International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

Catering the Telecom Conundrum of Revenue Leakage: Blockchain- A Business Paradigm

Charishma Idamakanti, Kislay Bhardwaj
Student, Symbiosis Institute of Telecom Management, Symbiosis International University, Pune, India

ABSTRACT:
A traditional telecom operation consists of a complex and long chain of inter-related operations that work jointly to deliver services to customers and then track and record the services delivered to bill the customers.Rapid increase in telecom subscriber base and the paradigm shift of consumer's expectation from getting basic telecom services which has not only put immense pressure on telcos to adapt latest technologies but also makes them vulnerable for financial leakage. Revenue leakages and frauds are the results of the porosity of the ecosystems, which is evident by the global losses recorded under them.Blockchain is a technology which carries the potential to disrupt business models in telecom by increasing transparency and efficiencies in the telecom network and its processing. This decentralized ledger documents each transaction that occurs across a fully distributed or peer-to-peer network, either public, private or hybrid. With the industry moving towards application in the industry, new codes and sources are coming up such as Hyperledger and Raiden network to broaden the spectrum of usage in an interdisciplinary approach.There is a dearth of models on how to implement blockchainin telecom industry, therefore this study tries to add to the literature by suggesting the followings related to the working model: (1) Risk and Fraud Scenarios (2) Concepts of Blockchain (3) Revenue Assurance & Fraud Management (4) Models to Implement Blockchain by Telcos (5) Conclusion.

KEYWORDS: Blockchain, Telecom, Revenue Leakage/Loss, Billing, Raiden Network, Hyperledger

1. INTRODUCTION:

Telecommunication has always been considered significantly important to the growth and development of the overall economy of any country. The industry accounts for approximately 2.5% of worldwide GDP [1]. It has witnessed a widespread and disruptive change in recent years, named as the period of significant transition. Many factors have led to the disruption of the industry, from technology changes to intense competition and consolidation to changing customer behaviours. This changing environment of business has forced telcos to do away with traditional legacy business models and adapt latest technologies to cope up with current trends and demands.

Service convergence and industry integration have become primary concern for telcos. Support for 5G, Internet of Things (IoT), Augmented Reality (AR), Virtual Reality (VR) and so on have brought new challenges like dealing with issues related to plethora of contents, data traffic explosion, mobility, security and many more to be listed, which eventually lead to revenue leakages and frauds. Need and building an infrastructure that sustains a healthy, safe, and efficient operationis, a scientific and engineering challenge which dates back to the 18th century, when the Industrial Revolution catalysed rapid urban growth. Therefore the above mentioned factors have not only shown their potential to reshape the fundamental relationship of telecom companies had with their customers, suppliers and their value chain partners but also making businesses vulnerable to different stages of risks, mainly related to data fraud and revenue. Blockchain, a young technology currently at hype, has highly resilient architecture and distributed nature thereby showcasing its potential to deliver the nervous system of the ICT industry.On micro level, implementation of blockchain by telcoscan address problems related to revenue leakages and frauds in an effective manner.

2. LITERATURE REVIEW:

Globalisation and the on-going world economic crisis have burdened a lot of companies, especially in terms of credit crunch, economic recession, difficulties in international partnerships and complexities in matching the global development along with the needs of adaptation to the latest generation technologies and telcos are no

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

exception. Uncertainty and complex composition have added to the factors that are making businesses vulnerable to different stages of risks, mainly related to data fraud and revenue. Telecom operators in 2016 faced an estimated average loss of 13% or $294 billion (USD) globally, resulting from fraud and uncollected revenue [2]. Hence, it is necessary for telecom operators to understand that their goals/objectives may eventually face defeat without an effective Revenue Assurance and Fraud Management system during the transformation phase.

Risk is defined as a probability or threat of loss, damage, liability, injury or any other occurrence; negative in nature, that is caused by internal or external vulnerabilities, while fraud refers to criminal or wrongful deceit, intended to result in personal or financial gain [3]. Both of them are often caused to the inefficient handling of data, the most important incorporeal property of all organisations. Data is the most complex and valued property, generated with a speed of 2.5 quintillion bytes per day [4]. This is one of the reasons why unfolding its complexity and protecting it from fraud has been tedious and of high maintenance for all organisations. Fraud and misconduct have posed serious threats by undermining the efforts of organisations, exposing it to regulatory, financial, legal, or reputational damage. Therefore business leaders have been working and are having been showing a keen interest in effective approaches to ensure that the data related risks are mitigated.

Researchers and data scientists have observed a ten-fold increase in the number of occurring retractions attributed to suspected fraud [5]. Many technologies have been developed over the decades to safeguard it from reaching the hands of marauders. It is estimated that fraud itself costs in the industry of over USD 38 billion annually [6]. It has become a pre-requisite for all organisations to develop a strong infrastructure and defence against vulnerability to fraud. The risks faced my telecom operators could be reduced or avoided through pre-emptive action. In today's market conditions the spell to succeed is through enhanced efficiency, which will elevate the organizational agility. This will enable operators to rapidly respond to the changes and would help bring products/services faster and more competitive to the market. The top five risks faced in telecommunications industry in the year 2016 are given in the figure:

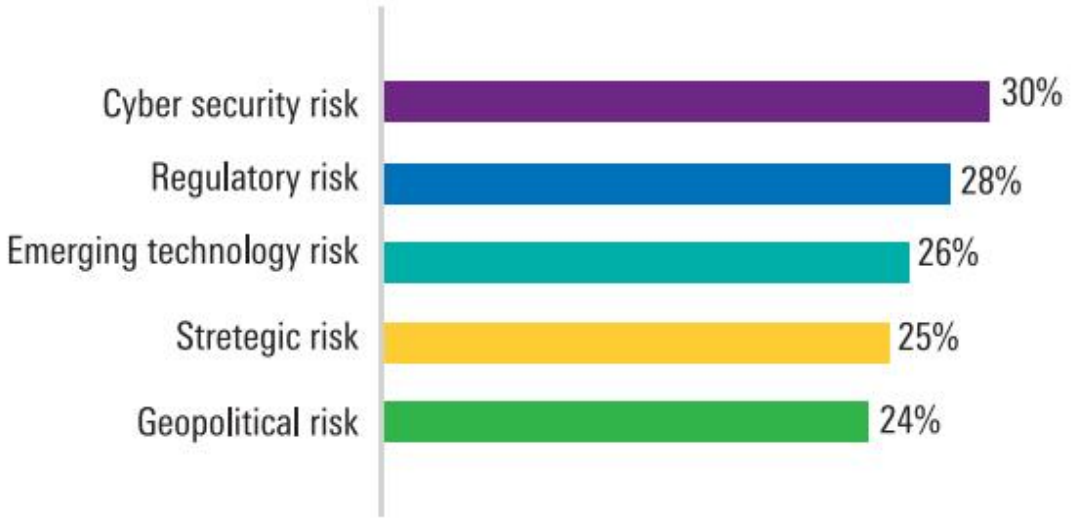

Fig. 1: Top five risks of telcos [7]

