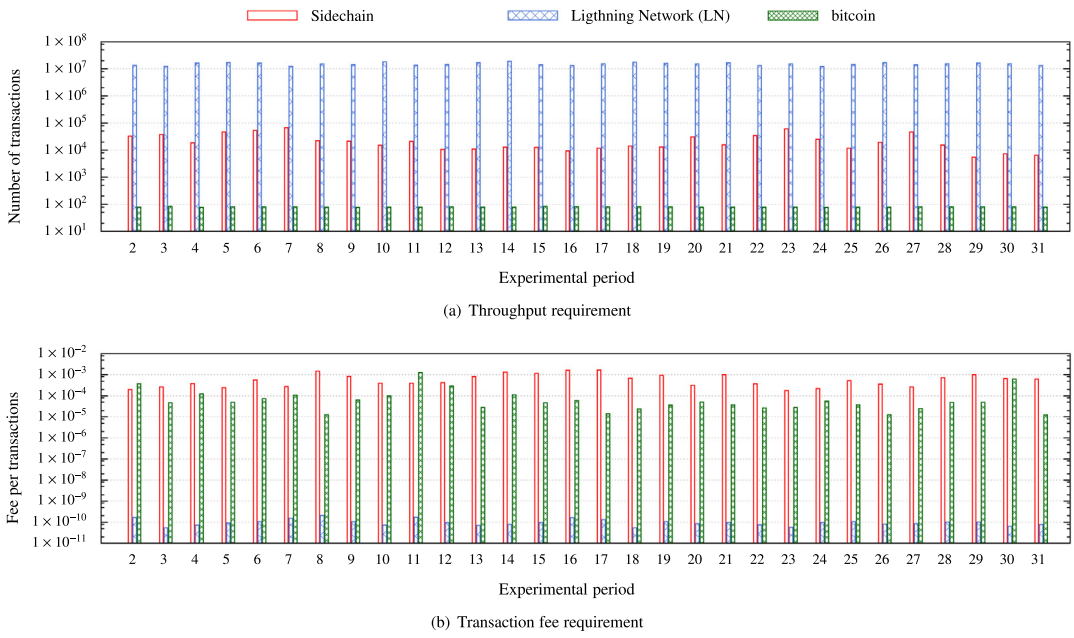


Fig. 4. Bitcoin *vs.* LN from a (i) Throughput and (ii) Transaction fee perspective over a 1-month period.

In case of heterogeneous atomic cross-chain swaps, fees must be paid on each of the chains that are part of the system (*cf.*, Fig. 3), meaning that one transaction would incur multiple transaction fees. For homogeneous off-chain swaps, and particularly in the context of LN that introduces the concept of payment channels[8], users can conduct multiple transactions (valued at micro-units) without committing all of them towards the main chain. As a result, if a payment channel is kept opened on a sufficiently long-term basis, the overall transaction fee can be significantly reduced, or at least remain in profit. Furthermore, one may expect that payment channels could also contribute to greatly improve performance of blockchain-based IoT systems, whether in terms of scalability, speed and throughput. To confirm this, we conducted a first benchmark analysis, which is presented in the next section.

2.3.2. On-chain blockchain vs. heterogeneous & homogeneous off-chain atomic swaps: A comparison study

The objective of this section is to carry out a first comparison analysis between the well-known bitcoin (on-chain) cryptocurrency and two off-chain technologies respectively belonging to the heterogeneous and homogeneous off-chain swaps categories. In this respect, we considered Sidechain (heterogeneous) and LN (homogeneous). We evaluated the three technologies – *from a throughput, speed and transaction fee viewpoint* – over a one month period. The experiments were performed under Testnet3,[9] which is the development instance of the public bitcoin blockchain, although Testnet3 slightly differs in its valuation of bitcoin and the mining difficulty. Experiments were run over a 1-month period.

Fig. 4(a) shows the extent to which LN and Sidechain allow for performing a higher number of transactions compared with bitcoin. Overall, on a daily basis, LN enables to carry out around 1000 times more transactions than Sidechain and 100.000 times more than bitcoin. This result is not negligible in the context of large-scale IoT ecosystems, where business transactions may reach 450 billion a day by 2020 according to market prediction estimates [61].

Fig. 4(b) provides insight into the overall transaction fee that must be paid for each technology. For comparison purposes, we considered a scenario where the end-user unlocks her/his LN-related funds on a daily basis, leading to the closing of the channel at a given point in time every day (midnight in our experiment). Similarly with Sidechain, the end-user freezes her/his funds on the main chain at midnight and waits for approx. 10 min before the funds are claimed on the sidechain and used for transactions. It should be noted that transaction payment values are randomly selected between 0.001 and 0.0001 in order to approach micro-payment's reality. This experiment clearly shows that the use of LN significantly reduces the overall fee on a daily basis, reducing by around 1.000.000 times the fee paid if payment channels where not used (i.e., difference between bitcoin and LN results). Note that this reduction could be even more significant if the channel would be kept open on a longer time-scale (e.g., on a weekly basis). Likewise, the overall fee paid with Sidechain is lower compared with bitcoin, but remains higher when compared with LN.

Regarding the speed dimension, no comparison study was conducted because the finding is well-known by the blockchain community, namely that bitcoin aggregates transactions into blocks that are approved on an average of 7 to 10 min apart, while payments in LN are in principle instant and atomic (only constrained by the network bandwidth). Let us note that bitcoin confirmation period still exists but only when a LN channel is opened or closed, which results in a bitcoin transaction. Sidechain, on the other hand, has high latency mainly due to the fact that a transaction from the main chain to the Sidechain requires the 7 to 10 min bitcoin approval time, adding multiple blocks to be validated when getting the assets back to main chain. All in all, each transaction cycle (main chain to sidechain, transactions and then sidechain to main chain) requires approximately 1 hour on average.

8 A payment channel in LN follows specific steps in order to be successful:
1. A state is locked on the blockchain using multi-signature (form of smart contract that provides irrefutable claims for users).
2. Users who are the party of the multi-signature have to update the state of the blockchain among themselves by constructing and signing transactions that could be submitted to the main chain at any given point in time (each new updated transaction cancels out the previous one);
3. Users can decide to submit the state back to the main chain, thus resulting in the closing of the channel and associated state.

9 https://en.bitcoin.it/wiki/Testnet, last access Aug. 2019.

