BALAdIN for blockchain-based 5G networks

Vincent Messié, Gaël Fromentoux, Xavier Marjou, Nathalie Labidurie

BALAdIN for blockchain-based 5G networks

Vincent Messié*, Gaël Fromentoux**, Xavier Marjou** and Nathalie Labidurie Omnes**
*IMT Atlantique
655 Avenue du Technopôle
29 280 Plouzané
**Orange Labs Lannion
2 avenue Pierre Marzin
22 300 Lannion
vincent.messie@imt-atlantique.net; nathalie.labidurie@orange.com

***Abstract*— In this article, we highlight a novel solution for densifying 5G access networks. Taking benefits from local actors and prosumers, our proposal allows offering a better connectivity to end-users in a model involving network operators and a crowd of local actors. We show that building a multi-actors and densified access network infrastructure has become possible in a distributed way. Incumbent actors with a large footprint act as trusted partners securing the infrastructure and providing guarantees, while the crowd of local actors deploys multiple access points and are rewarded for their contribution. Rewarding is possible thanks to a distributed Bandwidth & Identity ledger along with a Proof of Bandwidth (PoB) mechanism. This article presents the main principles of this new connectivity platform, BALAdIN (Bandwidth Ledger AccountIng Networks), which relies on a consortium blockchain with access control mechanisms removing communitarian Wifi and *ad hoc* networks drawbacks. Indeed, combining distributed ledgers and edge networks allows local actors to cooperate with trusted parties, which leverages the full potential of multi-actors access networks.**

Keywords—blockchain; access network; edge; ledger;

I. INTRODUCTION

Deploying dense 5G access networks is soon going to be a burden for network operators, for this represents huge investments. Why not thus rely on crowd deployment, with multiple local actors cooperating to improve the edge connectivity? Our proposal is to federate edge connectivity resources on a handful of platforms. Confidence being crucial for such deployment, the involvement of network operators acting as trusted actors linked to a large customer basis is essential.

Yet the large customer basis is not sufficient. The local actors we are targeting at include for example shop owners or stadium tenants. Most of them represent very small companies that do not have the ability to develop network skills. Moreover, there is currently no coordination between the deployed access points, making the emergence of this type of model impossible.

In the meantime, alternative companies such as Helium [1] or Ammbr [2] have put forward disruptive blockchain-based solutions. Nevertheless their success requires a large adherence to make a breakthrough. They are intending to release network access units to build up a fully decentralized, self-sustainable, wireless access network. These community networks would rely upon customized hardware and dedicated consensus methods.

In section II, we present the outcomes of our state-of-the art study starting from Bitcoin up to the most recent advances on network access, and including TOR and Torcoin. Our proposal is then presented in section III. This starts by describing the main principles (III.A) before describing the actors of the system (III.B). We then provide a more detailed description in section IV, including the connection establishment (IV.A), the data traffic flow and accounting (IV.B), the abort process (IV.C) and the hotspot reputation management (IV.D). We finally conclude and discuss open questions in section V.

II. STATE OF THE ART

The Distributed Ledger Technology (DLT) has emerged in the wake of **blockchain** and **Bitcoin,** a cryptographic currency [3]. The true DLT potential is its ability to make a fully-distributed, trustworthy transactional ledger. Indeed, everybody can access such database, and modify its state with the agreement of other peers. However, each transaction is kept, and the transaction history cannot be modified. The Bitcoin ledger relies on a Proof-of-Work (PoW) mechanism to validate transactions and build the chain of blocks, each block being fed with transactions. It is well known that participating nodes, the miners, must spend huge computing resources, wasting astonishing amount of energy to solve the cryptographic puzzle. Other consensus mechanisms are thus currently discussed and deployed such as Proof of Stake (PoS) [4], in which the probability for a peer to mint a block increases with the number of coins he earns. Indeed, his interest for the blockchain to be reliable increases with the number of coins he earns. Furthermore, the minting difficulty depends on the profile of the minting peer. This avoids wasting resources in a PoW consensus. Some implementations exist, such as PPCoin [5].

The **TOR** network [6] is known by the general public as the « darknet ». Indeed, it allows participating nodes to transmit data packets while remaining strictly anonymous. To do so, traffic flows are routed in a path getting through multiple relays (generally 3 relays). Each relay hides the previous one, performs specific treatments and ciphers the result before transferring the resulting packet to the next hop. The

specific treatment involves encapsulating the ciphered data in a new IP packet having the relay as source address and the next hop as destination address. This overlay network is thus open to anyone ready to cope with the induced complexity for the sake of anonymity. As a consequence, the darknet has the reputation of attracting malicious internet users. If anonymity is the main strength of this network, it is also its main weakness: relays cannot be rewarded as they must remain anonymous and so the motivation for providing relay resources is weak. For that matter, the TOR network currently lacks resources.