Fraud monitoring across business lines, geographies and functions using pre-defined detection business rules for each sub-sector vulnerable to fraud such as Cellular Operators, Value Added Services (VAS), OTT services, Passive Infra, M-commerce, E-wallets and also across the functions such as Customer Service Department (CSD), supply chain management, sales and IT/network marketing and more importantly the Billing, and IT revenue assurance that are often seen to be customized as per the organization's business source feed and operations.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

3. REVENUE ASSURANCE & FRAUD MANAGEMENT:

Revenue assurance is the application of a process or software solution that enables a Communication Service Provider (CSP) to accurately capture revenue for all services rendered [8]. It's undertaken within businesses to detect revenue leakages through the use of data quality and process improvement methods that minimize opportunity loss, revenue loss and improves cash flows without influencing demand.

Telecom industry lives in a technologically complex, competitive and global environment. Wireless market saturation, new technologies and the arrival of new trends such as OTTs, bundling and convergence, have meant increased competition with highly disruptive business models. This competitively saturated global market where customers face information and choice overload than ever before have stimulated operators to invest in consistent service innovation. Billing, collection and storage, which were previously fairly manageable exercises, have become increasingly complex in nature.

Despite the intensive checks by in-house financial departments, an ERP and audit system, approximately 1% to 5% of the predicted EBITDA is still lost. Reasons of revenue leakage can be broadly classified into System Error and Human Interventions. Errors in a process of a system is a common cause of leakage which is linked to the network infrastructure while greater risk lies in the combination of system error and unwanted human intervention which would be further catalysed by poor communication between different departments of the business. Revenue leakages generally occur outside the conventional control mechanisms, thereby making it often difficult to judge, the real danger threatening the business [9].

91% of global operators view real-time assurances as the most important, priority for revenue protection [10] yet fail to achieve the practically desired accuracy. Revenue assurance spectrums from retail and corporate sales to interconnect, wholesale contracts, margins and profitability of investment. It accommodates Revenue leakage, Cost leakage, Margin leakage, Fraud management and Network downtime in its objectives. In order to achieve its reason of adoption, it is important to understand what the possible areas of revenue leakage. Leakages can happen at:

- Network elements
- Mediation Level
- Billing Level
- Provisioning and Customer Service
- Collections and Dunning
- Product Development
- Order Management

In this modern age of competition, reduction in leakages can help operators to marginally increase their revenues. With convergence the number of points of connectivity or touch points will be more, which will increase the chances of revenue leakages.

Telecom Fraud refers to the purchase or use of telecom product or service with intent to avoid payment. Fraud is an act raised as a consequence of many factors like competitive market pressure, unstable returns, network complexity, poor database management, high cost of lost distance calling and VAS and so on. Telecom Fraud can be classified broadly into Revenue fraud and Non-Revenue fraud which are bounded by motivation to acquire anonymity to mask criminal activities or obtain the thrill of challenging the security of telecom service provider. Telecom Frauds can further be also divided into Usage Frauds and Subscription Frauds. Misusing another subscriber' services, running unauthorized Private Exchange and technical frauds like by-passing network, Conference and call forwarding frauds are known as Usage frauds. Subscription Frauds include Activation fraud, unauthorized operations on customer account, subscriber data anomaly between network elements and billing, etc.

With the increase in the risks and frauds, new solution providing technologies are always admired by organisations, one such ledger trending technology is Blockchain.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

4. BLOCKCHAIN:

Blockchain or Distributed ledger technology (DLT) is one such young and evolving technology which has the potential to disrupt the established business models in many industries with added benefits like increased transparency and efficiencies in the process and thereby mitigate the above risks. It has attracted increasing attention from businesses and regulators in the recent times as it's considered to provide a high-level, albeit non-exhaustive potential benefits. Bockchain is a technology originally devised for Bitcoin crypto-currency, could be a strong anti-fraud and proactive stance. It could be a comprehensive approach to combating intruders with an intention of fraud. It is a decentralized public ledger system maintaining the integrity of transaction data.

In blockchain each participant hosts a copy of the database, which is continuously updated across all nodes of the network as and when new information is added. Decentralisation means that the information updated or listed is not controlled by any single person or organisation. All copies of the database must be in sync with every another node or else the information would be reckoned corrupted. Blockchain uses multiple cryptographic tools to store the information into "blocks" which are verified by the network participants popularly known as "miners" before being added to the database to prevent potential corruption. Each blockchain network will have its own pre-defined rules on how the verification process must work.