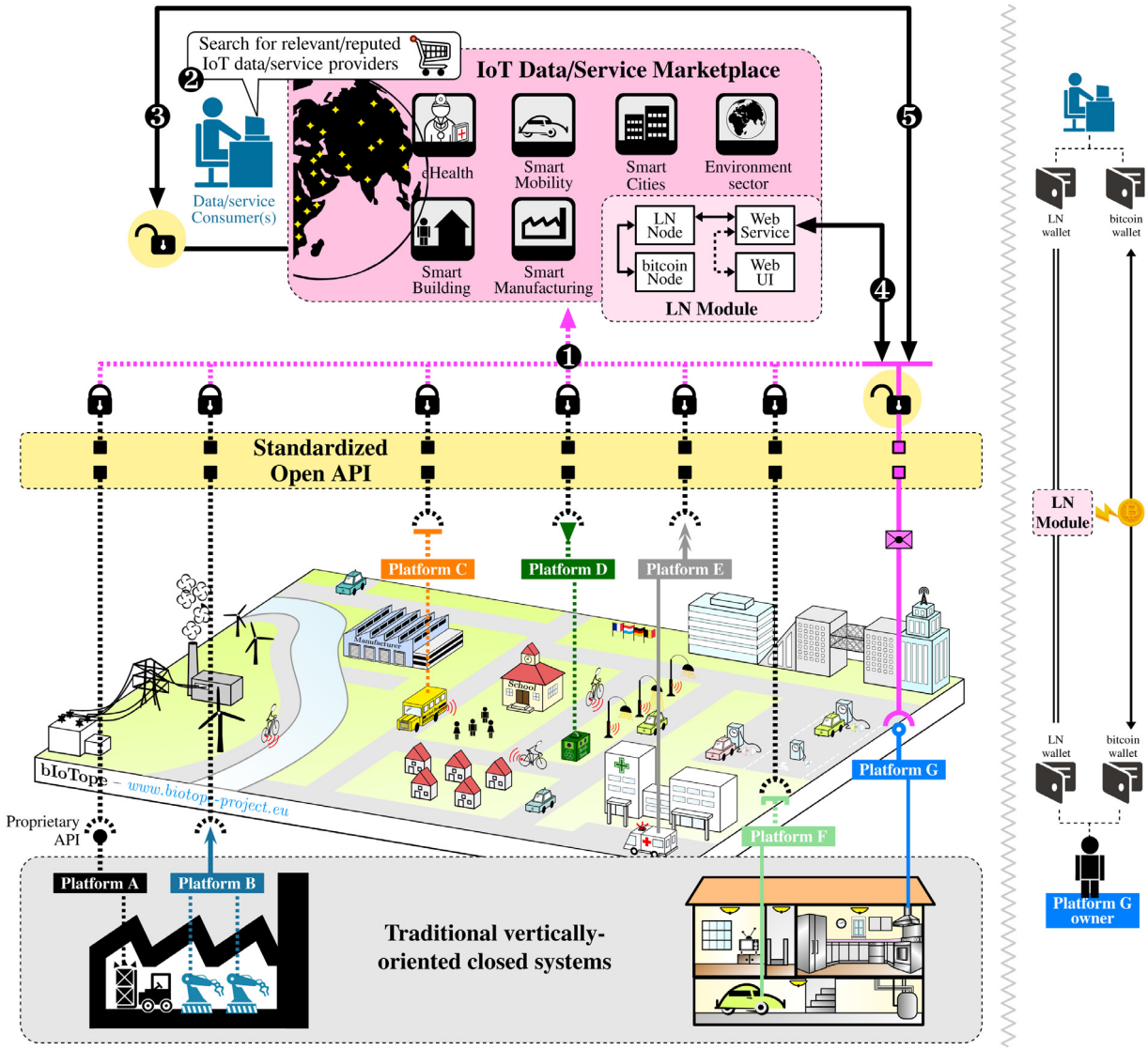


Fig. 5. High-level overview of how LN could be integrated into an open IoT ecosystem & underlying digital marketplace.

2.4. Wrap-up

As a concluding section, the literature review presented in Section 2.1 (see Table 1) has shown that a number of papers deal with the integration of blockchain with IoT systems and/or platforms. However, at this date, most of the papers focus on defining smart contract logics for a given IoT application, but too rarely tackle the micro-billing/payment problem in large-scale IoT ecosystems. Furthermore, no study has ever proposed an algorithm seeking to minimize transaction fees in off-chain platforms, which is a key contribution of our research.

The comparison analysis previously presented has evidenced that LN is a serious candidate to achieve efficient micropayment in IoT settings. Given this, we introduce in Section 3 a framework for integrating LN with an existing open IoT ecosystem, following which the algorithm for payment channel fee reduction is detailed.

3. LN-based micropayment framework in IoT ecosystems

A brief introduction of Lightning Network (LN) is given in Section 3.1. In Section 3.2, we present the framework proposed for integrating LN into the open IoT ecosystem developed in the bIoTope H2020 project [5,62], although this framework could be generalized to any other off-chain-like technology. Finally, we present in Section 3.3 the novel algorithm aiming to optimize the closing/opening process of LN payment channels in order to reduce the overall transaction fee.

3.1. Introduction to LN

LN was originally proposed in 2016 and has since seen an increasing interest from the research community active, leading to the release of the first stable version in 2018. LN is built on top of bitcoin, aiming to solve the issue of bitcoin scaling and instant micropayments. To this end, as a first step, LN performs transactions between two parties/users away from the main blockchain, allowing parties/users to endlessly shift the funds between themselves, and in a near instantaneous way, without having to continuously update/synchronize with the main blockchain. This highly contributes to increase transaction speed and scalability, while reducing transaction/traffic load and associated fees on the main blockchain (bitcoin in this case). To achieve this, LN relies on a payment channel network - *set up on top of bitcoin* - that enables the opening and closing of channels. The operational cycle of a payment channel in LN consists of the following steps:

1. **channel funding** enables the opening of a channel by broadcasting a funding transaction to the main chain; once validated, end-user balances are set up;
2. **payment execution** is made by sending a new commitment transaction reflecting the new balances;
3. **channel closing** is done when one of the two parties wants to close the channel, resulting in sending the last updated commitment transaction to the main chain;
4. **punishment** can be implemented in a contract in a way that one channel party can keep all channel-related funds if the second party misbehaves;
5. **unbalancing** exists when payments of a channel are made in a single direction or if the balance of one party reaches zero. In such a case, the transaction cannot be finalized;
6. **multihop payment** is also a key feature of LN in order to enable payments between parties that do not have a 'direct' channel between them. Multihop payment is done via a contract called Hashed Timelock Contract (HTLC) [63].

Although LN is still in its infancy, applications already exist such as MOON.[10] for shopping or LN.PIZZA to order pizza[11] Let us note that this paper does not attempt to change or improve the set of mechanisms underlying the above-described LN's operational cycle, but rather to propose an additional module for both (i) integrating it into an existing IoT ecosystem, and (ii) optimizing the closing/opening process of LN payment channels in order to reduce the overall transaction fee. This additional module is presented in the next section.

3.2. Architectural framework for LN integration into the bIoTope ecosystem

First and foremost, it is important to understand what an open IoT ecosystem is aimed at, what it consists of, and what architectural design choices have been made in the bIoTope H2020 project. An important prerequisite for any successful open IoT ecosystem is to create a solid foundation, both technologically and economically viable, to ensure its take up by end-users. To this end, appropriate building blocks to efficiently find, share and compose distributed and heterogeneous data sources in and across platforms must be set up. Such building blocks have been summarized in Fig. 5. First, it is important to leverage the available vertically-oriented platforms and cloud endpoints through open and standardized APIs, as thoroughly discussed in [2]. Second, IoT stakeholders must be provided with the necessary tools and support to help (i) data owners to select what data/service items they want to make available/visible to the user base engaged with the IoT ecosystem (*cf.*, ❶ in Fig. 5), and (ii) data consumers to search, trade and access valuable IoT data/service items (*cf.*, ❷). While the first stage (*cf.*, ❶) has been detailed in [5, 62], the integration of LN with the bIoTope ecosystem has ever been done so far. Such an integration is presented hereinafter.