TOR relies on **Onion encryption** [7]. Let us assume the path between an anonymous end-user and the open Internet is made of several relays: the entry relay, one or more middle relays and an exit relay. Before transmitting data, the anonymous end-users ciphers each packet with the session key of the exit relay then with the session key of each middle relay and finally with the session key of the entry relay. As the packet travels upstream, each relay deciphers the packet with its own session key. In the downstream path packets are ciphered by each relay. Session keys (one for each relay) are generated by the client at initialization, and sent to each relay ciphered with relay's public key. All relays are thus needed to completely unencrypt upstream packets (or encrypt downstream packets), ensuring end-user privacy. Thus privacy increases with the number of relays.

Torcoin [8] is a TOR network topology which uses a blockchain for rewarding relays with coins in order to overcome the TOR lack of resources. All data exchanges remain anonymous: each node, which includes end-users and relays, knows only its neighbors. Unlike TOR, Torcoin relies on a group of trusted servers: the **assignment servers**, responsible for establishing the TOR circuits. They form a consensus group, as they must cooperate to take decisions and ensure Torcoin robustness. They prevent a group of malicious relays to generate minting frames while no traffic has flown. Even if half of the relays were malicious, only one circuit out of 16 would be malicious. Assignment servers control the blockchain: they decide of remuneration, and can remove an entire path if needed.

While Bitcoin relies on a PoW, Torcoin relies on an alternative **Proof-of-Bandwidth (PoB)** mechanism. The consensus is fulfilled by minting frames regularly generated by the end-user. This frame is doing a round-trip along the path. Each relay adds to the frame both ways its digital signature. Such mechanism ensures that the frame has truly performed the roundtrip, and is duly signed thanks to relay signatures. As the minting rate increases linearly with the number of sent packets, relays are rewarded based on the amount of traffic they transfer, and yet their anonymity remains.

In Torcoin, the PoB mechanism is seen as a mean for creating coins. From our point of view, it is above all a way to accurately estimate the amount of traffic transferred by a relay without requiring an external entity to attest this amount. The Torcoin PoB can further be embedded in a P2P application in end-users devices, distributed at the edge of the network. Torcoin is thus a decentralized network, yet not fully distributed as trusted entities are still needed.

Ammbr [2] aims at building "*the world's largest fully decentralized, self-sustainable, wireless mesh network using blockchain technology*". Ammbr will sell access units – first low-cost off the shelf Wi-Fi routers then IoT and cellular embedded modules. Purchasers of these units will be rewarded according to the traffic they route. Actually, a blockchain and token-based model will incentivize and drive supply and demand. Ammbr's unique blockchain model is based on a custom ASIC which performs a hybrid Proof of Elapsed Time (PoET) and Proof of Velocity (PoV) as an energy efficient and high speed consensus method measuring the resources provided. The PoET measures the amount of computing resources actually used, while the PoV is linked to a specific hardware component. This solution allows operators to heterogeneously deploy 5G networks - in a leopard skin like pattern - and rely on small cells to further densify their networks [9]. However it will necessarily rely on operator's backhauls. This foundation is noticeably backed by some African countries and possibly Ethereum co-founders.

Helium [1] aims at leveraging the full potential of wireless network, using a dedicated blockchain and a specialized "Proof of Coverage" consensus method. Such mechanism allows earning money depending of the quality of the offered coverage. The goal of such protocol is to certify that a given frame, send by a Challenger node, has been broadcast to a set of sequential targets. The challenger sends a frame ciphered multiple times. Then such frame could be deciphered only by each target in the correct order. Helium thus provides a fully decentralized wireless network suitable for billions of users, using DLT.

Bubbletone [10] replaces traditional roaming technology with a blockchain solution, starting by the statement that end-users face high roaming charges on mobile data during foreign trips. Their will is to reduce costs by de-intermediating data clearing house actors and improve the performances with a new generation solution. Bubbletone translates the inter-MNOs' agreements into smart contracts to shorten reconciliation delays and to reduce fraud. A consortium of Telecom actors is thus developing this novel solution. The customer journey starts by "Offers" created by network operators for extending their market to travelling end-users. This Offer contains the detailed description of the tariff plan and the profile to be downloaded onto end-user's SIM-card. Then, when a customer arrives to a new country, he can select an Offer of a local mobile operator. A new smart-contract called "Request" is created. All payments between subscribers and operators are made in Global Online Tokens, named GOT. Smart contracts are negotiated between the visited and home network operators, the latter filtering the offers proposals to its customers. Though not designed for the same purpose, Bubbletone is however a seducing solution to consider in our case. A consortium of actors takes advantage of blockchain inspired technologies to smoothen the roaming issues: reduce fraud and simplify the customer journey. Thanks to a renewed and trustable KYC database and an evolving technology, the consortium should be able to enlarge rapidly its portfolio of services.

The Carrier Blockchain Study Group, CBSG [11] is yet another next-generation global cross-carrier blockchain platform and ecosystem set-up by a consortium involving SoftBank, Sprint, Far East Tone and TBCA Soft. It will provide users various services such as secured clearing and settlement, personal authentication and IoT applications. The project aims at connecting carriers' telecommunication backend systems to eliminate late transactions or transaction failures between telecom carriers.

The IETF is further showing a growing interest in this type of decentralized Internet [12]: "*Now is a good time to investigate these systems from an Internet technologies perspective, and to connect the domain expertise in the IRTF and IETF with the distributed systems and decentralized ledgers community.*"

In the massive digitalization perspective boosted by the 5G advent but firstly by societal, economic and technological trends, the consortium model is likely to be the winning one. Most 5G Verticals, such as the Health or Smart city, are seeing such organizations taking place (e.g. 5G openfog). We believe cooperation is also necessary within a consortium sharing access resources to reduce deployment and operating costs. It is also notable that traceability may not be required only for small radio networks, like Helium cover, but also for bigger WAN-type structures.

This paper thus addresses a hot topic, on which many start-up companies are emerging. Nevertheless the solutions put forward by these companies are not self-sufficient: a multi-actor cooperation, as depicted here, is necessary. BALAdIN removes both the technical and economical hurdles that have prevented communitarian Wifi and *ad hoc* networks from getting widely deployed. First, BALAdIN is not restricted to the community of a single operator's customers. Then, it is not plagued by the short outdoor range, the need for a map of spots in nomadic use or the connection restricted to one guest at a time in a family-owned box, which are inherent to Wifi communitarian solutions. *Ad hoc* networks had been well studied in early 2000. However, their limitations explain their lack of success. If blockchain solutions answer the crucial nodes' certification issue, other limitations persist. The scalability is drastically limited by the lack of user-equipment's radio power. The network reliability is doomed by the number of nodes available and by their intermittence since users switch them on/off at will. In this perspective, combining mesh or ad-hoc network with distributed ledgers is much more promising. Efficient mining techniques can now solve the consensus issue, certifying members, nodes, of the network and reward actors. Blockchain solutions as well as smart contracts are now high on the agenda of operators as shown in [9, 10, 13]. Not only does Blockchain enable the collaborations between the involved network operators - including a common reward scheme -, it also provides the mean to set-up a reliable, auditable ledger shared by actors.

III. BALAdIN, OUR SOLUTION

Let us now present BALAdIN, our cooperation model.

A. BALAdIN main principles

Our proposal is then to cooperate with local actors in order to federate multiple network access points. Network operators could indeed establish partnerships with multiple local actors, paying them in return for the local access networks they open to end-users. Thanks to these local actors, both the available bandwidth and the network coverage could be enhanced at once, pragmatically improving the network connectivity for end-users.

This model allows network access offers to line up with new and disruptive consumption models: the network operators offer the connectivity platform and the link to end-users, local actors are rewarded by network operators depending on the traffic they actually convey, and end-users benefit from a better connectivity offer. The network operators further provide a simple authentication system that is required for the system to resist to malicious end-users and provide the needed guarantees.

Let us consider the network operators depicted in Fig. 1. They are associated to colors: Green, Yellow and Blue. Let us assume they are cooperating for this access densification. Thanks to this cooperation, a distributed **Bandwidth & Identity ledger** is built and fed with information provided by each operator. After this initiation process, the ledger is then fed by each participating node. This ledger implements a blockchain with access control. Actually, authentication is based on credentials provided and certified by operators. They are stored within the Bandwidth & Identity ledger.

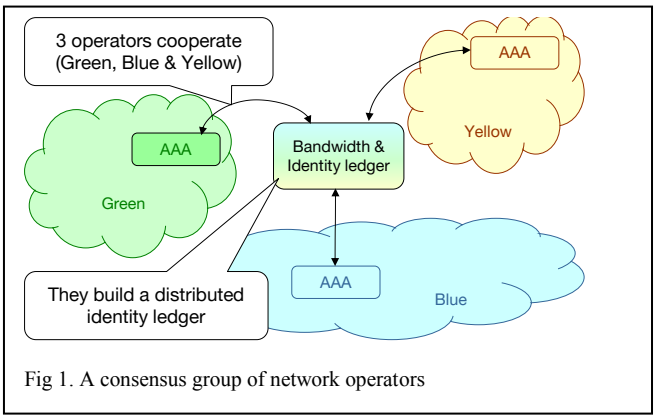

Fig 1. A consensus group of network operators

This Bandwidth & Identity ledger is enriched with measurements of the **reputation** of each end-user and local actor, to promote the best actors and evict suspicious ones. Thus malicious or doubtful end-users and access networks will be refused by the access control, enhancing the overall security of the system. Access control shall take into account subjective criteria provided through evaluation forms, objective criteria based on QoS (Quality of Service) and QoE (Quality of Experience) measurements, as well as means for evaluating offer and the demand.

B. Description of the actors

Our proposal is made of three actors as depicted in Fig. 2.
Local actors (Alice): establish a partnership with a group of network operators and deploy local hotspots that enhance the experience of their clients. They are then rewarded for their contribution to the network access densification, based onthe resources they provide.

End-users (Bob): clients of a network operator, wishing to benefit from the best network connectivity.

Operators (Green, Yellow, Blue): network operators providing access, backhaul and core networks, together with a framework including Authentication, Authorization and Accounting (AAA) for facilitating the integration of local actors in a shared network & IT infrastructure.

In the example presented in Fig. 2, **Alice is a restaurant owner.** Network connectivity was not so good in her restaurant and she contracted with the network operator consortium, with the help of her Green network operator, to deploy a local antenna **relay**, hardware equipment embedding software modules. This equipment offers connectivity to the end-users located under its coverage. Deploying the relay is an investment for Alice, but in return she is paid depending on both reputation and usage.

Bob has just arrived in Paris and wishes to benefit from an extended and low-cost network access, even out of his Yellow network operator's coverage. As his Yellow network operator is a partner of Green network operator in France, he can benefit from the relay deployed by Alice.

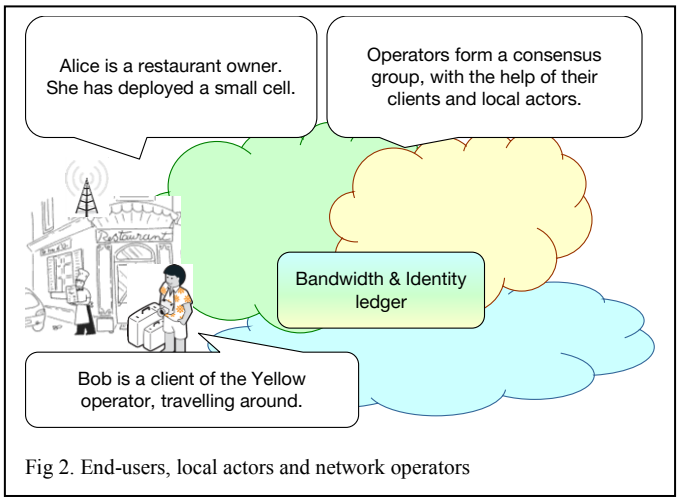

Fig 2. End-users, local actors and network operators

Fig 2 also depicts **the network operators' alliance**: Green, Yellow and Blue. They cooperate with their local actors and end-users, thanks to Proof of Bandwidth. As said before, these operators are responsible for authenticating end-users, local actors and for performing access control.

As Bob attaches to the access network exposed by Alice a circuit is established between Bob's device, Alice's relay and Green's access network. The price, negotiated between Alice, Bob and the Green operator, varies depending on offer and demand as well as on the reputation of the hotspot. How to determine this price is a question to address.

IV. DETAILED DESCRIPTION

A. *Connection establishment*

Bob walks around in Paris while his edge device autonomously searches connectivity resources. As Bob reaches Alice's access network, his device discovers this access network upon other access networks and decides to launch the network attachment process, as depicted on the first step of Fig 3.

At step 2, Alice's relay interacts with the multi-operators Bandwidth & Identity ledger to authenticate Bob.

At step 3, Alice requests the ledger to perform access control for Bob's network attachment. At this step the access may be refused by the ledger for different reasons: for example if Alice's antenna or Bob's edge device are blacklisted by theirs operators, or if Bob's balance is insufficient to honor the contract with Alice.

In other words, by accepting the request, **the Operator consortium and especially the Green operator engages his responsibility towards both Alice and Bob**. In particular, Alice is guaranteed she will be paid for the resources she offers, resources that are provably and securely stored within the Bandwidth and Identity ledger. In our example, we assume Green accepts the incoming request. If this was not the case, Bob would simply look for another antenna to attach to. At step 4, the attachment is spread into the ledger while accepting incoming request at step 5. Alice then answers to Bob at step 6, providing Bob with a connection context including an IP address.

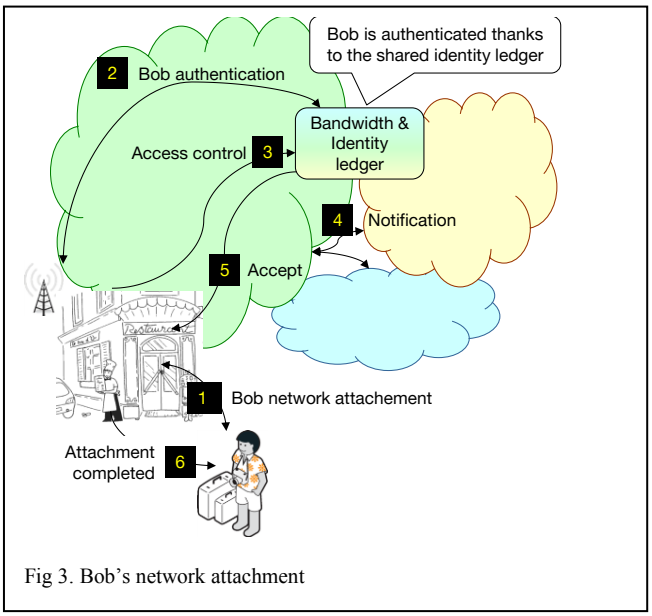

Fig 3. Bob's network attachment

B. *Data traffic flow and accounting*

As Bob uses this connectivity, the packets are counted to estimate the amount of traffic he transmits as depicted on the following Fig 4.

At step 2, Bob generates a minting frame, which works as described in Torcoin [8]. This PoB mechanism measures the traffic flowing through a circuit, enabling to prove the amount of traffic a relay has transferred. The proofs are stored on a distributed Bandwidth & Identity ledger.

At step 5, Bob adds the proof of bandwidth frame to the ledger by performing a light consensus mechanism such as Hyperledger Proof of Elapsed time [14]. The question of which consensus mechanism to use is still open. By doing so, Bob pays the Green operator. This triggers Step 6, where Alice is rewarded by Green for the resources she has offered to Bob. When Bob ends the connection, a new minting frame is launched by his device. The usual end of connection procedure is the following: Bob ends the connection; the Green acknowledges the connection ending to Alice, who in return acknowledges it to Bob. In our opinion, such mechanism is compulsory, for ensuring the transparency of the measure. Indeed, with such mechanism

each actor (relays, operators, end-users) has a crucial role for generating the frame.

With a minting frame generated each megabit, the excepted rate could reach 1 Gigabit per second. Indeed, using a PoET-based ledger would allow 1000 transactions per second [14]. Despite the fact other metrics such as latency or usage are still unknown, as there is no implementation yet, we believe a typical 5G network would thus not be impacted.

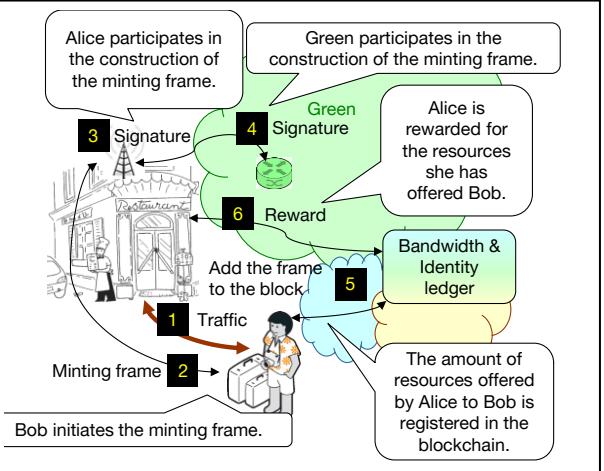

Fig 4. Bob's traffic accounting

C. *Abort*

The connection may abort for different reasons. Indeed, the local hotspot, Alice's relay ends the connection if the expected minting frames are not generated**.** Obviously, relays are not rewarded without minting frames. In addition, the local operator, Green, may also abort the connection by revoking any node rights. For example, if the local hotspot does not meet the expected quality (available bandwidth, latency, reputation, etc.). In all cases, the actor deciding to end the connection launches the abort procedure by sending to the whole path an abort message and kills the connection.

D. *Hotspot Reputation*

While all users of the network participate in the validation, it is the network operators' consortium that manages and shares the reputation of each hotspot upon multiple criteria: rating data collected from end-users, monitoring data collected by agents during the connections as well as the estimation of the supply and demand. The rating of each hotspot is kept up-to-date in the Bandwidth & Identity ledger. It may be upgraded by any network operator based on the feedback it receives from its clients. Based on this rating, each network operator may remove a contract with a local hotspot under its responsibility, temporarily or definitively, thus blacklisting the node on the ledger.

V. CONCLUSION

In this article, we present BALAdIN, a solution combining network edge point of access and distributed ledger. It relies on three different types of actors: the network operator offers the connectivity platform and the link to end-users, local actors deploy new antennas and are rewarded by network operators depending on the traffic they actually convey, and end-users benefit from a better connectivity offer. The role of ordering and executing transactions lies in the hand of the consortium whereas local actors perform the PoB mechanism as a sort of virtual mining. Connectivity metrics are monitored without the need of any trusted party or operators, thus the rewarding mechanism is fully distributed. Hence multiple actors cooperate for densifying the access network, based on crowd deployment. The network operator's presence as trusted parties ensures that for the end-users, required security and quality of experience are provided, as they have the control of reputation and authentication. This also ensures local actors remuneration, and no legal issues for the local actors about providing connection and be rewarded. We further rely on Proof-of-Bandwidth (PoB), an energy-efficient consensus method firstly used by TorCoin. It allows end-users and local actors to participate in the system by an active way, while simplifying accounting. Our solution, BALAdIN, has been patented. Furthermore, we are currently developing a Proof-of-Concept (PoC).

Fairly rewarding each type of actor is crucial for this type of solution to become popular and hence reach a critical mass. The fees, negotiated between end-users, local actors and operators, shall vary depending on offer and demand, on the reputation of each actor as well as on local regulations. A full autonomous and distributed mesh network solution is still foreseeable. However, BALAdIN is compliant with the regulation since operators pay for the frequencies they use and it proposes rewards to users to share their infrastructure with external users.

REFERENCES

[1] A. Haleem, A. Allen, A. Thompson, M. Nijdam, R. Garg, "Helium: A Decentralized Wireless Network", 14 November 2018, http://whitepaper.helium.com/

[2] B. Pang, J. Lanshe, R. Rajagopal, D. Smithand, K. Ghosh, "Ammbr white paper", 15 August 2017, http://ammbr.com/docs/201708/Ammbr_Whitepaper_v1.1_15Aug2017.pdf

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf

[4] BitFury Group, "Proof of Stake versus Proof of Work", 13 September 2015 (version 1.0), *Bitfury*

[5] S. King, S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", 19 August 2012

[6] C. A. Holm Hansen, "Analysis of Client Anonymity in the Tor Network", NTNU Trondheim, June 2015

[7] J. Feigenbaum, A. Johnson,P. Syverson, "A Model of Onion Routing with Provable Anonymity", 11th International Conference on Financial Cryptography and Data Security, Tobago, 2006.

[8] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, "A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays", Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), Amsterdam, 2014

[9] "How do we plan for 5G NR deployments?", November 2018, *Qualcomm,* https://www.qualcomm.com/news/onq/2018/11/27/how-do-we-plan-5g-nr-deployments

[10] Y. Morozov, O. Pravdin and S. Ivanov, "Blockchain in Telecom, White Paper", October 2017, *Bubbletone*

[11] A. Burkitt-Gray, "Sprint, SoftBank and Far EasTone launch blockchain consortium for cross-carrier payments", Global Telecoms Business, 8 September 2017

[12] D. Kutscher and M. Shore, "Decentralized Internet Infrastructure Proposed RG (dinrg)", IETF RG, November 2017

[13] "Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid", GSMA Digital Identity; January 2018

[14] The Linux Foundation, Intel Proof of Ellapsed Time, https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html