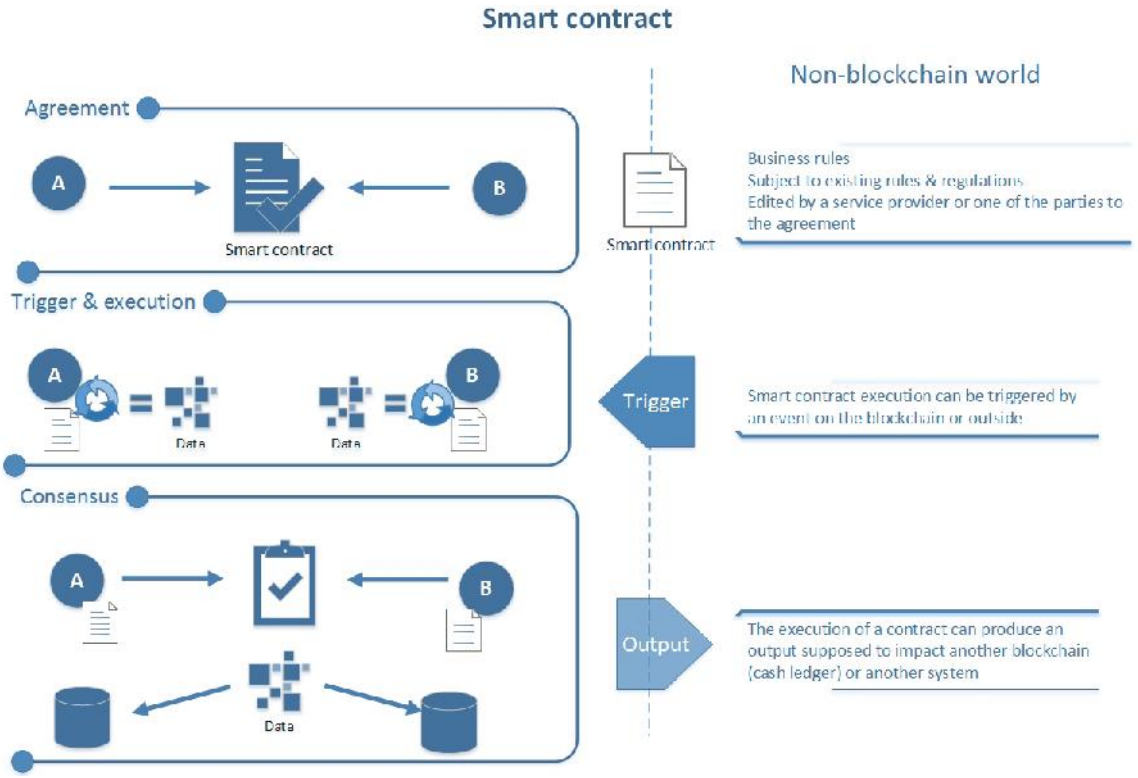

Fig. 2: Smart Contracts [13]

The information in the blocks is stored in a structured manner that enables users to interact at the application layer. This layer sits above the blockchain technology and would be customised as per the requirements of the participants, to access that information. Cryptography is used in blockchain technology in combination with blockchain's distributed nature therefore it is currently impossible to alter information in the database, thereby showcasing the ledger analogy. This security and transparency provision is key to the appeal of blockchain to businesses around the world.

The essential feature of Blockchain is the use of the Public Key Infrastructure (PKI) mechanism, in which the user has one pair of public and private keys. Software at the application layer manages the issuance of these keys, and their pairings. Among the two the public key is used in the address of the user and the private key is used for the authentication of the user. These set of public and private keys are created by an asymmetric

algorithm in such pairs that the keys have a mathematical relationship which allows the private key to decrypt the information encrypted by the paired public key.

Smart contracts is one of the features accommodated by blockchain, which has the nature and potential to substantially boost efficiency in many areas of business and law. A smart contract is an agreement in digital form that is self-executing and self-enforcing [11]. Smart contracts provide a viable method of issuing tracking ownership of unique digital representations of value, with the help of the keys mentioned above. Smart contracts also known as self-executing or digital contracts are simply computer programs that act as agreements. The programmed code can then be automatically executed by a distributed ledger system and the terms of the agreement can be pre-programmed with the ability to self-execute or self-enforce itself. The smart contracts enable two anonymous parties to trade and do business with each other, usually over the internet, without the need for or intervention of a middleman [12].

Ability of the user to remain pseudo-anonymous with the help of smart contracts, in a blockchain network has proven to be particularly attractive from a data protection perspective, evidently seen in the hype generated by Bitcoin. Blockchain can also provide benefits to telecom companies across countries to instantly validate a subscriber's identity who is registered with the operator in their network [14]. It will increase transparency of transactions between the operators and the money transfers by the subscribers. The Regulators can also be a part of blockchain network to have visibility in the movement of money and delivering of services for better regulation.

4.1 PERMISSIONLESS (PUBLIC) BLOCKCHAIN:

Anyone can set up as a node with a computer and internet connection, which is continuously synced with the entire blockchain history. Though this induces redundancy, making the public blockchain extremely secure, it also makes it slow and wasteful. The benefit of this system is that every transaction is public and users can maintain their anonymity.

A public blockchain is most recommended when a network needs to prioritize decentralization, accommodate full transparency of the ledger or achieve individual anonymity. Though the public chains are faster and less expensive than the accounting systems and methods used today they face reluctance due to higher costs and slower speeds over a private chain.

4.2 PERMISSIONED (PRIVATE) BLOCKCHAIN – ACCESS TO PREDEFINED AUTHORITIES/PERSONS ONLY:

A private blockchain network always requires an invitation which must be validated by either the company or by a set of rules defined by the company. Unlike public chain, it accommodates the middlemen to a certain extent. Every transaction is written and verified by the organization, this allows for much greater efficiency than public chains. Therefore, the transactions on a private blockchain would be completed significantly faster and the company could also choose who has access to read their blockchain's transactions, developing an ecosystem for greater privacy than a public blockchain.

A private blockchain is more appropriate to traditional business and governance models. Adoption and integration are likely slower in this sector due to lack of standardisation but if adopted they would cut billions of dollars being spent behind the scenes.

4.3 CONSORTIUM BLOCKCHAIN:

Consortium blockchain is hybrid or partly private. It provides a hybrid between the low trust characteristics of public blockchains and the highly-trusted traditional centralized system of private blockchains with a degree of cryptographic auditability model. Instead of permitting any person to person the job of a 'Miner' or restricting only one company to have full control, consortium blockchain allows to predetermine a set of selected nodes [8]. Without comprising on benefits affiliated with private blockchain, it allows the distribution the consolidating power. The permissioned nodes are generally known entities and have administrative authorities to decide who has read and verification access to the blockchain ledger. This platform would prove to be a less complex and more efficient in the case of organizational collaboration.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

5. SCOPE OF BLOCKCHAIN IN TELECOM INDUSTRY:

5.1FRAUD MANAGEMENT:

In 2015, the Communications Fraud Control Association estimated the global revenue of the telecom industry to be approximate $2.25 trillion; but global fraud loss was estimated close to $38.1 billion in that same year. Despite the innovations, the industry has not found a sustainable method to mitigate fraud. Blockchain has high capacity to reduce the potential probability two types of frauds – roaming fraud and compromised identity.