A payment module, referred to as "LN module" in Fig. 5, has been designed, which consists of four components:

- *bitcoin node:* it connects with the bitcoin network that serves as the backbone of our payment system. This node is necessary to operate a LN wallet and support the channel opening/closing process;
- *LN node:* it implements the LN logic, among other things the (i) opening and closing of payment channels between peer systems; (ii) token generation; (iii) payment confirmation. In bIoTope, this node serves both as wallet and payment hub at the marketplace level;

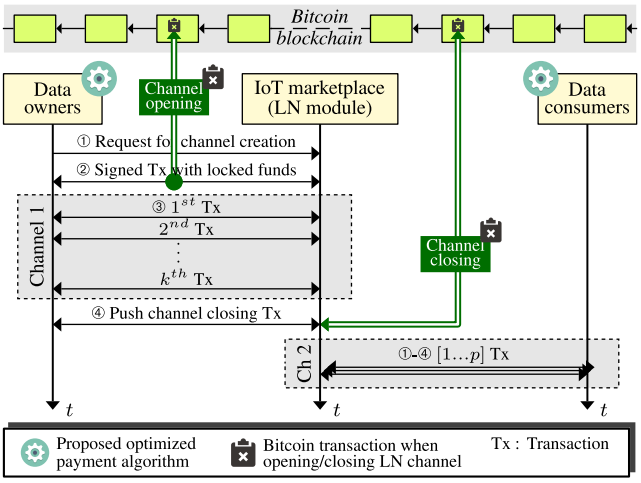


Fig. 6. Sequence of exchanges using LN channels in an IoT ecosystem marketplace.

- *Web-service:* it exposes the API to manage the token generation at the marketplace level, and the validation of payments depending on the token validity;
- *Web UI:* front-end that allows data-consumers to interact with the back-end system during payment operations.

Fig. 5 provides a high-level overview of both how the LN module is integrated into the bIoTope ecosystem and how it interacts with the different ecosystem stakeholders and components, spanning from the discovery of IoT data/service items to their purchase and access (*cf.*, ❷ to ❺). More specifically, any data-consumer who has beforehand (i) registered to the IoT marketplace; (ii) created a LN wallet; and (iii) discovered (non-free) IoT data/service items, can proceed to the payment for being granted with access to the selected items. Given the example in Fig. 5 (i.e., data consumer wants to access data/service items owned by "Platform G", *cf.* ❸), the marketplace requests an LN-based invoice token – *containing information needed for payment* – from the LN module. Once the payment has been confirmed (❹), the user can proceed to calling/accessing the purchased data/service using the appropriate URL (❺). At each API call, the IoT gateway requests the LN module (❹) for verifying the token validity (e.g., checking whether the data consumer paid for enough API calls).

As illustrated in Fig. 5, the LN module handles the money transfer between the LN and bitcoin chains. In order to better understand this process, Fig. 6 provides a detailed version of the message exchange between the LN module (IoT marketplace), the bitcoin blockchain, and the data owner/consumer. The LN module, or the underlying LN node to be more precise, is in charge of creating channels between data consumers and owners, but also handling the routing of payments and associated data in case more than one marketplace platforms would cooperate. A request for channel creation is first sent to the bitcoin node, after which the channel's fund is locked if, and only if, the bitcoin blockchain validates the associated transaction (*cf.*, ② in Fig. 6). Once the channel is opened, data owners and consumers can perform as many micropayments as necessary with peers who have, at least, one opened channel (*cf.*, ③). In the example given in Fig. 6, the LN node takes care of routing micropayments through channels 1 and 2 respectively. Once the data owner, or consumer, wants to close the channel for releasing the associated funds (*cf.*, ④), the LN node sends a notification to the bitcoin node in order to submit the bitcoin transaction to the public blockchain. Channel

10 https://paywithmoon.com, last access Dec. 2019.
11 https://ln.pizza, last access Dec. 2019.

Table 2
Variable & function description.

Variable/function	Description
$ch_{i,j}$	Existing channel between user i and hub j
Ch	Set of channels $ch_{i,j}$
$\ddot{\mathbb{B}}^{open}_{ch_{i,j}}$, $\ddot{\mathbb{B}}^{close}_{ch_{i,j}}$	Cost paid to respectively open/close channel $ch_{i,j}$
$\ddot{\mathbb{B}}_t$	bitcoin fee at time t
`closeChannel(`$ch_{i,j}$`)`	Function call to close channel $ch_{i,j}$
`openNewChannel(`i, j`)`	Function call to create a channel between user i and hub j
`computeCost(`$ch_{i,j}$`)`	Function call to compute the cost of channel $ch_{i,j}$ (i.e., sum of bitcoin fees paid to open/close $ch_{i,j}$)

associated funds are then unlocked upon successful completion of the public bitcoin transaction. This figure emphasizes the possibility of carrying out a near infinite number of micropayments within the channel, denoted by k^{th} *Tx* in Fig. 6.

At this stage, it should be noted that various aspects could be improved in LN, spanning from the routing strategy of transactions between different payment channels, to the optimization of the opening/closing of channels to reduce the total transaction fee. In the next section, we do propose an algorithm aiming at reducing the overall transaction fee.

3.3. LN channel optimization algorithm

Minimizing transaction fees over time implies finding a trade-off between releasing the channel-related fund when needed/desired, while being cost-effective when opening/closing the channel(s). To do so, we propose a novel algorithm (see Algorithm 1) which is run at the data owner/consumer side in a periodical manner (i.e., interval of time based on which the data owner/consumer wants to retrieve his/her fund, e.g., on a daily or weekly basis). In other words, the digital marketplace and LN module never take part to the channel closing decision-making process.

Overall, the algorithm periodically checks for a given channel $ch_{i,j}$ whether the current bitcoin fee at time t is (or not) higher than fee at $t-1$ (*cf.*, Table 2 for more details about each variable/function used in Algorithm 1). Considering the fee volatility/inflation, we make the assumption that it is better to close a given channel as soon as fees start to increase. If so, the channel is automatically closed and a new one opened. Algorithm 1 finally returns the overall cost of all channels $\in Ch$, which corresponds to the sum of the bitcoin fees paid for opening and closing a given channel $ch_{i,j}$ (i.e., $\ddot{\mathbb{B}}^{open}_{ch_{i,j}} + \ddot{\mathbb{B}}^{close}_{ch_{i,j}}$).

As will be discussed in Section 4, the proposed algorithm could be more fine-tuned by adapting some of the conditions based on which decision to keep opened/closed a channel is made. For example, such a decision could depend on the amount of bitcoins available at the data owner/consumer side, or still the amount of bitcoin locked in a given set of channels. Nonetheless, such parameters have not yet been taken into consideration in the current version of the algorithm.

4. Experimental results

A set of experiments have been carried out with a twofold objective: (i) to demonstrate the practicability of the proposed LN-based micropayment framework in the context of the bIoTope ecosystem (presented in Section 4.1) and; (ii) to show that the proposed channel optimization algorithm contributes to reduce the transaction fee cost (presented in Section 4.2).

