Article can be accessed online at http://www.publishingindia.com

Blockchain in Telecom Sector: An Analysis of Potential Use Cases

Rahul Darmwal

Senior Consultant, Ericsson India. Email: Rahul.darmwal@ericsson.com

Abstract

Furious customers disputing bills, issues of payments between operators for roaming services, sim clones and illegal eavesdropping, troubleshooting in multi-vendor – These are some of the most well-known issues faced by Telecom Operator. What if there was a way to overcome these issues. The potential benefits would be huge and at same time greatly improve perception of Operator in eyes of its customers. One such disruptive technology, Blockchains, which uses Distributed Ledgers and operates trustless, is being envisioned to solve such problems within Telco's.

A lot of literature is available describing how blockchain can be used to power todays Telecom use cases, however, hardly any papers describe the challenges that needs to be overcome to actually make blockchain a mainstream technology in Telecom sector. This lack of reality check was inspiration for writing this paper. In this paper, we try to understand "Blockchains", some proposed blockchain implementation for Telecom use cases and challenges that need to be addressed to enable these use cases.

Keywords: Block Chain, Telecom, Operator, Use Case, Distributed Ledger, Bitcoins, Challenges

1. Introduction

In recent years, Telecom systems have gone through a revolution. From call and sms days of 2G, we now have always on IP network which provides blazing fast upload/download speeds and enable all forms of communication (voice, text, video, email, etc.) through data pipes and applications installed on smart phones. However, the core technology and processes fundamentally remain the same. This means that in spite of great technological achievements, we still face same key issues (customer complaints, sim cloning, charging complaints etc.) today, that we have been facing since long time.

Blockchain is being positioned as a disruptive technology (Analysis Mason: Nine Blockchain opportunities that Telecom Operators should explore) that is expected to completely change the way systems interact with each other. It will make transactions cheaper, transparent, secure and enable efficient use of time and resources. By using Distributed Ledgers and Trustless processes, we could solve a number of fundamental problems in Telecom sector.

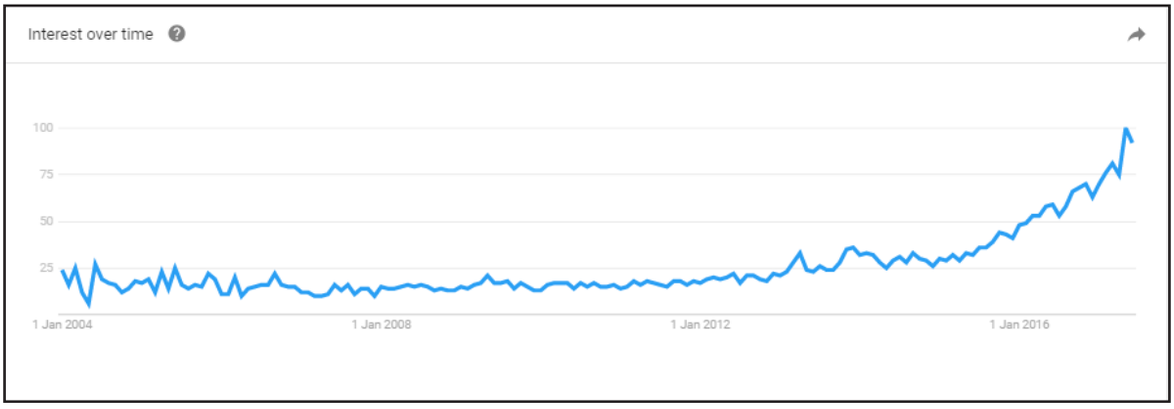

Fig. 1: Interest in "Blockchain" Over Time. 100 Indicate Peak Popularity for Search String

Source: Google Trends website

Fig. 2: Market Price of Bitcoins Since Inception

Source: "blockchain.info"

Interest in block chains has peaked in last few years based on success of Bitcoin, a cryptocurrency currency which is not controlled by central authorities like banks, states, government etc. Due to success of Bitcoins, financial institutes have already announced major initiatives to explore this area and we see similar interest from other domains.

We are already seeing a lot of interest on how block chains can help improve Telecom operations and its impact on existing products and services. Available literature was used to identify key use cases that will form part of this analysis in addition to some new use cases proposed by author.

