Blockchain and Its Impact on Telecom Networks

Rajat Kochhar, Barjinder Kochar, Jatinder Singh, Varun Juyal
Ericsson Global Services India (Pvt.) Ltd.
Gurgaon, India
e-mail: {rajat.kumar.kochhar, barjinder.kochar, jatinder.a.singh, varun.juyal}@ericsson.com

Abstract **- For the last couple of years, Blockchain has been the most talked about technology across a range of industries, e.g., currency markets, banks and financial services, supply chain, logistics, manufacturing, etc. The telecom industry has also shown huge uptake for Blockchain-based solution. Plenty of use cases for telecom networks are already proposed and proof of concepts solutions are available via many vendors, operators, and telecom software companies. Identity management, Fraud prevention, Smart contract, Internet of Things (IoT) Security, Mobile data tokenization and Initial coin offering are some of the use cases which will be offered by telecom operators/companies in the very near future. This paper discusses in detail some of the important use cases and their implementation complexities. This paper also addresses how smaller or startup telecom companies/operators can leverage the Blockchain opportunity and disrupt the markets they are based in.**

Keywords-Blockchain; Consensus Methods; Communication Service Provider; Smart Contracts; Initial Coin Offerings.

I. INTRODUCTION

Blockchain is a decentralized and distributed ledger technology that uses algorithms and strong encryption to record digital transactions or data in a transparent, secure, and anonymous way [1]. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. To put it very simply, Blockchain is a data-structure, like a linked list, where every new block of data is cryptographically linked to its predecessor (Figure. 1). By design, Blockchains are inherently resistant to modification of the data [3].

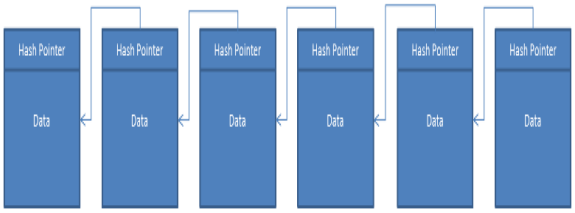

Figure 1. Simple visual representation of Blockchain.

As seen in Figure 1, this block of data has a unique hash which is the address or link to the next block. This chain of blocks is copied to all the peers of the network, making it distributed in nature, resulting in a chain of blocks known as Blockchain. This peer to peer architecture creates data redundancy, but ensures that there is no single point of failure, as shown in Figure 2.

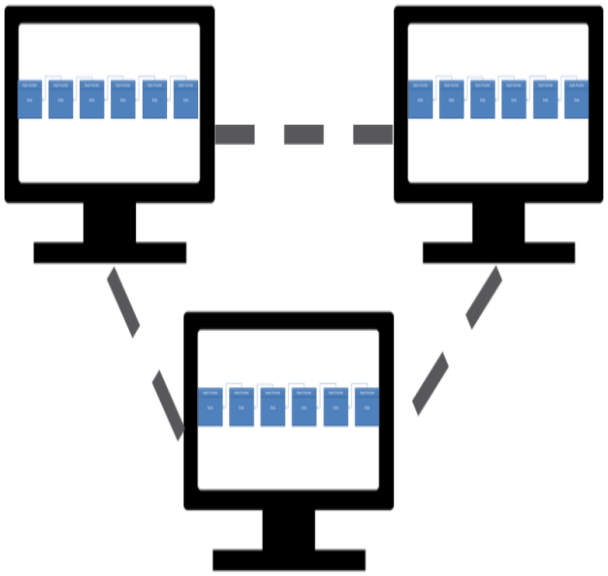

Figure 2. Peer to Peer distributed ledger architecture.

In this paper, we discuss basics of Blockchain technology, types of Blockchains, different consensus methods. We also suggest in the paper, plenty of Blockchain based use cases which can impact telecom networks. This paper also talks about how startups or incumbent operators can utilize this Blockchain opportunity and disrupt the economic and business model of the telecom industry.

The remainder of the paper is organized as follows: Section II talks about work done previously on this topic and our proposals. Section III describes types of Blockchains and compares their characteristics. Section IV deals with various consensus methods used in the network. Each consensus mechanism has its own pros and cons. We will propose multiple telecom use cases based on Blockchain in Section V. Section VI deals with business impact of Blockchain for startups and small operators. We conclude our paper in Section VII.