Data: Ch;
Result: $\ddot{\mathbb{B}}_{ch_{i,j}}$;
$\ddot{\mathbb{B}}_{t-1} = \ddot{\mathbb{B}}^{open}_{ch_{i,j}}$;
begin
  Periodically
    $\ddot{\mathbb{B}}_t \longleftarrow$ `update(`$\ddot{\mathbb{B}}$`);` `// Latest bitcoin's fee`
    foreach $ch_{i,j} \in Ch$ **do**
      if $\ddot{\mathbb{B}}_t - \ddot{\mathbb{B}}_{t-1} \geq 0$ **then**
        `closeChannel(`$ch_{i,j}$`);`
        $\ddot{\mathbb{B}}_{ch_{i,j}} \longleftarrow$ `computeCost(`$ch_{i,j}$`);`
        $ch_{i,j} \longleftarrow$ `openNewChannel(`i, j`);`
      end
      $\ddot{\mathbb{B}}_{t-1} = \ddot{\mathbb{B}}_t$;
    end
  end
end

Algorithm 1: LN channel optimization run by user i

4.1. LN-based micropayment in bIoTope

As part of the bIoTope project, a digital (IoT) marketplace called IoTBnB,[12] standing for "IoT service puBlication and Billing", has been developed to ease data trading between data owners and consumers. The LN module described in Section 3 has been developed and integrated with IoTBnB. Fig. 7 provides an in-depth overview – *in the form of a sequence diagram* – of how this module interacts with the different components and stakeholders of the ecosystem, along with screenshots of the IoTBnB web interface (note that numbering ❶-❽ used in the sequence diagram corresponds to ones referred to in the different screenshots).

First, the end-user – *referred to as "Consumer" in Fig. 7* – can search for specific IoT data/service items. This can be done either using the web interface (see ❶-❷) or the corresponding REST API(s). In the scenario given in Fig. 7, the search is made using the keyword `Parking facilities Brussels` (*cf.*, web interface ❶). For the purposes of this example, the corresponding REST API request message, which is designed based on the O-MI/O-DF standards, is given in Fig. 8 where: (i) O-DF is defined as a simple ontology, specified using XML Schema, which is generic enough for representing "any" object and information that is needed for information exchange in the IoT, and (ii) O-MI is specified at the communication level, enabling peer-to-peer communications between O-MI nodes/devices and supporting a number of messaging operations including subscription mechanisms (e.g., event- or interval-based subscription) [2,64]. In the request example given in Fig. 8, the `searchServices` function is called (using an O-MI read request), taking as input parameters the following ones: *(i) price:* to search for services depending on a price range; *(ii) type:* to search for services depending on what they refer to (e.g. mobility, monitoring, smart home-related services); *(iii) reputation:* to search for services depending on their reputation (assuming the availability of a data/service quality-rating functionality at the marketplace level); *(iv) GeoCoordinate:* to search for services depending on a given geographical area. While in the following we showcase the practicability of our framework through web interface screenshots, note that all the presented steps could be achieved in a similar way using the IoTBnB REST APIs.

Assuming that the end-user has identified and selected/added one or more data/service items to her/his cart (*cf.*, ❷), she/he

[12] http://iotbnb.jeremy-robert.fr, last accessed May 2019.

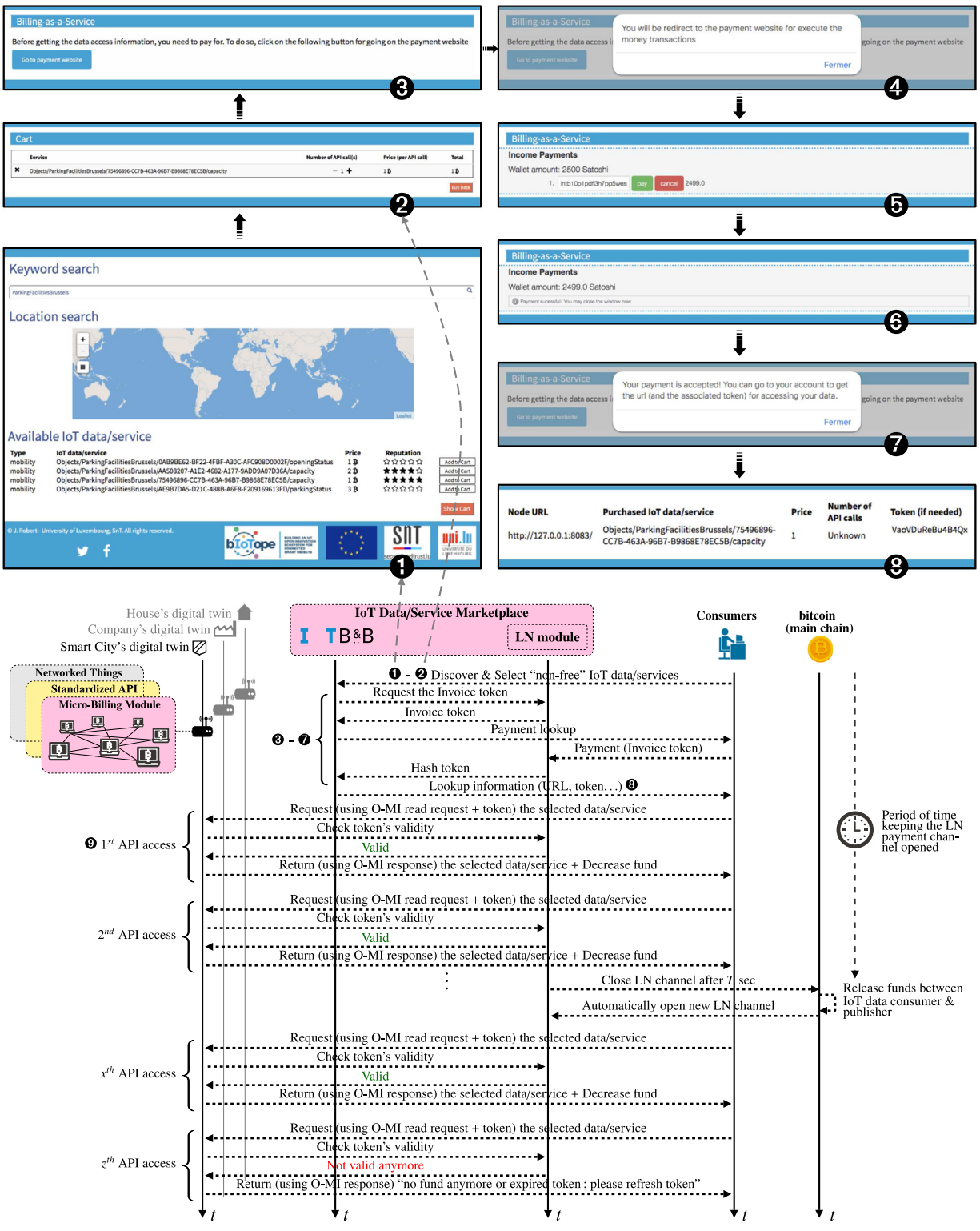


Fig. 7. Sequence diagram and associated web interfaces highlighting the LN-based micropayment functioning in bIoTope.