2. What is Block chain?

Wikipedia explains block chain as:

A block chain – originally block chain – is a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. A block chain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks.

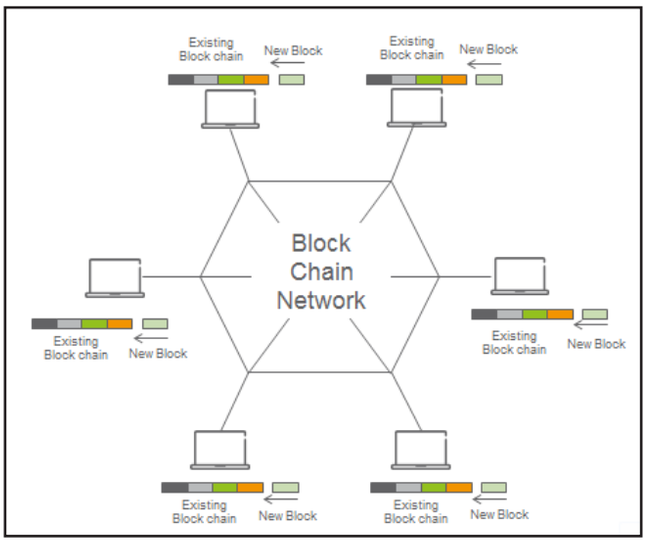

Fig. 3: Concept Drawing Showing New Block Getting Added to Distributed Ledger

So, Block chain is just a chain of data blocks, with linkages to previous blocks. And data blocks are shared with all participants on the network.

People familiar with ways of storing data will point out that this is fundamental shift in way data is stored. It is due to this change in storage strategy; block chains are revolutionizing existing use cases across industries.

To better understand how this is done, let's look at how block chain system will add new block of data. Assume that block chain has data in till Block 10.

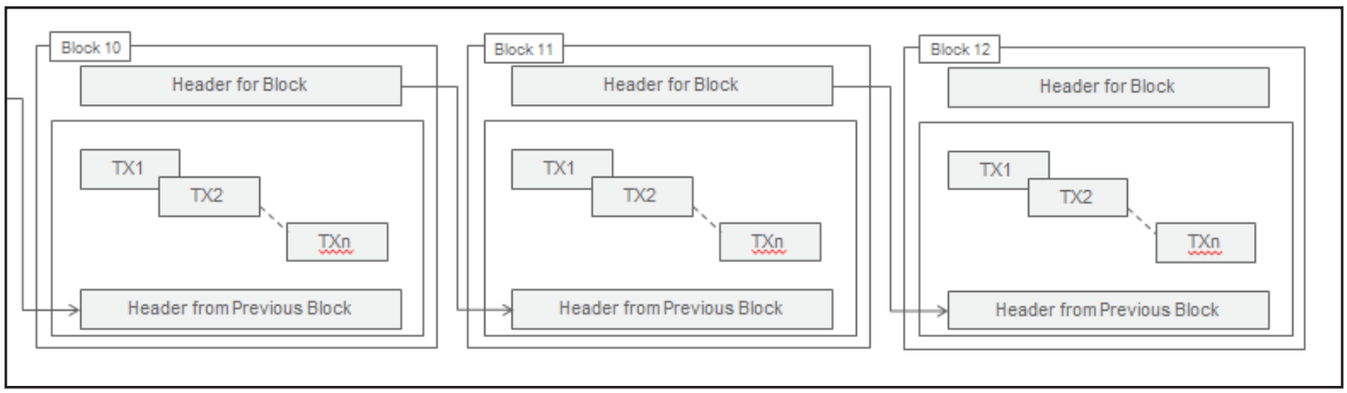

Fig. 4: Concept Drawing Showing Linkages Between Blocks in Blockchain

1. New transactions need to be added to existing block-chain. For this, Block 11 is being created by participant and this will get added to chain.
2. The various transactions are ordered sequentially in the block.
3. Header from previous block (Block 10) is added to current block (Block 11).
4. Using encryption algorithms, a header is created for new block (Block 11). The encryption algorithm considered transaction data in block along with Header from previous block (Block10). The headers are generally created using hashing algorithms, which are commonly used in cryptography. The block is then signed using participant's digital key.
5. The newly created block is now broadcasted to all participants of block chain.
6. The participants verify the block using headers included into blocks and digital signature of participants. The header contains link to previous block. The header is decoded to verify this linkage. The digital signature of sender is also verified electronically. If all checks are cleared, the participant adds the block to its chain. As, this is being done by all participants of block chain, it is almost impossible to get fraudulent transaction into the block chain without raising suspicion amongst the participants.