5.2 IDENTITY MANAGEMENT:

Blockchain can help create new sources of revenue by providing data management and identity authentication solutions to enhance their user base. Cellular Service Providers (CSPs) could utilize their relevant customer data to provide a dynamic platform for identity transactions, such a system establishment would involve a multi-step process where first the subscriber creates a digital identity similar to a digital signature which would be placed on the eSIM.

5.3INTERNET OF THINGS (IOT):

Sensitive information is carried by IoT sensors pertaining to their users, therefore, securing these systems would be certainly a priority in the near future. Blockchain provides a secure dynamic peer-to-peer distributed network solution through the utilization of nodes which can be represented by embedded IoT sensors that verify every block being changed into a real-time monitoring system for IoT systems.

5.4SUPPORT FOR 5G NETWORK:

Network provisioning rules and real-time processing are the current issues being faced that need to be addressed before mass adoption of 5thGeneration networks. To automatically execute rules and agreements between access points and allow for real-time availability of network resources, smart contracts can be used which are one of the core functionalities of blockchain.

5.5FUTURE SCOPE:

With sustainable scalability still a challenge, on defining the parameters of implementation, blockchaintechnology can be used to help design more leakage proof,efficient and real-time neurology for SDN/NFV, SLA Management, Storage Management, Cellular-WiFi convergence and many more.

6. PROPOSED APPLICATION OF BLOCKCHAIN:

An effective Revenue Assurance system not only tracks and identifies the discrepancies in usage as reported by OSS/BSS systems but also ensures that usage is billed at appropriate rates. The Revenue Assurance system must be able to validate charges against rates and inventory of installed/activated equipment, leased facilities and circuits. This requires a sophisticated rating engine that is able to accommodate a wide variety of charging models. Operators must demand and verify that the Revenue Assurance system has an independent and sophisticated rating engine that allows for configuration of all types of rate plans and charging models and do so with ease. In this paper we propose five networks which could be implemented by telcos to mitigate the currently facing levels of risks and frauds.

6.1ROAMING MANAGEMENT:

Roaming is the facility that enables subscriber of one network (call HPMN, i.e., Home Public Mobile Network) to use all the services provided by their network remotely, while remaining away from home network via retrieving it through a different network service provider (call VPMN, i.e., Visited Public Mobile Network). Mobile operators suffer consequential fraud losses due to ever increasing number of International Revenue Share Fraud (IRSF) cases. The average losses incurred are of about €15,000 per hour and go up to €40,000 during severe incidents caused by fraudulent roaming calls. The actual total loss per case can reach hundreds of thousands of Euros [15]. Therefore mitigation of these leakages is essential.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

6.1.1 PRESENT SCENARIO:

When a request to process or an event is initiated by a roamer, VPMN sends a query about the roaming related subscriptions of that roamer to the Home Location Register (HLR) of HPMN through signalling link. To this signal the VPMN responds by sends all the information related to Call Detail Record (CDR) to their billing system and to HPMN so that they settle the account with VPMN as per the cost was borne. Often Telcos outsource transmission of CDR files and its conversion into billing traffic according to individual's subscription to the third party, called Data Clearing House (DCH).

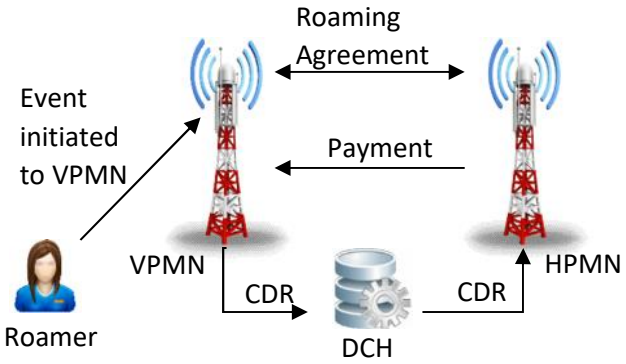

Fig. 3: Present Roaming Scenario

6.1.2 ACCIDENTAL ERRORS & DELIBERATE FAULTS:

Roaming fraud occurs when HPMN cannot charge to the subscriber (roamer) to use the resources of VPMN, but still liable to pay to VPMN. Followings are the primary reason for roaming fraud [16] –

- **Longer detection time:**The time elapsed between the penetration of the fraud , the instant of detection and measures to combat it are deployed is determined by the time involved in sending the CDR related information from the VPMN to the HPMN, and the time employed to investigate the potential existence of a fraud attack [16]. It takes HPMN longer time to detect frauds because it has occurred outside of its network, under the network of VPMN and there have been delays in the information exchange between VPMN and HPMN.
- **Longer response time:** Even after the fraud has been detected, HPMN does not have direct control over the network of VPMN. So, it takes more time to respond than usual.
- **Technical difficulties:** Inefficient operation, maintenance procedures and inadequately trained technical staff are the considered to be configuration difficulties [16]. For example when unprotected short message service centres (SMSCs) receive short messages from subscribers other than their home subscribers, though the processes are carried out but are not charged afterward. Due to the vast diversity in the networks of HPMNs and VPMNs, there are more technical difficulties for prevention, detection, and automatic response systems to initiate actions against fraud.

6.1.3 IMPLEMENTATION OF BLOCKCHAIN IN THE PROCESS:

Implementation of a permissioned blockchain [6] could replace the conventional ways of sending CDR. All the communication service providers (CSPs), which have undergone roaming agreement, can broadcast CDRs on permissioned Blockchain network as shown in the figure below.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

Permissioned nature of blockchain will allow only authorized access to the network, so there will be no any chance of data invasion. A Hyperledgerblockchain [17] could be implemented to restrict the transfer of unwanted blocks of the blockchain to designated nodes [6] of VPMN and HPMN act as miners to verify the authenticity of the data broadcasted on blockchain network. Whenever a request to start an event has been initiated by a roamer, a transaction having all the details about CDR data is broadcasted on the network. Since the transfer of communication happens in runtime, the HPMN can calculate billing amount for each and every subscriber, according to their subscribed services, and also the payment to VPMN on runtime itself.