must pay for accessing the underlying data/service resource (*cf.*, ❸). Although the payment model could differ depending on the digital marketplace, the model considered in IoTBnB is based on the pay-as-you-go API call model. When proceeding to the payment, IoTBnB redirects the end-user to the *LN module* (*cf.*, ❹ in Fig. 7). Assuming that the user has beforehand filled out her/his profile (wallet-related address, *etc.*), the LN module retrieves all the necessary information to proceed to the payment (e.g., the wallet balance, as shown in ❺). Given the balance, the payment is then performed (*cf.*, ❻), thus resulting in a completion notification (*cf.*, ❼). Upon successful payment completion, the end-user is provided with an URL and a token (*cf.*, ❽) that allow her/him to access the purchased IoT data/service in a peer-to-peer manner on the corresponding (remote) IoT gateway. What is important to understand here is that IoTBnB does not collect/store any data but only the data/service description (i.e., metadata). In other


```
<omiEnvelope xmlns="http://www.opengroup.org/xsd/omi/1.0/" version="1.0" ttl="0">
  <call msgformat="odf">
    <msg>
      <Objects xmlns="http://www.opengroup.org/xsd/odf/1.0/">
        <Object>
          <id>Service</id>
          <InfoItem name="searchServices">
            <value type="odf">
              <Objects>
                <Object>
                  <id>MyParameters</id>
                  <InfoItem name="price">
                    <value type="xs:String">0</value>
                  </InfoItem>
                  <InfoItem name="type">
                    <value type="xs:String">all</value>
                  </InfoItem>
                  <InfoItem name="reputation">
                    <value type="xs:String">all</value>
                  </InfoItem>
                  <Object type="schema:GeoCoordinates">
                    <id>geo</id>
                    <InfoItem name="latitude">
                      <value type="xs:string">60.187317</value>
                    </InfoItem>
                    <InfoItem name="longitude">
                      <value type="xs:String">24.821929</value>
                    </InfoItem>
                    <InfoItem name="radius">
                      <value type="xs:String">100</value>
                    </InfoItem>
                  </Object>
                </Object>
              </Objects>
            </value>
          </InfoItem>
        </Object>
      </Objects>
    </msg>
  </call>
</omiEnvelope>
```

Fig. 8. IoTBnB standardized REST API to request for existing IoT data/services in a given geographical area.

words, IoTBnB is only aimed at providing end-users with the necessary information and access rights to access, in an ad-hoc manner, specific data/service items on the corresponding remote IoT gateway(s), as illustrated through the *"1st API access"* phase in Fig. 7 (*cf.*, ❾). At each API call, the IoT gateway therefore checks with IoTBnB the token validity. If valid, the gateway returns the requested data/service. After a given period of time, denoted T in Fig. 7, the LN channel is closed by the LN module, resulting in the release of the funds between the data consumer and publisher. Note that the channel closing process is not dependent on whether the end-user is still granted access to the purchased data/service, but it is intrinsically linked to the LN functioning. As a consequence, to make the process fully transparent for end-users, a new channel is automatically opened after its closing. As highlighted in Fig. 7, the end-user can keep accessing/requesting the purchased data/service as long as the token is valid.

Beyond this proof-of-concept, which shows the feasibility of using/integrating LN with the bIoTope ecosystem, it is important to evaluate the overall system performance. The comparison analysis whose presented in Section 2.3.2 has evidenced that LN outperforms bitcoin and Sidechain in terms of throughput, speed and transaction fee. In the next section, we present a second analysis seeking to evaluate how the proposed LN channel optimization algorithm (*cf.*, Section 3.3) performs in terms of transaction fee savings.

4.2. Evaluation of the LN channel optimization algorithm

As was discussed in Section 2.3.2, experiments in our study were performed under Testnet3 over a 1-month period (04/11/2019 to 03/12/2019). As part of our experimental setting, only one LN payment channel denoted by $ch_{i,j}$ was set up and maintained between two end-nodes i and j, which correspond to the data publisher and consumer phones. The closing date of the channel, denoted by t_{close}, is performed on a daily basis (e.g., at 15:00 every day, as depicted in Fig. 9). As part of our experiment, Algorithm 1 is applied considering a closing/opening tolerance period τ (*cf.*, Fig. 9), whose maximum tolerance period is set to $5h$ (i.e., $\tau = 5$). Note that if the condition described in line 6 of Algorithm 1 is not reached at $t_{\text{close}} \pm \tau$, the channel is anyway closed to ensure that the user can still unlock her/his fund on a daily basis. The cost saving resulting from our algorithm was measured for three distinct tolerance periods ($1h$, $3h$ and $5h$), denoted by $\Delta = t_{\text{close}} \pm \tau$.

Fig. 10 presents the cost saving resulting from the three tolerance periods. These experiments consist of the beginning of a Monte-Carlo scenario since a stochastic phenomena exists in the process of fee computation. Indeed, several parameters such as the number of miners at a given time, the computational complexity, the number of addresses involved in the transactions are taken into consideration. The results show that closing the channel at an early or late stage makes it possible to reduce the overall transaction fee and thus save money (between 0 and

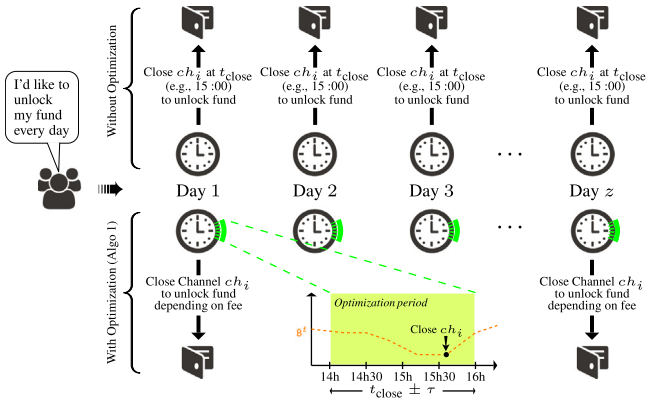


Fig. 9. Logic underlying the proposed LN channel optimization algorithm.

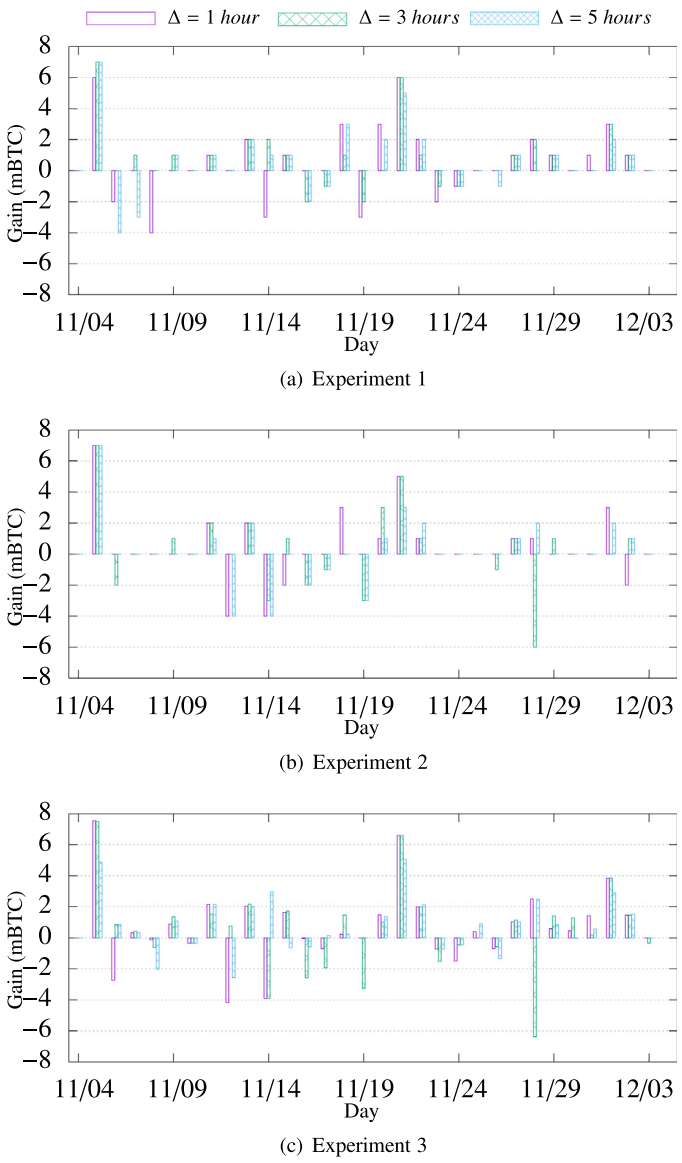


Fig. 10. Cost saving per day of using the LN channel optimization algorithm over a month (Nov. 4 to Dec. 3, 2017).