This linkage between current block and previous block makes each block permanent and irreversible as blocks cannot be changed without impacting previous blocks. Additionally, as data is distributed across multiple participants, it is impossible for single participant to change contents of blocks as everyone has copies thus making records permanent and non-editable.

Additionally, block chains can also be used to execute smart contracts. These are small if-then codes that run on block chains. Based on transactions taking place, the smart contracts get executed and results can impact participants of contract, e.g. if delivery receipt of order is received on block chain, release payment through block chain transaction.

Using above example, we can easily understand characteristics of block chains as explained by Deloitte:

1. Distributed Ledger: Transactions in block chain are stored on ledger that is available with all participants of block chain. What this means is that all participants in block chain have whole ledger (information about each and every transactions taking place between participants) and not just parts related to its own transaction.
2. Digital: Block chains are digital in nature with no linkages with physical assets in real world. This made its use in digital currencies (like Bitcoins) possible.
3. Updated near real time: Being digital in nature, transactions and updating ledger can be done in near real time.
4. Chronological and timestamped: Due to unique nature of block chains, it is possible to identify the exact time of each transaction. Even storing of transaction is done chronologically.
5. Cryptographically sealed: Each block is encoded with specific headers from previous block to create chain. This linkage means data in block cannot be changed without modifying whole chain.
6. Irreversible and auditable: Each block is created as permeant record. Once finalized, it is impossible to

modify content of block. This also makes auditing very simple.

7. Operates trustless: There is no central authority to monitor and approve transactions. Transactions are authenticated by solving complex mathematical puzzles (proof of work), based on stake in transaction (proof of stake) and other such proofs that need to be shared by transacting parties.
8. Fewer third parties: Distributed ledger and ability to operate trustless enables block chain based implementation to completely eliminate need of 3rd party mediators and trusted service providers.

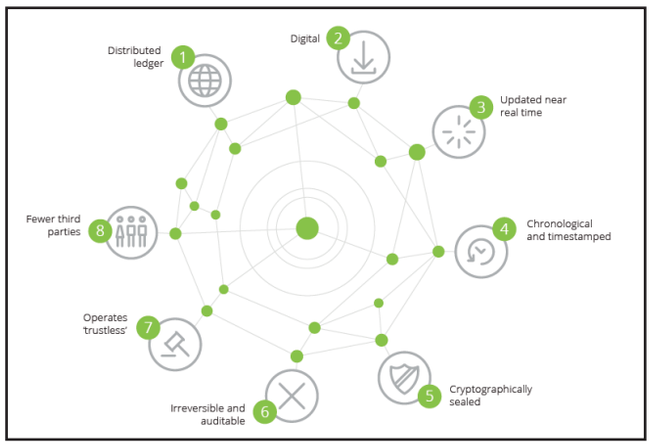

Fig. 5: Block Chain Characteristics by Deloitte

3. Block Chain Use Cases For Telecom

Block chains have already made their mark in Finance industry. Success of cryptocurrencies has helped test this concept and blockchains are now being proposed for almost every data centric use case across industries. However, Finance Industry is much ahead in testing block chains use cases and it is doing so by setting up collaborative endeavors across eco-system. Some prominent ones are: (1) R3 - Alliance of world's largest finance institutes with mission to realize the benefits of distributed ledger. Some examples include Barclays, Credit Suisse, RBS, Bank of America, etc. (2) Bank-Chain, India's first Block chain exploration consortium for banks led by SBI, (3) Digital Trade Chain (DTC): built on the back of a prototype designed by the Belgian bank KBC.

Telecom industry has very recently started exploring Block chain. Initial view of leaders in this area predicts block chains will revolutionize the way Telecom Industry works. Described below are some proposed Telco use cases which can benefit from Blockchains. These have either been collected from available literature or have been proposed by author based on his experience of Telecom Operators. Besides talking of benefits, key challenges that need to be overcome have also been highlighted to explain the complexity for development and adoption of use cases.