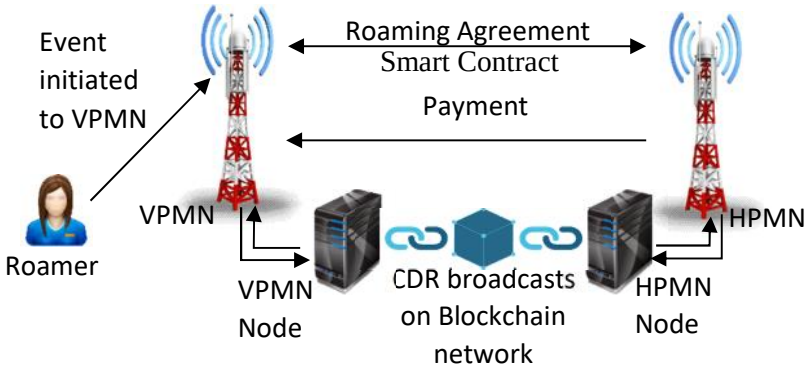

Fig. 4: Blockchain Implementation in Roaming Management

This helps to achieve certified and smooth settlement transition between HPMN and VPMN, without having fear of fraud. Moreover, in this scenario, since CDRs being transferred through blockchain network via broadcasting, so it makes the role of DCH irrelevant [6]. It helps telcos to save even more cost as this process does not require a middleman.

6.2 IoT:

We are witnessing the rise of smart cities nurtured by smart technologies. It is predicted that by 2020 there will be 200 billion connected devices, which could result into increased probability of devices being vulnerable to attacks. Frost & Sullivan, a consulting firm, forecasts that by 2020, the market for smart cities is predicted to reach $1 trillion [18].

An IoT ecosystem is an integration of multiple interconnected devices connected to a centralized hub, which in turn is connected to the IoT platform. IoT platform consumes the data generated by these smart devices to make sense of this data. To establish this network of devices internet is needed, which is catered to by Telcos.

6.2.1PRESENT SCENARIO:

A smart Hub ensures all smart devices speak the same language, which enables the users to remotely control the devices, independent of location. The data gets transmitted from smart devices to the IoT Platform, which analyses the data, applies logical algorithms and makes imparts intelligence to devices based on the usage patterns. Telecom operator plays a critical role in this ecosystem which is to ensure internet connectivity for all the devices to communicate. They can also bundle voice and SMS services along with data to perform actions based on the pre-defined logics. Telco needs to supervise crucial activities like the complex partnership models, Partner Management, Billing and Settlements as they will result in the Cost and Revenue identification [18].

Contemporary ecosystem for IoT is highly centralized and completely relies on internet [19] for any sort of communication amongst connected devices which makes it vulnerable to high level of risk if security is not prioritized.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

6.2.2ACCIDENTAL ERRORS & DELIBERATE FAULTS:

An ecosystem for IoT needs a lot of processing, power and storage space to authenticate and identify all the connected devices through centralized server, so can only support small-scale network [19].

- **Packet loss:** Irrespective of the distance between two devices, all the communication and transfer of information has been executed through the internet [19], results in packet loss and makes eco-system expensive. Packet loss is often correlated to the QoS of the ISP. Loss in packets is equal to loss in revenue for the service providers.
- **Single point of failure:** Cloud servers are used in existing IoT ecosystem which makes network highly vulnerable as failure at this point can disrupt the entire network. The causes could range from power outages to database errors to faulty software updates to overloaded servers.
- **Interoperability issues:** Cloud services are provided by multiple manufacturers and since there is no any single platform to connect all the devices [20], interoperability and compatibility issues arises. This is very dangerous because of increase in dependency of IoT in some sensitive sectors like health care.

6.2.3 IMPLEMENTATION OF BLOCKCHAIN IN THE PROCESS:

With the implementation of Blockchain technology in IoT ecosystem, one centralized model can be replaced by Distributed Digital Ledger (DDL) for all the transactions, makes it extremely secure peer-to-peer self-managed network.

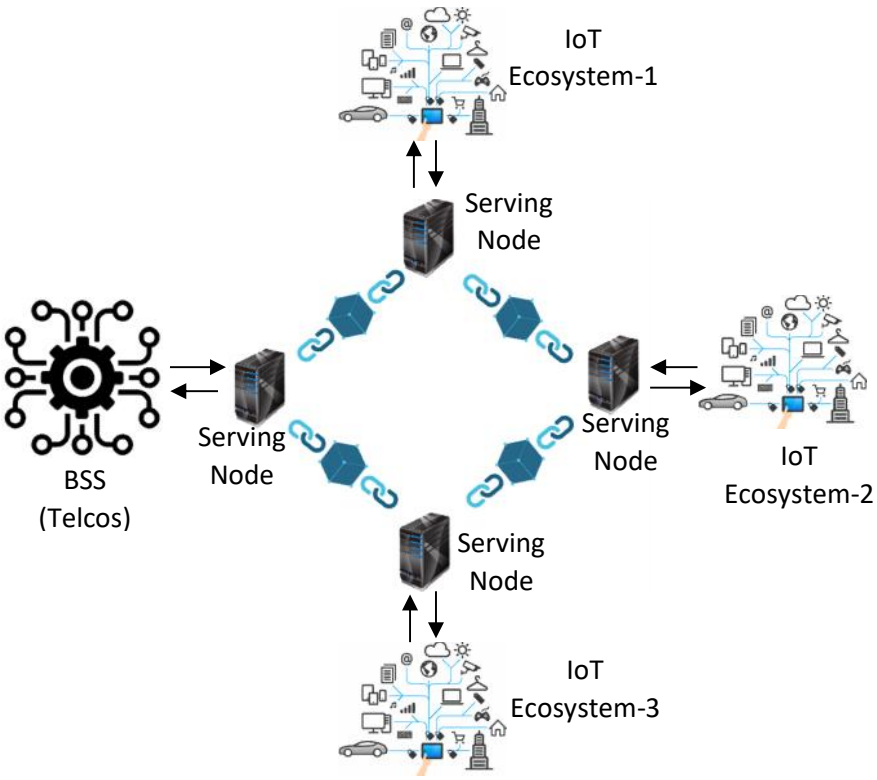

Fig. 5: Blockchain Implementation for IoT Billing

The need for securing IoT devices emerged increasingly after a massive DDoS attack on the internet which exploited several connected devices to do their bidding. The secure and tamper proof nature of cryptocurrencyblockchain can be utilized by the consortium to ensure the security of the inter-connection between various IoT devices. A blockchain technology industry consortium emerging has the potential to move forward in defining the scope and implementation of a smart contracts protocol layer across several major blockchain systems/ecosystems. Through this system the barriers to interoperability and security within

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

IoT can be overcomed and along with complementing the existing IoT platforms with a blockchain back-end to add value to IoT, supply chain, and trade finance.

6.3 MICRO PAYMENT:

Apart from basic telecommunications services, there are two other types of services which consumers get by availing telcos network – VAS and OTT services. VAS is a non-core service, provided by telcos, to add value to their entire service offerings. VAS could be standalone from operational perspective or be consolidated with some existing core services, depends upon characteristics and importance. On the other hand, OTT services are beyond the control of telcos. They just carry IP packets from source to destination through their network, but bears no control, right, claim or responsibility on these services [21]. User is free to use OTT services on their will because everyone is independent to use the internet the way they want. Telcos have to integrate VAS and SDP to provide such services to the consumers.

6.3.1 PRESENT SCENARIO:

IP packets of VAS or OTT services flow as same as the basic services offered on telcos' network. Deep Packet Inspection (DPI) is the technology used by telcos to segregate these packets. DPI enables telcos to read & scan the payloads of each packet, unlike only headers in old techniques, in run time so the decision on how to classify & control traffic on their network have been taken based on applications, content and subscribers also [22] along with origin and destination.

6.3.2 ACCIDENTAL ERRORS & DELIBERATE FAULTS:

Telcos either produce content for VAS on their own or take it from vendors. Sometimes even the OTT services are not free and subscriptions are bundled with telcos' offers. In all these collaborations, telcos bill to the consumers for the services they have used and pay money back to the vendors (VAS and OTT both) for their content, after keeping their share. Followings are the vulnerable points for revenue leakage in micro payment scenario –

- **Inability to handle IP packets efficiently:** IP packets, provided by vendors, need to be handled efficiently to the end consumer according to their subscription type and need to bill them according to the usage. Due to latency and packet losses, exact usage by the consumer in not properly calculated by the telcos but have to pay to the vendors because their content is calculated properly. Here telcos loose heavy revenue because of paying to the vendors without having billed to the consumers.
- **Interconnect issues:** Content Delivery Networks (CDNs) are enlisted to provide streaming capacity worldwide to meet demand, with has increased the importance of supporting infrastructure, deployed deep in ISP networks, close to consumers and which can boost overall delivery capacity thereby providing improved Quality of Experience for viewers.
- **OTT Frauds:** OTT Bypass, a fraud had raised an alarm in the recent times in which a normal phone call is diverted over IP to a voice chat application on a smartphone instead of being terminated over the normal telecom infrastructure. This hijack is performed by an international transit operator in coordination with the OTT service provider, but without the authorization from the caller, callee or their operators. Through this they collected a large share of the call charge thereby inducing a huge loss of revenue to the bypassed operators. This practice degrades the quality of service without providing any benefits for the users.

6.3.3 IMPLEMENTATION OF BLOCKCHAIN IN THE PROCESS:

With the implementation of blockchain technology in micropayments network, not only will transactions cost reduce but it will lead to an effective run-time billing and validation processing of transactions. Micropayments should have a blockchain network accommodating a unique scalable protocol called 'Rainden Network'. The Raiden network is a new protocol which will introduce high-speed asset transfers over the blockchainnetworks.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

This protocol can handle over one million transfers per second without running into any problems. A high number of transactions can pose a serious threat to existing financial payment networks as they are more expensive to use. The Raiden network is designed to facilitate low transaction fees, which could be 7 orders of magnitude [23] lower when compared to blockchain transactions on the current Ethereum network.