7.54 mBTC, which is equivalent to 0 and 69.39 € in Aug. 2019). However, it can also be seen that, for some days, the cost saving is negative (up to 6.37 mBTC, equivalent to 0 and 58.62 €). This means that the fees are higher than in the LN solution without optimization, which can be partly explained due to the fact that non predictable fee peaks occurred when only looking at the Δ timeframe (i.e., 1, 3 and 5h), although it has no direct impact on the cost saving, as observed in Fig. 10. However, it can be observed that the (maximum) losses are often lower than the (maximum) gain, therefore leading to money savings when running the algorithm on a long-term basis.

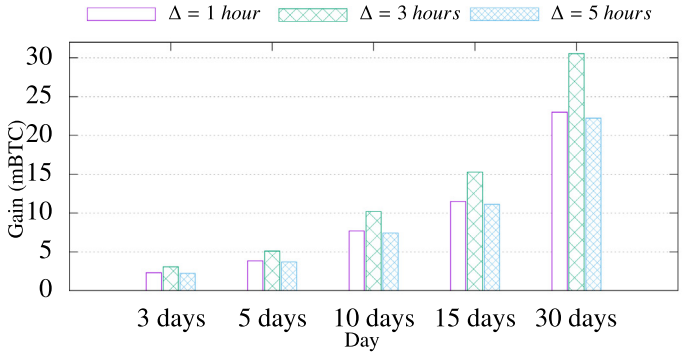
To confirm the above statement (i.e., money is saved when running Algorithm 1 on a long-term basis), we present in Fig. 11 the average cost saving when running the algorithm over 3, 5, 10, 15 and 30 days. The result/finding is clear: the longer the algorithm is run, the higher the cost saving. Indeed, when looking at 30 days, a user can expect to save between 7.4 and 30.55 mBTC (*cf.*, minimum value obtained in Fig. 11(c) for $\Delta = 3$ and maximum value obtained in Fig. 11(a) for $\Delta = 3$), which is equivalent to 68.1 and 281.13 € in Aug. 2019. Beside this finding, it is important to understand that we are dealing with the average cost savings; as a result, it can be possible to lose fees, especially when running the algorithm for 3 or 5 days as observed in our experiments (beyond there are cost savings), whose min/max values are respectively −6.99/11.82 mBTC and −8.13/9.59 mBTC. Having said that, an end-user needs to be aware of the possibility to lose money, in a similar manner as with the game theory, stock exchange, or even life insurance financial product (but with more important fees volatility), but this effect is strongly attenuated over time, as above-discussed.

5. Conclusion, implications, limitations & future research

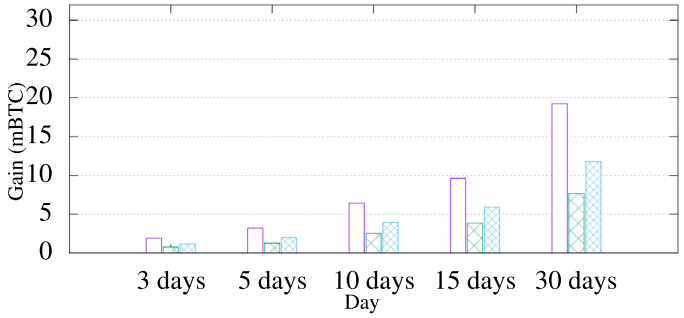
5.1. Conclusion

In today's connected world, a flourishing number of concepts and architectural shifts appeared such as IoT, Big Data and Cloud Computing, which have reshaped the contours of traditional business models. Personal data is increasingly used in business value creation, and can be seen today as the new currency that oils the wheels of the digital economy. There is an increasingly tendency to move from vendor lock-in solutions to open innovation ecosystems with a multifold objective: (i) increase the interoperability between vertically-oriented closed systems; (ii) give citizens back control over of their personal data and simplify the regulatory environment for business; (iii) foster joint capability of collaboration, including collaborative processes for co-creation and co-specialization. This imposes the provision of automatic enforcing mechanisms to guarantee ad-hoc transfer of various types of IoT data and services among various IoT stakeholders, as well as secured near-instantaneous micropayments for data/service access.

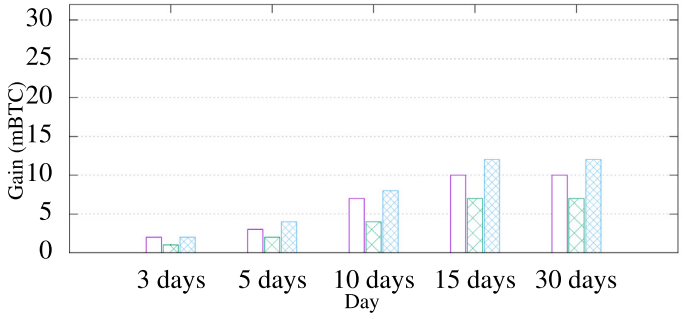
To achieve the above objective, our research is considering "off-chain" blockchain technologies in order to better meet the IoT requirements in terms of privacy, security, throughput, and latency, where traditional on-chain technologies usually fail. In a nutshell, it consists in temporarily moving some transactions off-chain for computation elsewhere, and then returning a summary to the main chain. Within this context, this paper presents a first experimental benchmark analysis to validate this claim, which consists in the comparison of the well-known bitcoin (on-chain) cryptocurrency with two off-chain technologies: Sidechain and Lightning Network (LN). Results show that LN outperforms the two other technologies, and thus proves to be more appropriate for supporting micropayment in large-scale IoT ecosystems in which business transactions may reach 450 billion a day by 2020. In a second phase, we presented the architectural design choices



(a) Experiment 1



(b) Experiment 2



(c) Experiment 3

Fig. 11. Average cost saving of using LN channel optimization for several days (3, 5, 10, 15, 30).

made for integrating LN into an existing open IoT ecosystem, which has been developed as part of the bIoTope H2020 project. In a third phase, we proposed a novel algorithm that aims to optimize the opening/closing of LN payment channels with the overall goal to reduce transaction fees.

Despite showcasing the practicability of our software integration framework together with the digital marketplace underlying the bIoTope ecosystem, we prove that the proposed LN channel optimization algorithm helps to reduce the overall transaction fees and thus achieve savings. Our experiments show that savings are increasing over time, which can lead to increased savings on a long-term basis.

5.2. Implications

This research presents two main theoretical implications. First, it contributes to the literature on blockchain for IoT with a focus on the provision of micropayment transaction services. In this respect, we propose a comparison study between three distinct blockchain technologies, one "on-chain" (bitcoin) and two "off-chain" solutions (Sidechain and LN). This study has put in evidence that LN better meets micropayment requirements in IoT settings. Second, a novel LN payment channel optimization algorithm is proposed, which could be used as a benchmark basis.

Finally, our research also presents a software engineering implication, as the successful integration of the LN technology into an existing IoT ecosystem (and underlying digital marketplace) is showcased. Even if this implication is not that relevant from a scientific viewpoint, we believe that it can prove helpful for blockchain and IoT practitioners.

5.3. Limitations & future research

Several limitations of our research can be pointed out. First, the proposed comparison/benchmark study should be extended in three respects: (i) other off-chain technologies such as the ones investigated by the Trusted IoT Alliance or Enterprise Ethereum Alliance; (ii) the comparison study should be run over a longer period in order to strengthen the analysis results and findings; (iii) the comparison study should cover, to the extent possible, the seven dimensions highlighted in Fig. 2(b) (only three out of the seven dimensions being covered/evaluated in our analysis).

Second, the logic of the proposed LN channel optimization algorithm does not take into consideration bitcoin price and volatility predictions, while could lead to better decision-making about the closing/opening of LN channels over time. In future research work, we plan to consider state-of-the-art bitcoin prediction models to improve the efficiency of our algorithm. Among other models, the ones proposed in [65–68] could be studied.

Third, the proposed integration of such LN framework within the bIoTope ecosystem only relies on self-generated wallets hold by the IoT marketplace (IoTBnB), which acts as a trusted third party and thus raises concerns in terms of privacy and reliability. Furthermore, the framework does not provide any wallet portability provision for transferring wallets from one ecosystem to another [69]. Finally, wallets could be encrypted in future work in order to improve security.

Fourth, one may wonder whether LN should be used for large payments, and/or whether the opening/closing process of a channel should be adapted accordingly (e.g., taking into account the transaction value instead of accounting/closing time). One potential research direction could be the study of a trade-off between different possible parameters (incl., time, transaction value, and potentially others), while taking into consideration end-user preferences.

CRediT authorship contribution statement

Jérémy Robert: Conceptualization, Methodology, Software, Writing - review & editing. **Sylvain Kubler:** Conceptualization, Methodology, Writing - review & editing. **Sankalp Ghatpande:** Investigation, Software, Writing - original draft.

Acknowledgment

The research leading to this publication is supported by the EU's H2020 Programme for research, technological development and demonstration (grant 688203).

Declaration of competing interest

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

References

[1] D. Guinard, V. Trifa, Building the Web of Things: with Examples in Node. Js and Raspberry Pi, Manning Publications Co., 2016.

[2] K. Främling, S. Kubler, A. Buda, Universal messaging standards for the IoT from a lifecycle management perspective, IEEE Internet Things J. 1 (4) (2014) 319–327.

[3] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.

[4] K. Holley, S. Antoun, A. Arsanjani, W.A. Bill Brown, J.F. Costas, C. Cozzi, P. Goyal, S. Iyengar, H. Jamjoom, C. Jensen, J. Laredo, J. Maddison, R. Narain, A. Natarajan, J. Petriuc, K. Ramachandran, R. Ravishankar, R. Reinitz, S. Vaidya, M. Vukovic, The Power of the API Economy – Stimulate Innovation, Increase Productivity, Develop New Channels, and Reach New Markets, IBM Corporate, 2014.

[5] S. Kubler, J. Robert, K. Främling, A. Hefnawy, C. Cherifi, A. Bouras, Open IoT ecosystem for sporting event management, IEEE Access 5 (1) (2017) 7064–7079.

[6] O. Vermesan, J. Bacquet, Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution, River Publishers, 2017.

[7] A. Smedlund, H. Ikävalko, P. Turkama, Firm strategies in open internet of things business ecosystems: framework and case study, in: Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, pp. 1591–1600.

[8] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, in: 19th International Conference on Advanced Communication Technology, IEEE, 2017, pp. 464–467.

[9] R. Yang, F.R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: A survey, some research issues and challenges, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1508–1532.

[10] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun. 136 (2019) 10–29.

[11] M.U.I. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Gener. Comput. Syst. 97 (2019) 512–529.

[12] W. Li, S. Tug, W. Meng, Y. Wang, Designing collaborative blockchained signature-based intrusion detection in IoT environments, Future Gener. Comput. Syst. 96 (2019) 481–489.

[13] H. Si, C. Sun, Y. Li, H. Qiao, L. Shi, IoT information sharing security mechanism based on blockchain technology, Future Gener. Comput. Syst. 101 (2019) 1028–1040.

[14] N. Kolbe, S. Kubler, J. Robert, Y. Le Traon, A. Zaslavsky, Linked vocabulary recommendation tools for internet of things: A survey, ACM Comput. Surv. 51 (6) (2019) 127.

[15] J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Commun. Surv. Tutor. (2019) 1–38.

[16] J. Al-Jaroodi, N. Mohamed, Blockchain in industries: A survey, IEEE Access 7 (2019) 36500–36515.

[17] L.W. Cong, Z. He, Blockchain disruption and smart contracts, Rev. Financ. Stud. 32 (5) (2019) 1754–1797.

[18] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: 2016 IEEE Symposium on Security and Privacy, 2016, pp. 839–858.

[19] J.S. Czepluch, N.Z. Lollike, S.O. Malone, The Use of Block Chain Technology in Different Application Domains, The IT University of Copenhagen, Copenhagen, 2015.

[20] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[21] J. Eberhardt, S. Tai, On or off the blockchain? Insights on off-chaining computation and data, in: European Conference on Service-Oriented and Cloud Computing, 2017, pp. 3–15.

[22] M. Miraz, D.C. Donald, Atomic cross-chain swaps: Development, trajectory and potential of non-monetary digital token swap facilities, Ann. Emerg. Technol. Comput. 3 (2019).

[23] J. Poon, T. Dryja, The Bitcoin Lightning Network: Scalable off-chain instant payments, Technical Report (draft), 2015.

[24] D. Raggett, The web of things: Challenges and opportunities, Computer (5) (2015) 26–32.

[25] AIOTI, Alliance for Internet of Things Innovation (AIOTI), European Commission, 2015.

[26] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, J. Song, Toward a standardized common M2M service layer platform: Introduction to oneM2M, IEEE Wirel. Commun. 21 (3) (2014) 20–26.

[27] R. Minerva, Towards a definition of the internet of things, IEEE Internet Initiative (2015).

[28] S. Rhee, Catalyzing the Internet of Things and smart cities: Global city teams challenge, in: 1st International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE) in Partnership with Global City Teams Challenge, 2016, pp. 1–4.

[29] C. Perera, Sensing as a service (S 2 aaS): Buying and selling IoT data, Newsletter (2016).

[30] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, IEEE Commun. Mag. 55 (1) (2017) 26–33.

[31] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Gener. Comput. Syst. 56 (2016) 684–700.

[32] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[33] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, M. Imran, Securing IoTs in distributed blockchain: Analysis, requirements and open issues, Future Gener. Comput. Syst. 100 (2019) 325–343.

[34] B. Seok, J. Park, J.H. Park, A lightweight hash-based blockchain architecture for industrial IoT, Appl. Sci. 9 (18) (2019) 3740.

[35] Z. Hao, R. Ji, Q. Li, Fastpay: A secure fast payment method for edge-IoT platforms using blockchain, in: 2018 IEEE/ACM Symposium on Edge Computing (SEC), IEEE, 2018, pp. 410–415.

[36] M. Green, I. Miers, Bolt: Anonymous payment channels for decentralized currencies, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2017, pp. 473–489.

[37] A. Pouraghily, T. Wolf, A lightweight payment verification protocol for blockchain transactions on IoT devices, in: 2019 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2019, pp. 617–623.

[38] Y.P. Tsang, K.L. Choy, C.H. Wu, G.T.S. Ho, H.Y. Lam, Blockchain-driven IoT for food traceability with an integrated consensus mechanism, IEEE Access 7 (2019) 129000–129017.

[39] T.M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, P. Fraga-Lamas, Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care, Sensors 19 (15) (2019) 3319.

[40] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto, J.M. Corchado, Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management, Inf. Fusion 49 (2019) 227–239.

[41] K. Fan, Z. Bao, M. Liu, A.V. Vasilakos, W. Shi, Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT, Future Gener. Comput. Syst. (2019).

[42] S.K. Singh, S. Rathore, J.H. Park, Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence, Future Gener. Comput. Syst. (2019).

[43] P. Shi, H. Wang, S. Yang, C. Chen, W. Yang, Blockchain-based trusted data sharing among trusted stakeholders in IoT, Softw. - Pract. Exp. (2019).

[44] P. Danzi, A.E. Kalør, Č. Stefanović, P. Popovski, Delay and communication tradeoffs for blockchain systems with lightweight IoT clients, IEEE Internet Things J. 6 (2) (2019) 2354–2365.

[45] K. Fan, S. Sun, Z. Yan, Q. Pan, H. Li, Y. Yang, A blockchain-based clock synchronization scheme in IoT, Future Gener. Comput. Syst. 101 (2019) 524–533.

[46] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, Fairaccess: a new blockchain-based access control framework for the internet of things, Secur. Commun. Netw. 9 (18) (2016) 5943–5964.

[47] J. Chen, Flowchain: A distributed ledger designed for peer-to-peer iot networks and real-time data transactions, in: Proceedings of the 2nd International Workshop on Linked Data and Distributed Ledgers (LDDL2), 2017.

[48] E. Reilly, M. Maloney, M. Siegel, G. Falco, A smart city IoT integrity-first communication protocol via an ethereum blockchain light client, in: Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco, 2019, pp. 15–19.

[49] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg, Tumblebit: An untrusted bitcoin-compatible anonymous payment hub, in: Network and Distributed System Security Symposium, 2017.

[50] H. Si, C. Sun, Y. Li, H. Qiao, L. Shi, IoT information sharing security mechanism based on blockchain technology, Future Gener. Comput. Syst. 101 (2019) 1028–1040.

[51] M.U. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Gener. Comput. Syst. 97 (2019) 512–529.

[52] S.T. Ali, D. Clarke, P. McCorry, The nuts and bolts of micropayments: a survey, 2017, arXiv:1710.02964.
[53] M. Jain, S. Lal, A. Mathuria, Peer2peer (P2P) micropayments: A survey and critical analysis, DA-IICT, Gandhinagar, 2008.
[54] J.-S. Coron, J.B. Nielsen, Advances in cryptology, in: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT, Vol. 10211, Springer, Paris, France, 2017.
[55] S. Ukustov, Micropayments for the Internet of Things, Tech. rep., Machinomy, 2016.
[56] J. Wettinger, U. Breitenbücher, F. Leymann, Any2API – Automated APIfication, in: 5th International Conference on Cloud Computing and Service Science, 2015, pp. 475–486.
[57] M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication, in: International Workshop on Open Problems in Network Security, Springer, 2015, pp. 112–125.
[58] P. McCorry, M. Möser, S.F. Shahandasti, F. Hao, Towards bitcoin payment networks, in: Australasian Conference on Information Security and Privacy, Springer, 2016, pp. 57–76.
[59] R. McMillan, The inside story of Mt. Gox, Bitcoin's $460 million disaster, Wired. March 3 (2014).
[60] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, P. Wuille, Enabling blockchain innovations with pegged Sidechains, https://blockstream.com/sidechains.pdf.
[61] J. Gantz, D. Reinsel, Extracting value from chaos, IDC IVIEW. Sponsored by EMC Corporation, 2011.
[62] J. Robert, S. Kubler, N. Kolbe, A. Cerioni, E. Gastaud, K. Främling, Open IoT ecosystem for enhanced interoperability in smart cities – Example of Métropole De Lyon, Sensors 17 (12) (2017) 1–21.
[63] M. Conoscenti, A. Vetrò, J.C. De Martin, Hubs, rebalancing and service providers in the lightning network, IEEE Access 7 (2019) 132828–132840.
[64] S. Kubler, K. Främling, A. Buda, A standardized approach to deal with firewall and mobility policies in the IoT, Pervasive Mob. Comput. 20 (2015) 100–114.
[65] M. Balcilar, E. Bouri, R. Gupta, D. Roubaud, Can volume predict bitcoin returns and volatility? A quantiles-based approach, Econ. Model. 64 (2017) 74–81.
[66] N.I. Indera, I.M. Yassin, A. Zabidi, Z.I. Rizman, Non-linear autoregressive with exogeneous input (NARX) bitcoin price prediction model using PSO-optimized parameters and moving average technical indicators, J. Fundam. Appl. Sci. 9 (3S) (2017) 791–808.
[67] L. Pichl, T. Kaizoji, Volatility analysis of bitcoin, Quant. Finance Econ. 1 (2017) 474–485.
[68] S. McNally, J. Roche, S. Caton, Predicting the price of bitcoin using machine learning, in: 2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), IEEE, 2018, pp. 339–343.
[69] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, The right to data portability in the GDPR: Towards user-centric interoperability of digital services, Computer Law & Security Review 34 (2) (2018) 193–203.

Jérémy Robert is a Research Associate at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) in the University of Luxembourg. He received his M.Sc. degree and Ph.D. degree in Computer Science and Engineering from the University of Lorraine (France) respectively in 2009 and 2012. He has broad expertise in industrial and embedded networks since his PhD research focused on the use of switched Ethernet embedded in the future space launchers. Since 2015, his work is more about heterogeneous data communication challenges in the Internet of Things (IoT) and the implementation of messaging services and high-level data formats. As the major research work was conducted in collaboration with the industry, these skills could be therefore applied in the area of the smart factory (industry 4.0), smart cities.

Sylvain Kubler is Associate Professor at the Research Center for Automatic Control of Nancy in the Université de Lorraine (France). Prior to that, he was Research associate at the Interdisciplinary Centre for Security, Reliability and Trust in the University of Luxembourg (2015–2017) and at Aalto University in Computer Science (2013–2015). He received his M.Sc. degree and Ph.D. degree in Computer Science and Engineering from the Université de Lorraine (France) respectively in 2009 and 2012. He was awarded the best Thesis in Automatic Control from the IFAC French Workgroup GdR MACS/Club EEA. He has a leading role in the bIoTope H2020 project (Building an IoT OPen innovation Ecosystem for connected smart objects), which is a 9.6M project involving 21 partners. He has broad expertise in Internet of Things, Networking, Semantic Web, Decision Support Systems, and Fuzzy Logic.

Sankalp Ghatpande is R&D Engineer with position of Research Associate at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) in the University of Luxembourg. He received his M.S degree from University of Luxembourg in 2016. Since 2016, he has worked in industry and academic R&D projects, national and international, as Engineer focused on Blockchain, IoT and Cryptography. He has also been active in multiple volunteering projects involving implementations of specific software(s), code-analysis and multiple open source projects. Recently, he has been involved in data analysis and machine learning project within the financial domain with industrial partner.