3.1 Postpaid Subscriber Billing

All Telecom operators' charge customers for calls/sms that they make or received. Data usage is also charged by Operators and bills generated for subscribers to pay for usage. Charging mechanism works in following way for postpaid subscriber:

- Subscriber make/receive call using his device.
- Network elements create call data records (called number, duration, location etc.).
- Call data records are sent to Billing system.
- Billing system analyses call data record and performs rating functions to determine exact charge.
- Charges are tagged against subscriber and bill generated at end of month.

As is evident, the main activity here is analyzing data streams of CDR's and tagging them against subscriber. Due to huge volume of CDR's, this is done using advance data base and functions.

Using block chains, charging mechanism can be implemented as follows:

- Subscriber makes call using his device.
- Network elements capture call data records.
- Call data records are sent to billing system through block chains.
- Billing system decrypts records and analyses them.
- For rating, smart contracts can be used.
- To generate monthly bill, bill generation application reads block chain and captures transactions against subscriber. The transactions are collated and monthly bill generated.

Benefits of Using Block Chain:

1. As transactions are stored on block chains, there is no need to buy expensive database licenses. Block chains replace existing database and provides simple and open method to store call data and other records.

2. Block chain storage provide higher level of data security and integrity as no single internal system will be in-charge of storing call data records(distributed ledger). Call records would be available with all participants in block chain (e.g. network elements, billing systems, archiving systems, etc.).
3. Smart contracts will make it simple and modular to create and modify rating plans.

Challenges that Need to be Addressed to Enable this Use Case:

1. Block chains deal with blocks of data, or multiple transactions in single block. Some time and effort are spent in encrypting the block using hashing algorithms. This means, there is inherent processing time taken by system to process a block. For postpaid billing, some delay is acceptable, but for pre-paid, system needs to be near real time which will make use of block chains challenging for prepaid market. This will limit scope of this technology for charging purposes.
2. Due to huge volumes of call traffic within operator's network, block chain file will continuously get appended by new blocks, resulting in file size reaching epic proportions. Larger the file, more difficult will it be to scan the file to calculate subscriber balance, etc. (as whole block chain is scanned to identify transactions of particular subscriber).
3. A very large number of smart contracts will need to be defined to handle charging logic deployed in operators. Additionally, depending upon complexity of charging logic, complexity of smart contracts will also vary.
4. There could be need to re-rate particular call data records and correct bills due to technical issues or human errors. This re-rating would be very difficult in system that diligently follows block chain logic (as block once written cannot be edited).

3.2 Interconnect Billing

Interconnect billings deals with settlement between Home Operator and Roaming network operators, where, customers of home network uses services provided by roaming network. Interconnect billing process is done for postpaid subscribers only, as prepaid subscribers still use home network for charging.

When home subscribers go roaming and makes phone call or uses data, CDR's are generated in roaming network. These CDR's are sent to the clearing house which is like a central agency connected to various operators. Clearing house helps connect operators by providing common place to share roaming records and help to settle their interconnect bills. In current system, it is responsibility of clearing houses to process CDR's and sends correct bills to Home network. Unfortunately, due to involvement of intermediator (i.e. clearing house), individual networks do not have visibility in the settlement process which may lead to disputes.

Proposed Improvements Using Block Chain

It has been proposed that concept of clearing house can be eliminated completely by using block chain technology. This can be done as follows:

A private block chain for partner Telecom network operators is created. Partner Network operators are authenticated and then allowed to join the block chain network to maintain security, authenticity and data integrity. The operators can now share roaming cdr's on block chain in near real time. Because the cdr's are shared with every host on network, the home operator receives copy of cdr generated in roaming network. As Home network receives CDR's in near real time, billing can be done immediately without need of third party (clearing House). Additionally, smart contracts can be implemented to develop automation in settlement process.

This eliminates need for clearing house, thus saving costs to Telco's. Block chain implementation are also expected to improve speed and efficiency of this operation.

Benefits of Using Block Chain:

1. Block chains allows for transparency in inter-network billing as CDR information is saved as distributed ledger and is available with every network operator. There will be no need to send CDR's to clearing house due to use of Distributed Leader. Operators can save fees paid to clearing house for their services.
2. Distributed Leaders will make this process transparent to all parties and enable near real time billing.