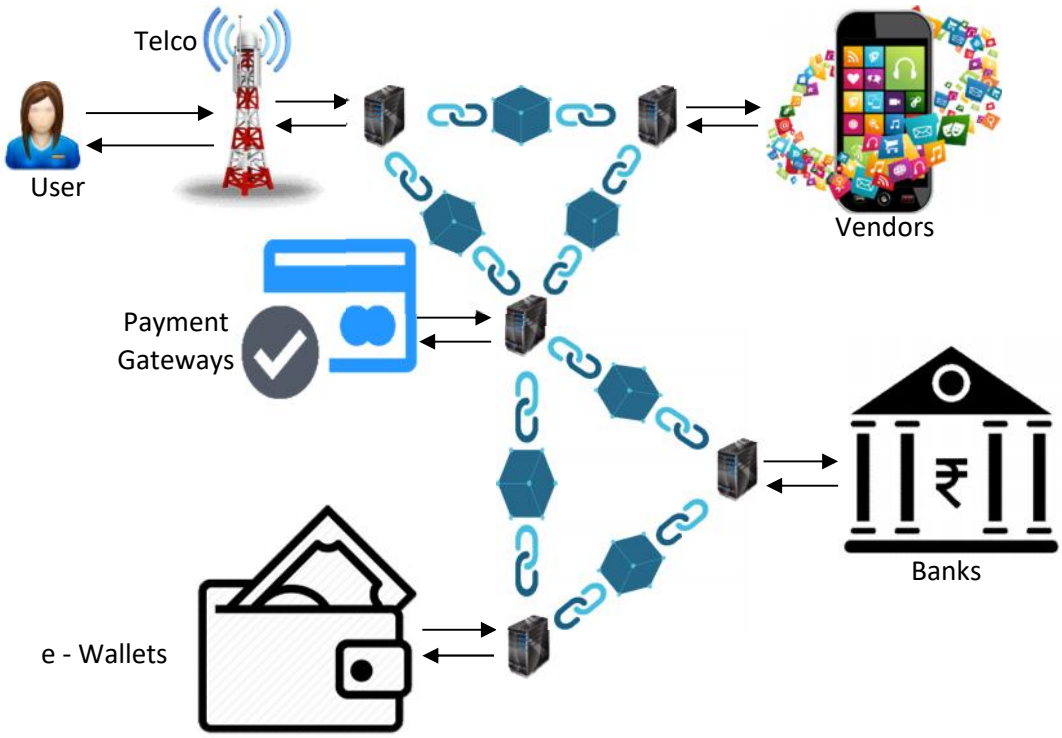

Fig. 6: Blockchain Implementation for Micro Payment

Rather than sharing all transactions on the blockchain, Raiden allows users to privately exchange messages to sign the transfer of value which is essential due to involvement to highly confidential monetary transfer. This protocol complements the existing ecosystem and makes it stronger. The first decentralized exchange on the Raiden Network, called raidEX, is already in development. This network will keep a track of runtime billing and also the content delivered for further business and trend analysis. It limits the frauds associated with bypassing.

6.4 BILLING:

Telecom service consists of four types of offerings i.e. Voice, Data, SMS, and MMS. Billing for telcos is the process consists of gathering collective usages data, apply applicable charge rates, generate the invoice to the consumers to pay the bill, receive payments from the consumers and produce acknowledgments of received payments.

6.4.1 PRESENT SCENARIO:

Telcos have divided their customers into post-paid and pre-paid segments. For post-paid customers, bills are generated on frequency based billing model and this frequency can be twice per month, once in a month, once in three months or could be anything depends upon individual subscribers' type of subscription. In this case, telcos need not generate bills at run time and they get enough time for reconciliation, so there is very less

chance for revenue leakage unlike pre-paid, where telcos have to generate bills and deduct the amount from customers' available balance on run time.

As we see billing for pre-paid customers is more vulnerable to revenue leakage than pre-paid, so here we will discuss only pre-paid scenario. Every time when a pre-paid customer uses any service, Service Delivery Platform (SDP) comes into the picture. SDP, a set of components, enables telcos to provide all digital services over the legacy network. It checks data related to tariffs, promotional plans, subscriber lifecycle, operation & maintenance, provisioning, deployment etc. It is an integral part of telcos business processes and comes under Intelligent Network (IN). IN is a network architecture in which service logic is taken out of the switch and has distributed throughout the network, enables telcos to introduce and to control new capabilities more efficiently and rapidly i.e. customised services for every individual without having redesigned switching equipment.

Actual billing process starts when a service is used by a customer. Mediation system gathers usage data from network switch in raw format and converts that in systematic Call Details Record (CDR). This CDR is then being rated by Rating Engines according to types of call, calling plans, origin & termination places, time & duration of call etc. followed by generation of invoice. After that, all the necessary adjustments are done in terms of applicable discounts and invoice is sent to the customers for the payment of the bill.

6.4.2 ACCIDENTAL ERRORS & DELIBERATE FAULTS:

Proper billing for services offered is the primary need of telcos. If they cannot bill the customers for their offerings, then they cannot survive in today's competitive word where there is already very less scope of billing is left and telcos are struggling to find new areas to generate revenue. Followings are the primary reasons for revenue leakage in billing –

- **Improper integration of network elements:** When a customer requests to unsubscribe from any service, that request goes to HLR (to stop providing services) and to BSS system (to stop deduction of charges). But sometimes due to the improper integration of network elements, this communication is not received properly to HLR. In this condition that service has not been stopped but BSS system has received the request so it has stopped charging for that service and even has sent the acknowledgment to the customer about the successful implementation of his request. So basically that customer still enjoying that service because getting billed for that. Even if this fault is detected, telcos cannot bill to the customer because customer had received the acknowledgment regarding the termination of service. This is the biggest revenue leakage for telcos due to lack of integration of network elements.
- **Introduction of new products:** Whenever telcos announce a new product, OSS/BSS system along with core network elements need to communicate well about the new price slabs.
- **Incomplete usage information:** Changing trends in technologies, introduction of various types of services and convergence has increased network elements manyfold and network becomes more and more complex. Sometimes switch cannot record all the usage data due to this load or even the data has been recorded but due to scalability issues, mediation system cannot convert all those data into proper CDR format.

6.4.3 IMPLEMENTATION OF BLOCKCHAIN IN THE PROCESS:

Implementation of permissioned blockchain for billing purpose include the elements of core network along with OSS/BSS system. In core network, switch and various registers can be put on blockchain network. It will help the switch to fetch all the information regarding consumers in run-time. Third node of this blockchain will be OSS/BSS systems, enabling them to be in sync with switch and registers.

All three nodes will work as miner on this blockchain network and when a consumer raises any request to subscribe or unsubscribe from any service, that request will be put on blockchain network by BSS and the nodes of switch and registers will update themselves accordingly through their nodes. Every status updating related to consumer in any of these systems will be broadcasted on blockchain network on run-time and others systems will keep themselves in sync with that information in run-time.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 10
October 2017

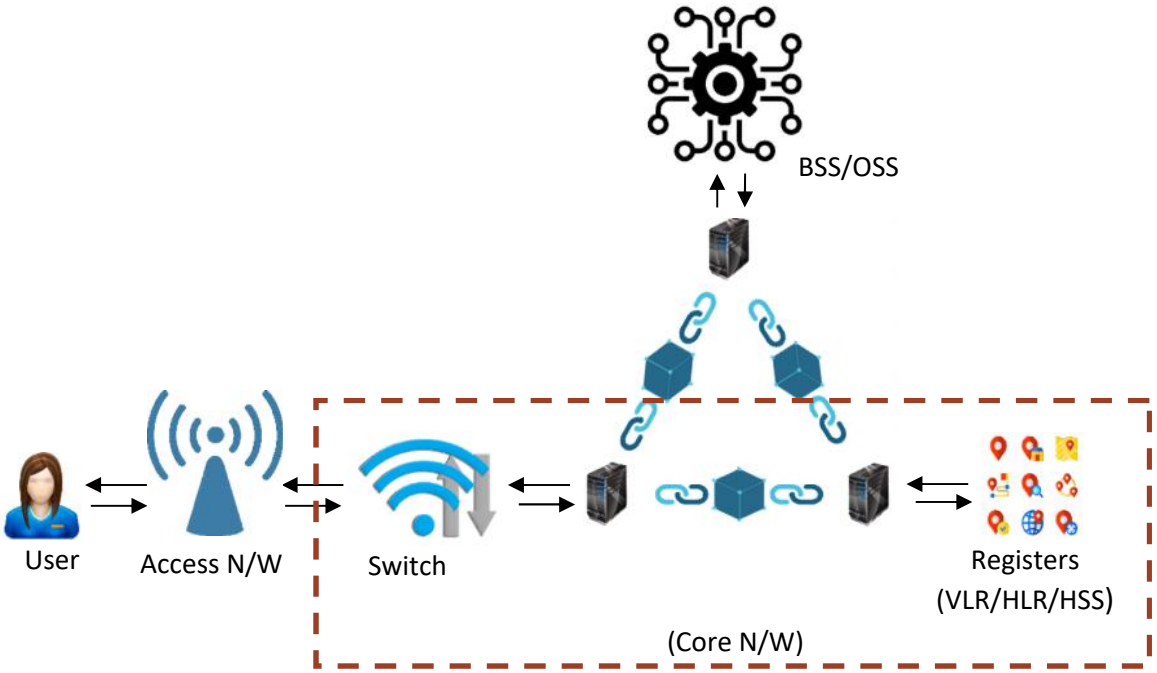

Fig. 7: Blockchain Implementation for Billing

Major improvement from the existing system will be seen as the same information getting updated in BSS and registers. So if BSS has unsubscribe a consumer for getting billed from one particular service, home location register too will unsubscribe that consumer to avail that particular service and vice-versa. The major problem of revenue leakage will be solved by the implementation of blockchain as consumers now get billed for every service which they are using. This not only improves service efficiency of telcos but also improve customer service experience.

7. CONCLUSION:

Blockchain technology has a lot of potential to streamline day-to-day business processes of enterprise, especially the introduction of smart contract with partners and run-time broadcasting capabilities of information on the network in all possible secure way. Through our proposed models of implementation, in place of the current nervous system for roaming, IoT, micropayments and billing; we could reduce the limitations of throughput, latency,bandwidth consumption and resource utilization which have been the root causes of revenue leakage and frauds globally. Our research also highlights the upcoming protocols and software such as Raiden Network and Hyperledger being developed by start-ups and technology giants to overcome the challenges of blockchain.

Many industries have already adapted blockchain in their business model and getting benefits in terms of run time load balancing, transfer of information, business transactions, to name a few. Telecom industries can cater their biggest need to make their service offerings elastic according to changing demand and billing process leak proof. Though blockchain in applications is certainly an interesting area for future research, but the moment highlights the technical limitations and challenges it suffers. Anonymity, data integrityand security attributes may solve limitations of many processes but scalability is an issue that needs to be solved for future needs. Therefore, to evaluate what challenges questioned are the most problematic issues in Blockchain at the moment which can be addressed by further research and testing.

8. REFERENCES:

[1] Maverick, J.B. July 16, 2015. What portion of the global economy is comprised of the telecommunications sector.http://www.investopedia.com/ask/answers/071615/.
[2] GSMA Press release. January 5, 2016. Telecoms operators face $300bn global loss from uncollected revenue and fraud in 2016.
[3] Insurance Law & Practice. Module 3.Elective Paper 9.3.The Institute of Company Secretaries of India.
[4] How Much Data Does The World Generate Every Minute. July 26, 2017. https://www.domo.com/news/press/how-much-data-does-the-world-generate-every-minute.
[5] Ravi SankarDamineni, Kapil Kumar Sardiwal, Sita Ram Waghle, M.B Dakshyani. 2015 Jan-Feb.A comprehensive comparative analysis of articles retracted in 2012 and 2013 from the scholarly literature.J IntSocPrev Community Dent.
[6] Deloitte.How blockchain can be impacted the telecommunications industry and its relevance to the C-Suite.Blockchain@Telco.
[7] KPMG.March 2017. Emerging trends in risk management.
[8] The difference between a Private, Public & Consortium Blockchain, http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html.
[9] EY Publication, A powerful and effective answer to revenue leakage.
[10] Opennet Press release. 27th February, 2017. 91% Global Operators View Real-Time Assurance as a Key Priority for Revenue Protection.
[11] Knowledge @ Wharton. May 18, 2017.The Promise and Perils of 'Smart' Contracts.
[12] Blockchain Technologies. Smart Contracts Explained. http://www.blockchaintechnologies.com/blockchain-smart-contracts.
[13] The Funds Chain. January 2, 2017. White Paper extract #4: Smart Contract.
[14] Preethi Mohan. October 17, 2016. Global mobile wallet using Blockchain, IBM BlockchainDevCenter.
[15] Starhome Mach. Press Release. December 20, 2016.New Starhome Mach Solutions Address Business Challenges Under EU Commission's Roam-like-home and Fair Usage Policies.
[16] Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, Jesus Diaz-Verdejo. December 2009. Fraud in Roaming Scenarios: an Overview.IEEE Wireless Communication.
[17] Hyperledger-Blockchain Technologies for Business. https://www.hyperledger.org/.
[18] Subex Blog. Feb 9, 2017. IoT Don't Be In the News for Wrong Reasons: Stay Ahead of Cyber Attacks.
[19] Ben Dickson. Jun 28, 2016.Decentralizing IoT networks through Blockchain.https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/.
[20] Dan Cummings. March 4, 2017. ETHNews.How Will The Blockchain Reinforce The Telecommunications Industry.
[21] NadeemUnuth. February 23, 2017. What is OTT and How is it Affecting Communication. https://www.lifewire.com/what-is-ott-3426369.
[22] Deep Packet Inspection. White paper.Telecommunication Engineering Center.Ministry of Communications, Government of India.
[23] Blockchain Research. March 28, 2017.Blogpost.What is the RaidenNetwork.