II. RELATED WORKS

Many telecom related use cases based on Blockchain have been proposed by operators, vendors, and different

 ISBN: 978-1-61208-642-2

consultants [1][2][4]. Very few of these proposed use cases are under implementation. Some of them are either at proof of concept stage while others are still at proposal stage. As part of our work for this paper, we researched many use cases and their feasibility. We are also proposing new use cases which will help operators in monetizing Blockchain in telecom networks. Since Blockchain deals with trust and security so cases related to identity management, IoT security, local and global registries containing subscriber/device data and telecom network transactional records are best fit for early Blockchain based use cases in telecom.

As part of our study during this work, we have found that use cases monetization will help the operators reduce the operational expenditure and will open new sources of revenue generation as seen in Section V.

III. TYPES OF BLOCKCHAINS

Blockchain can be classified into public, permissioned and consortium Blockchain depending how it is accessed and how the access permissions are granted [3].

A. *Public Blockchain*

A public Blockchain is a Blockchain that can be accessed by anyone (often, anonymously). There are no restrictions on who can join and what transaction they can post if the transactions are mathematically valid. Although members can join the network anonymously (revealing only their public key), every transaction that they undertake is visible to everyone (public), which can be carefully studied to identify the users. Bitcoin is the most famous example of public Blockchains [3].

In such a network, there is typically an incentive given to the participants for executing a computing resource intensive consensus protocol (e.g., validate a block using Proof-of-work).

B. Permissioned Blockchain

A permissioned Blockchain is one in which the interaction within the business is restricted to users who have the access rights provided by the network owner/s. In such a network, non-anonymous validation of blocks or interaction with the Blockchain is not permitted. Usually, a Certificate Authority (CA) is used to manage access to such a network. A Blockchain platform running its network as a permissioned network, will determine who can be validators and what privileges are given to what users. Hyperledger Fabric [6] is one of the most prominent example of a permissioned Blockchain framework.

C. Consortium Blockchain

It is possible that a single (originating) organization will maintain the Blockchain (centralized) and provide predefined access rights to interacting parties. Such a network typically suits government or regulatory bodies who have legal purview over other participants. However, it is debatable whether to call such a network a Blockchain network, as the ledgers are stored centrally and are not distributed among participating nodes. A consortium Blockchain provides some of the benefits affiliated with permissioned Blockchain—efficiency and transaction privacy, for example—without consolidating power with only one company.

Figure 3 provides key characteristics of a Blockchain based network.

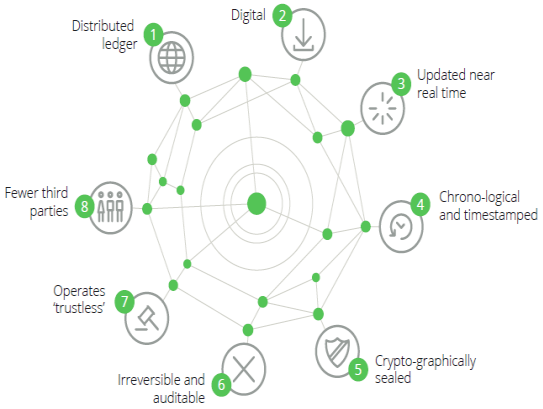

Figure 3. Key features of a Blockchain network [2].

IV. CONSENSUS METHODS

Consensus is a mechanism by which all nodes in the Blockchain network agree upon which block (transaction) gets added to the chain. Distributed computing existed well before Blockchains, but it is these consensus mechanisms which ensures that all the nodes in the network agree which makes the Blockchain so robust.

The ability to create honest self-correcting systems without the need of third-party to enforce the rules is what makes Blockchains so powerful. To enforce the rules, several variations of consensus algorithms/protocols are used, each with their pros and cons.

A. Proof of Work (PoW)

The most famous consensus algorithm is Bitcoin's Proof of Work (PoW), which make sure that the subsequent blocks in the chains are the only true versions. The correctness of the transactions can be verified by any participant using network consensus methods and cryptographic technologies in the Blockchain network. So, effectively the trust is established continuously within the network and not by any external central authority or auditor.

The Proof of Work protocol involves the following:

a) The miners solve cryptographic and complex puzzles to "mine" a block.
b) These puzzles are designed in such a way which makes it hard and taxing on the system as the

process requires immense amount of energy and computations usage.

c) After solving a puzzle, the miner must present the block to the network for verification. Then, it is concluded whether are not this block belongs to the chain, which is not a simple process.

B. *Proof of Stake (PoS)*

Proof of Stake (PoS) is ideologically different from PoW, wherein the complete mining process is done virtually and the miners are replaced with validators. The validators must lock up some of their coins as a stake before the validation process is begun. During the validation process, if a block is discovered which they think can be added to the Blockchain, it would be validated by placing a bet on it.

If the block's validation is successful, the block gets appended and the validators get a reward which is proportionate to the bets they placed.

C. *Proof of Activity (PoA)*

Proof of Activity (PoA) is a hybrid approach that combines the previous two consensus algorithms namely PoW and PoS. Here, the mining is commenced in the traditional Proof-of-Work way, where the miners compete to solve a cryptographic puzzle. Importantly, here depending on specific implementations, the 'mined blocks' does not contain any transactions but are more like templates. The successfully mined and validated block contains only a header and the miner's reward address.

D. *Proof of Burn (PoB)*

As can be derived easily, the first three consensus algorithms are quite resource-intensive, both computationally, financially, and energy-wise (massive electricity used for upkeep of expensive computer hardware and Application Specific Integrated Circuit or ASIC cards). To circumvent this drawback, the Proof-of-Burn (PoB) algorithms lets you 'burn' the coins by dispatching them to irretrievable addresses. The miners are selected randomly to mine on the system. Depending on the implementation, the miners may burn the native currency or the currency of alternative chain such as Bitcoin. The miners have better chance of being selected to mine the next block depending on how many coins they have burnt.

E. *Proof of Capacity (PoC)*

All the previous algorithms employ a variety of 'Pay-to-play' schemes where miners either have to solve a hard cryptographic puzzle, or give coins in stake, or burn some coins. Proof-of-Capacity is also in similar lines in that here we have to 'pay' with hard-disk space. The ones with more hard-disk space at stake have better chances of mining the next block to earn the reward.

The Proof-of-Capacity algorithm generates large data sets known as 'plots' before the mining process, which are stored in the hard-drive. The more plots available on the hard-drive, the more chances to find the next block in the Blockchain.

F. *Proof of Elapsed Time*

To come up with more energy efficient algorithms, chipmaker Intel pioneered an alternative consensus protocol called Proof-of-Elapsed time. Here, instead of having participants solve a cryptographic puzzle, this algorithm uses a Trusted Execution Environment (TEE) to ensure that the blocks are produced in a random lottery fashion, but without the required work and hence less resource-intensive.

Table 1. below provides a comparison between different consensus methods.

TABLE I. DIFFERENT CONSENSUS METHODS

Consensus Algorithm	**Brief Description**	**Pros/Cons**
Proof of Work (PoW)	Nodes must solve complex cryptographic puzzles to get the right to append new blocks to the chain and get the rewards.	Pros: Being the first algorithm, it's currently the most popular. It's also highly scalable, which makes it attractive. Cons: Resource- intensive (Computational, financial, energy). Vulnerable to "51% attack"
Proof of Stake (PoS)	Validators lock up some of their coins as stake after successful validation block is added to the chain.	Pros: No need to solve complex cryptographic puzzles. Fast, efficient and uses less hardware Cons: Vulnerable: Someone with enough money to invest exclusively into the destruction of this system can do so by investing only

		money, as opposed to PoW where they should invest money, time, expertise, hardware, electricity, etc.
Proof of Activity (PoA)	Hybrid approach combining PoW and PoS. The successfully mined and validated block contains only a header and the miner's reward address.	Pros: Combines best features of both PoW and PoS Cons: Less resource-intensive (Computational, financial, energy)
Proof of Burn (PoB)	Nodes must send their coins to an irretrievable address to mine a new block. The miner sending the largest number of coins get the chance to mine a new block.	Pros: No need to solve complex cryptographic puzzles. Cons: Burning coins is expensive as there is loss of coins. Less resource intensive.
Proof of Capacity (PoC)	Large number of plots generated in hard disk on stake, to get the right to mine the next block.	Pros: Miners does not need specialized hardware to mine. It decentralizes the mining process. Cons: Need lots of hard-disk space
Proof of Elapsed Time (PoET)	All nodes receive different waiting time duration, and the node with shortest duration will mine a new block.	Pros: Highly energy efficient as no cryptographic puzzle to be solved. Cons: Reliance on third-party (Intel). Relies on specialized hardware

V. TELECOM USE CASES

A. *Identity and Data management*

Identity and data management is a big use case for Blockchain which the telecom companies can use to generate new sources of revenues. Operators could provide their subscribers with an embedded SIM (eSIM) or app that creates unique virtual identities for each subscriber which are encrypted and stored in a Blockchain. Subscribers can use this identity to automatically authenticate themselves when visiting e-commerce websites, secure buildings, smart vehicles, airplane tickets, and so forth, as well as verification of personal documents such as passports, driving licenses, birth and marriage certificates, and educational degrees. For example, a virtual identity stored in a Blockchain using the operator's app could be used by a subscriber to sign into Facebook or Google on a mobile device. The benefit of having such a service is that the subscriber doesn't need to provide his or her personal details to different service providers to create new accounts and complex passwords. The virtual identity stored through the operator's app could be provided to numerous partner websites, utility service providers and apps as a unique identifier [1]. People will much more easily try new services if they do not have to subscribe from scratch –logging in with your Google/Facebook account is the best example of this.

This use case will open new sources of revenue for the operators and could be a game changer in how we access third party sites, apps, government facilities etc. In fact, United Nations is already working on a project called ID2020 [7] which is a public private partnership dedicated to providing identity services to the one billion people who live without an officially recognized identity and Blockchain is a key technology for this project.

B. *IoT Smart contracts*

A smart contract is a protocol used to facilitate and verify the negotiation of a contract. Just like a physical contract, smart contract defines the rules and penalties around the agreement, but it can also automatically enforce them. Industries like insurance, legal services, financial services, asset management use smart contracts to enforce rules and protocols. For telecom industry, Internet of Things (IoT) is one area where Blockchain based smart contracts could be extremely useful.

One of the biggest issues in IoT is how to maintain trust and security among millions (if not billions) of sensors that are getting connected with the network. The devices in the IoT ecosystem are the points of contact with the physical world. When IoT platforms use a Blockchain based solution for connectivity/authentication, time-consuming workflows can be automated in new and unique ways, achieving cryptographic verifiability, as well as significant cost and time savings in the process.

C. *Decreasing OPEX by proactively using transactional network profile*

Telecom operators can save millions of dollars of Operational Expenditure (OPEX) by using transactional network profile to proactively identify and resolve potential network issues. Proactive customer retention efforts are kind of process enhancements, service improvements and quality initiatives that encourage loyalty by removing the causes of defection in the first place. Decreasing OPEX by proactively using transactional network profile will also help in:

a) Debugging call related issues
b) Identification of degraded cells

 ISBN: 978-1-61208-642-2

c) Anomaly detection
d) Compliance and regulatory checking in future
e) Reducing fraud between collaborating operators

Currently, the primary reason for the increase in churner rate is the degradation of quality. Quality degradation could be because of frequent dropping of calls or lack of throughput. In most of the cases the operators are not aware of the issue. Either there is excessive load on the cell or there is configuration mismatch or software issue. As the operators rely on alarms for action and in most of the situation there is no alarms generated for these scenarios.

Blockchain can help in storing network transactional data. The persisted data can be studied further to detect degraded services, their patterns from the past, and reasons behind those patterns. Important Performance Monitoring (PM) counters related to cells e.g., Radio Resource Connection (RRC) connection successes, throughput across a cell for weekday and public holiday can be stored on a Blockchain based records. This trend could be compared with the current trend of a cell. If the variance is quite high, operator could be alerted about the cell. Operator can then proactively take action so that customer's experience is not degraded. Even the operator's customers could be informed of the potential issue enhancing the trust further.

D. *Initial telecom/network coin offerings*

Initial Coin Offering (ICO) has been a buzzword for the last couple of years due to the emergence of so many cryptocurrencies in recent past. For the uninitiated, ICOs are means of crowdfunding a new cryptocurrency or Blockchain based startups. Now, even telecom based companies have started to issue telecom/network related coins. The ICO are normally related to public Blockchain-based systems that anyone can participate in and so are the "coin offerings".

The main rationale behind these network coin offerings is that the it allows different models of monetization with pricing being governed by external factors rather than telecom operators or service providers. ICOs are good way of tokenizing mobile data, voice, app based packages and other network capabilities.

E. *Mobile data tokenization*

Mobile data plans are normally moderated by operators with unused data expiring at the end of every billing cycle in most parts of the world. Mobile data rates vary from 1$/GB to 10$/GB across different operators and regions. Millions of dollars of unused data expire every month across the world. Even with more than 2 decades of mobile connectivity, more than half of the world's population still does not have mobile and data connectivity. The unused data could be provided to underprivileged or unconnected parts of the planet thereby providing data connectivity.

A simple Blockchain based exchange could help to bridge this gap whereby users can donate or sell their unused data plans in the form of tokens to other users. A decentralized solution for providing mobile data will enable recipients to buy from providers at transparent terms, and reduces costs than buying from operators. The use case will require partnerships with operators to offer mobile data packages and enable user-to-user data transfer.

F. *Global and country-specific registries*

These registries could be databases both short and long term where information may get updated once in a week, month, or year. These registries could contain lists of blacklisted customers, lost devices, number portability updates and shared spectrum usage rights and allocations. Blockchain-enabled trust and security will be the most important differentiating factors which will keep these registries different from normal databases and will be accessible to different operators. Cross operator registry having International Mobile Equipment Identity (IMEI) of lost mobiles can be used for identifying and location lost devices. Of course, these registries require a lot of collaboration among the operators along with regulatory framework put in by regulatory body.

In fact, in May 2018, Telecom Regulatory Authority of India (TRAI) has proposed the use of Blockchain based ledger to curb the menace of spam or unsolicited commercial communication (UCC).

VI. HOW STARTS UPS , SMALL OPERATORS CAN LEVERAGE UPON BLOCKCHAIN OPPORTUNITY

Blockchain is one technology which could be compared to dot com boom of the late nineties. Blockchain has the potential to disrupt telecom industry in a big way. Different startups can specialize with innovative Blockchain solutions for facets such as virtual SIM card provisioning, authentication, national and international roaming solutions, micro-payments, customer care, data storage on a common cloud across operators.

Also, the backend operations, such as Operation Support System (OSS) and Business Support System (BSS) processes like billing of consumers, validation and number portability databases can be improved upon using block-chain. Dent wireless [8] and Airfox wireless [9] are two such startups which are disrupting the telecom data markets by their unique offerings. Mobile Virtual Network Operators (MVNO's) and tier 2-3 operators can also make use of this unique opportunity by offering innovative solutions based on Blockchain and challenge the big operators.

VII. CONCLUSION

Blockchain has been most talked and hyped technology of recent years with use cases coming out in almost every domain. Although Blockchain in its initial years had been centered around currencies, banks and insurance sectors

 ISBN: 978-1-61208-642-2

now industries like telecom see greater value from Blockchain implementation. Trust and security are important from the telecom network point of view. Blockchain presents a possible use case due to its inherent characteristics, especially in use cases where a third party is involved.

Blockchain will also enable new data monetization plans, enterprises will come up with innovative business models challenging and disrupting the traditional models employed by many of the telecom operators. It is expected that within the next few years, the use of Blockchain technology by the telecommunications industry will become more widespread and eventually become the norm in services like identity management, and registries to start with. As is often the case with any new technology, Blockchain is being developed and implemented at a faster rate than the existing regulations and government's frameworks. Regulatory authorities should also enable flexible legal and specification frameworks, such as data protection laws, for faster implementation of technologies such as Blockchain in telecom.

ACKNOWLEDGMENT

The authors would like to thank Carlos Alberto Martinez - Head of EDOS DP PDG and Juan Jesus Sanchez Sanchez, both of Ericsson Malaga, Spain and Neeraj Narang, of Ericsson Global India Pvt. Ltd. for their valuable feedback, support, and guidance. The authors will also like to express their gratitude towards Nipun Sharma and Praveen Arora, both of Ericsson Global India Pvt. Ltd for their comments.

DISCLAIMER

This paper reflects the authors own opinions and not necessarily those of their employer.

REFERENCES

[1] R. Kochhar, "Blockchain in telecoms: Is it still all hype or are we moving towards reality", Nov. 2017, [online]: https://www.telecomstechnews.com/news/2017/nov/17/Blockchain-telecoms-it-still-all-hype-or-are-we-moving-towards-reality/ , [accessed: June 2018]

[2] A. Babu, B. Davis, T. Bruwer, "How Blockchain can impact the telecommunications industry and its relevance to the C-Suite" , Deloitte , 2016, [online]: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf , [accessed: April 2018]

[3] A. Roychowdhury, "Blockchain fundamentals", [online] : https://arkarc.gitbooks.io/weekend-workbook-Blockchain-fundamentals/ , [accessed: April 2018]

[4] E. Velasco-Castillo, "Nine Blockchain opportunities that telecoms operators should explore", Analysys mason, Jun.2016, [online]: http://www.analysysmason.com/Research/Content/Comments/nine-Blockchain-opportunities-Jun2016-RDMY0/ , [accessed: April 2018]

[5] "Reimaging telecommunications with Blockchains", IBM, Jan 2018, [online]: https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03901usen/reimagining-telecommunications-with-Blockchains.pdf , [accessed : Feb 2018]

[6] Hyperledger, The Linux Foundation project, [online] : www.hyperledger.org , [accessed : Feb 2018]

[7] United Nations Digital Indentity Program, [online] :https://id2020.org , [accessed : June 2018]

[8] Dent Wireless, [online] : https://www.dentwireless.com/ , [accessed : May 2018]

[9] Airfox Wireless, [online] : https://www.airfoxwireless.com/ , [accessed : May 2018]

 ISBN: 978-1-61208-642-2