Challenges that need to be addressed to enable this use case:

1. There will be need for Operators to create implementation strategy and develop the closed block chain network required for this purpose. Details could in-

clude how network is funded/created/managed, what will be process for operators to join, how settlement will take place, etc. To enable wide usage, this would need to be developed into standards.

2. The responsibility of data reconciliation and settlement will rest on Network operators and accuracy of block chain.
3. Without trusted third party to intervene, Telecom Operators would have to manage relations with huge number of operators.
4. Data privacy concerns will need to be addressed as cdr's from all partner networks will be accessible to all networks.

3.3 Using Public-Private Keys for Customer Authentication

The Telecom network authenticates subscribers using information stored on SIM card and through A3 & A8 algorithms. It follows challenge response concept for authentication. The process consists of challenge sent by network towards handset which has requested to be authenticated. The handset uses data on SIM and authentication algorithms to determine the right response and sends it back to the Network Element. The response received by network element is compared with calculated response determined by Network elements and if response matches, handset is allowed to access network.

To be able to achieve this, subscriber specific information is coded on SIM card. Same information is also stored on Network elements and it is imperative that both these set of information matches. During challenge and response, this subscriber related information is used to calculate, respond and verify authenticity of subscriber.

Proposed Solution Using Block Chains:

Within block chains, individuals are identified using their public and private keys. Public and private keys have been used successfully for doing transactions on internet. Similar concept can be deployed for authenticating subscribers on Telecom network. Subscriber will be the only person who will have access to his private key. Public key will be used for authentication and requesting services from network. As private keys are not shared with network at any point in customer life cycle, this method of authentication is a lot more safer than existing SIM based methods as subscriber specific parameters are stored on Network element and sim card and can be compromised easily.

Benefits of Using Block Chain:

1. Public private key is de-facto standard used on Internet for authentication. If used in Telecom networks, this will improve security many folds.
2. Private keys are not stored on Network elements, thus reducing risk of cloning and fraudulent usage of services.

Challenges that Need to be Addressed:

1. To be able to use Public-Private key authentication, there will be need to redesign authentication process for telecom infrastructure. This will be a major change for everyone in the eco-system requiring collaboration at massive scale and development of new standards
2. This will also have to be globally accepted and implemented as standard to enable concepts such as roaming, inter-operability etc.

3.4 Integrated O&M

Elements of mobile network elements are connected to their respective network monitoring platforms. These platforms interface with network elements and send commands for configuration, collect alerts, logs, and generate statistics. As the alerts/logs are coded in vendors own proprietary interface, they can be understood by their corresponding platforms only. The platforms for various network elements are then connected to central O&M elements such as those present in Network Operations Center(NOC). The central elements then translate individual messages to common language and store them in their database. These are then processed and analyzed to get Network level view of what is happening in network.

Proposed Solution with Blockchain:

It is proposed that, the network elements can form part of trusted private block chain network. Events triggered on one element can be broadcasted, using block chains to all elements on network. As all network elements are able to receive information about each other, there can be greater degree of understanding on what is happening within network. For e.g., incase an element is made operationally disabled for maintenance, the NMC's of those element can broadcast alerts to all network elements in block chain. This will help in quicker diagnosis (other elements know there has been operational activity and that they can ignore the alarms generated), add transparency by creating

non-destructible record for future auditing and improve collaboration amongst various network elements.

Similarly, configuration changes can be broadcasted to partner elements, thus enabling communication link between various network elements. Smart contracts can also be created to automate task based on specific triggers.

Benefits of Using Block Chain:

1. Individual Network Elements are not aware of what is happening to other elements of network. Only operators in NOC are able to get full picture and take required decisions. And even NOC operations are susceptible to translation errors, data loss and such other issues which will reduce effectiveness of their analysis. This can be avoided using proposed approach.
2. Distributed Leaders for Network elements will help create sequential, non-destructible and non-refutable log of events available across all network elements. These logs can be used to make informed decisions and execute smart contracts to automate tasks.
3. Sequential logs will create transparency between elements, which generally could be from different vendors. Transparency will improve RCA and help operators manage their network better.
4. Information shared directly between various network elements will enable an whole new way of performing O&M for network elements

Challenges that Need to be Addressed:

1. This will impact Network elements and the way they are monitored and managed. Standards will need to be defined and agreed for block chain implementation to enable inter-operability across network elements and vendors.
2. Such implementations will directly impact vendors of central monitoring systems used in NOC's etc. Many a times these are same as those providing network equipment leading to conflicts on what is right approach

3.5 Customer Purchase Management

Currently, purchases made by customers are tagged in CRM or similar tools. The customer does not have record of his active services and is dependent on database of operator to tell him about his active services. This leads to frequent mismatch complaints and results in time and effort spent to audit records and take corrective actions.

Proposed solution: It is possible to create private block chain group in which subscriber and operator are members. Any transaction initiated by customer (e.g. purchase of plan) is stored in block chain which is accessible to Subscriber and Operator. Similarly, any transaction initiated by Operator (e.g. bonus plan) will be stored in Block Chain available with subscriber and network operator. As subscriber and operator have copy of same distributed ledger, there is no scope for ambiguity between operators record and customers view (which he can see using software tool).

Benefits of Using Block Chain:

1. Distributed leader between Operator and subscriber will drastically reduce complaints of service mismatch(what is ordered by customer and what has been activated on Operators systems)
2. Such an initiative, if explained and marketed properly, can drastically improve perception of operator in minds of its users

Challenges that Need to be Addressed:

1. To be able to provide this service on block chain, individual block chains for each subscriber with operator as participant would be needed. This is to avoid sharing information of other customers. Feasibility for such 1 to 1 deployments on large scale (to cover all subscribers of operator) would need to be evaluated as existing systems are focused on creating group of interested participants.
2. Customers would need to be educated on block chain concepts to be able to appreciate the merits and benefits of this new technology

4. Conclusion

Blockchain offers a completely new way of storing transaction information. The technology has already shown its capabilities in cryptocurrency space and the world believes, this will fundamentally change the way we store and process data. The use-case for distributed ledger are far and wide. However, for established industries like Telecom, which have been built on standards to enable inter-operability and high performance, technology shift will have to be gradual to avoid disruptions in current services. Telecom domain has yet to embrace Block

chains and to create a plan for its testing and adoption. The best way forward would be to cautiously explore this new technology by building consortiums or using available standard bodies to discuss and debate as being done by other Sectors.

Development of block chains could be compared to development of another revolutionary technology which is TCP/IP. Sending data as packets using IP has been in making since early 1970's. What started out as technology to send emails within participating universities has now become backbone of our digital economy and is used in almost every digital transaction that we do. However, this took about 20-30 years with contribution from various companies and institutions. Telecom Operators have also started exploring Block chain to support them in their operations. However, adoption of Block chains for Telecom use cases is in its infancy. There has not been any consolidated effort by Telecom Sector which is required for wider acceptance of this technology. So, it is safe to say that we are at least 5-10 years away from seeing major blockchain deployments within Telecom Operators space. Block chains are here to stay, though Telecom Block chain is yet to take shape.

References

Blockchain/Bitcoin for beginners. (n.d.). Retrieved from https://www.youtube.com/watch?v=xwA2TkcAQgQ

IBM Blog: Blockchains in Telco's, (n.d.). Retrieved from https://www.ibm.com/developerworks/community/blogs/IndustryBPTSE/entry/Blockchain_in_Telcos?lang=en

HBR. (Jan-Feb, 2017). Truth about Block chains. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

Mckinsey Interview. (May 2016). How Blockchains could change the World. Retrieved from http://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

The Economist: The great chain of being sure about things, Retrieved from http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

Monitor Deloitte: Blockchain@Telco. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Jover, R. P., & Lackey, J. (n.d.). *dHSS - Distributed Peer-to-Peer implementation of the LTE HSS based on the Bitcoin/Namecoin architecture.*

TM Forum. (Feb 2017). *Disruptive Analysis: Blockchain and Telecom Industry.*

Analysis Mason: Nine blockchain opportunities that telecoms operators should explore

Blockchain Luxemburg: https://blockchain.info

Bitcoin: https://bitcoin.org

Wikipedia: https://en.wikipedia.org/wiki/Blockchain

Application of Block chain technology to Banking and Finance Sector in India. (n.d.). Retrieved from http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf

Blockchain technology as a platform for digitization: Ernst & Young. (n.d.). Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/$FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf