

Blockchain And Cloud Computing
In Engineering Application

OrangeBooks Publication

Smriti Nagar, Bhilai, Chhattisgarh - 490020

Website:www.orangebooks.in

© **Copyright, 2022, Author**

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form by any means, electronic, mechanical, magnetic, optical, chemical, manual, photocopying, recording or otherwise, without the prior written consent of its writer.

First Edition, 2022

ISBN: 978-93-5621-071-4

Price: Rs.500.00

The opinions/ contents expressed in this book are solely of the authors and do not represent the opinions/ standings/ thoughts of OrangeBooks or the Editors .

Printed in India

BLOCKCHAIN AND CLOUD COMPUTING IN ENGINEERING APPLICATION

NATARAJAN R



OrangeBooks Publication
www.orangebooks.in

Index

Part – 1 Block Chain In Engineering Application

Chapter - 1

Introduction To Block Chain Technology 1

Chapter - 2

Block Chain Technology In Telecom Industry 9

Chapter - 3

Blockchain In Wireless Telecom Communications 33

Chapter - 4

Wireless 6G in Blockchain Technology 44

Chapter - 5

Security Of Block Chain In Telecom Operations..... 68

Part – 2 Cloud Computing In Engineering Application

Chapter - 6

Introduction To Cloud Computing 97

Chapter - 7

Cloud Computing In Service Providers 104

Chapter - 8

Cloud Storage With Blockchain Technology 144

Chapter - 9

Applications Of Cloud Computing 159

Chapter - 10

Data Security In Cloud SaaS (Software As A Service)..... 170

Chapter - 11

Integrating Cloud Computing & Block
Chain in Engineering Application 190



PART – 1
BLOCK CHAIN IN
ENGINEERING APPLICATION

CHAPTER - 1

Introduction To Block Chain Technology

Blockchain was first introduced as the core technology behind Bitcoin, the headline-grabbing decentralized digital currency ecosystem proposed in 2008. The appeal of blockchain technology lies in its use of peer-to-peer network technology combined with cryptography. This combination enables parties who do not know each other to conduct transactions without requiring a traditional trusted intermediary such as a bank or payment processing network.

By eliminating the intermediary and harnessing the power of peer-to-peer networks, blockchain technology may provide new opportunities to reduce transaction costs dramatically and decrease transaction settlement time. Blockchain has the potential to transform and disrupt a multitude of industries, from financial services to the public sector to healthcare. As a result, a number of venture capital firms and large enterprises are investing in blockchain technology research and trials to re-imagine traditional practices and business models. Blockchain technology has the potential to impact all recordkeeping processes, including the way transactions are initiated, processed, authorized, recorded and reported. Changes in business models and business processes may impact back-office activities such as financial reporting and tax preparation. Independent auditors likewise will need to understand this technology as it is implemented at their clients. Both the role and skill sets of CPA auditors may change as new blockchain-based techniques and procedures emerge.

For example, methods for obtaining sufficient appropriate audit evidence will need to consider both traditional stand-alone general ledgers as well as blockchain ledgers. Additionally, there is potential for greater standardization and transparency in reporting and accounting, which could enable more efficient data extraction and analysis.

Blockchain technology could bring new challenges and opportunities to the audit and assurance profession. While traditional audit and assurance services will remain important, a CPA auditor's approach may change. Just as the audit and assurance profession is evolving today, with audit innovations in automation and data analytics, blockchain technology may also have a significant impact on the way auditors execute their engagements. Moreover, CPAs may need to broaden their skill sets and knowledge to meet the anticipated demands of the business world as blockchain technology is more widely adopted. A blockchain is a digital ledger created to capture transactions conducted among various parties in a network. It is a peer-to-peer, Internet-based distributed ledger which includes all transactions since its creation. All participants (i.e., individuals or businesses) using the shared database are "nodes" connected to the blockchain,⁵ each maintaining an identical copy of the ledger. Every entry into a blockchain is a transaction that represents an exchange of value between participants (i.e., a digital asset that represents rights, obligations or ownership). In practice, many different types of blockchains are being developed and tested. However, most blockchains follow this general framework and approach.

When one participant wants to send value to another, all the other nodes in the network communicate with each other using a pre-determined mechanism to check that the new transaction is valid. This mechanism is referred to as a consensus algorithm.⁶ Once a transaction has been accepted by the network, all copies of the ledger are updated with the new information. Multiple transactions are usually combined into a "block" that is added to the ledger. Each block contains information that refers back to previous blocks and thus all blocks in the chain link together in the distributed identical copies. Participating nodes can add new, time-stamped transactions, but participants cannot delete or alter the entries once they have been validated and accepted by the network. If a node modified a previous block, it would not sync with the rest of the network and would be excluded from the blockchain. A properly functioning blockchain is thus immutable despite lacking a central administrator.

Near real-time settlement	A blockchain enables the near real-time settlement of transactions, thus reducing risk of non-payment by one party to the transaction.
Distributed ledger	The peer-to-peer distributed network contains a public history of transactions. A blockchain is distributed, highly available and retains a secure record of proof that the transaction occurred.
Irreversibility	A blockchain contains a verifiable record of every single transaction ever made on that blockchain. This prevents double spending of the item tracked by the blockchain.
Censorship resistant	The economic rules built into a blockchain model provide monetary incentives for the independent participants to continue validating new blocks. This means a blockchain continues to grow without an "owner". It is also costly to censor.

1.1 Characteristics of Block Chain:

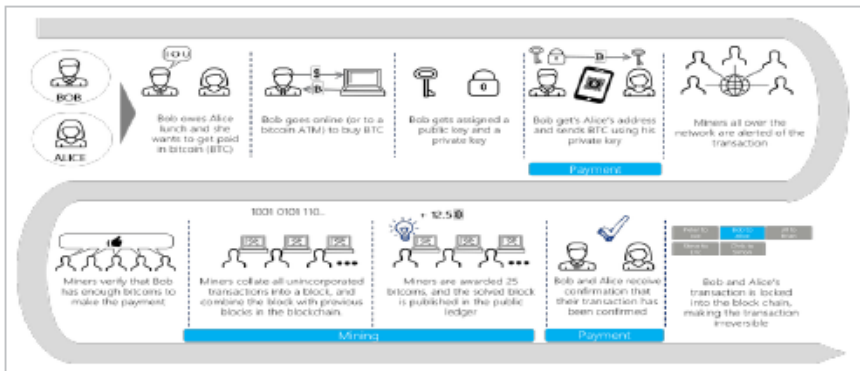
A major advantage of blockchain technology is its distributed nature. In today's capital markets, the transfer of value between two parties generally requires centralized transaction processors such as banks or credit card networks. These processors reduce counterparty risk for each party by serving as an intermediary but centralize credit risks with themselves. Each of these centralized processors maintains its own separate ledger; the transacting parties rely on these processors to execute transactions accurately and securely. For providing this service, the transaction processors receive a fee. In contrast, a blockchain allows parties to transact directly with each other through a single distributed ledger, thus eliminating one of the needs for centralized transaction processors.

In addition to being efficient, the blockchain has other unique characteristics that make it a breakthrough innovation. Blockchain is considered reliable because full copies of the blockchain ledger are maintained by all active nodes. Thus, if one node goes offline, the ledger is still readily available to all other participants in the network. A blockchain lacks a single point of failure. In addition, each block in the chain refers to the previous blocks, which prevents deletion or reversing transactions once they are appended to the blockchain. Nodes on a blockchain network can come and go but the network integrity and reliability will remain intact as long as it is being used. In this way, no single party controls a blockchain and no single party can modify it or turn it off. CPA auditors should be aware that blockchain technology is a new form of database and each blockchain implementation may have different characteristics that make it unique. While the

technology is emerging, there is a risk that a specific blockchain implementation does not live up to the promise of the technology. In the current ecosystem, there are two major classifications of blockchain networks: permissionless and permissioned. The biggest difference is the determination of which parties are allowed access to the network. A blockchain may be shared publicly with anyone who has access to the Internet (i.e., permissionless or “public” blockchain), or shared with only certain participants (i.e., permissioned or “private” blockchain).

1.2 Permissionless Blockchain:

permissionless blockchain is open to any potential user. For example, the Bitcoin blockchain is a public or permissionless blockchain; anyone can participate as a node in the chain by agreeing to relay and validate transactions on the network thereby offering their computer processor as a node. Joining the blockchain is as simple as downloading the software and bitcoin ledger from the Internet. Because the blockchain maintains a list of every transaction ever performed, it reflects the full transaction history and account balances of all parties. Figure 1 is an example of a transfer of bitcoin (BTC) from one individual to another. When one party sends bitcoin (i.e., buyer sending value) to another party (i.e., seller receiving value), the Bitcoin blockchain is updated by the following process, including a process referred to as “mining”.



An example of a bitcoin transaction which is a public/permissionless blockchain: peer-to-peer payment over the Bitcoin network. **Note:** Permissioned blockchains may have consensus protocols that may be similar to or different from Figure 1 because they are dependent on the agreement of the participants.

While a permissionless blockchain lives up to the potential of the technology by allowing anyone access, it can have limitations that are difficult to remedy. For example, when the blockchain is created, transaction volume or size may be set to the best available technology at the time. As technology advances, initial settings may become limitations that may make the blockchain out of date, potentially slowing transaction speeds. Users of permissionless blockchains should also be aware that their transaction history is exposed to anyone who downloads the database for as long as the database is active. While it may be difficult for an outside party to identify a participant on the blockchain, if a participant is identified, their entire transaction history would be public.

1.3 Permissioned Blockchain:

The limitations of permissionless blockchains have led some organizations to explore the use of private or permissioned/consortium blockchains, which restrict participation in the blockchain network to participants who have already been given permission by agreed-upon administrators. These blockchains address some of the drawbacks of public blockchains, but also sacrifice some of the potential benefits (e.g., decentralized transactions, wide distribution of the ledger, and a truly decentralized environment without any intermediaries). Permissioned blockchains are likely to be set up by a consortium of parties that can collectively benefit from a shared ledger system. For example, a supply chain network may want to use a blockchain to track the movement of goods.

Given the widely acknowledged limitations inherent in public blockchains, private or permissioned/consortium blockchains are expected to have a higher adoption rate in the near term, especially in enterprise environments. However, adoption of public blockchains is also expected to increase in the longer term once the key infrastructure and technical challenges of the new technology have been addressed. The paradigm shift introduced by blockchain (and the level of interest in blockchain-based initiatives) in many ways parallels the development of the Internet in the 1990s. With Internet technology, there was a strong initial emphasis on corporate intranets until a critical mass was reached and the broader public Internet began to offer more benefits to offset the perceived risks of participating in an open network.

1.4 Evolution Of Block Chain:Smart Contracts:

A key development in blockchain technology was the introduction of smart contracts. Smart contracts are computer code stored on a blockchain that executes actions under specified circumstances. They enable counterparties to automate tasks usually performed manually through a third-party intermediary. Smart-contract technology can speed up business processes, reduce operational error, and improve cost efficiency.

For example, two parties could use a smart contract to enter into a common derivative contract to hedge the price of oil at the end of the year. Once the terms of the contract have been agreed to, it is appended to the blockchain and the wagered funds are held in escrow and registered on a blockchain. At year end, the smart contract would read the price of oil by referencing a trusted source defined in the smart contract (known as an “oracle”), calculate the settlement amount, and then transfer funds to the winning party on the blockchain. Ethereum⁹, at the time of publication the second largest blockchain network after Bitcoin (based on market capitalization), was the first platform to introduce the concept of a smart contract that could be deployed and executed on a distributed blockchain network. Ethereum is a public protocol that allows anyone accessing the Ethereum blockchain network to view the terms of each contract unless they are protected by encryption.

This may prove problematic for contracts involving sensitive information (e.g., a hedge fund using smart contracts to execute a proprietary investment strategy or to quietly build a position in a particular stock).However, developers are actively building solutions to preserve confidentiality while taking advantage of public blockchains. Even with such perceived limitations, there is significant market interest across industries in smart contract applications because they could transform the processing and settlement of a wide range of contracts, from hedging and futures derivatives to automated payments under lease contracts.

Smart contracts are a method to automate the contracting process and enable monitoring and enforcement of contractual promises with minimal human intervention. Automation can improve efficiency, reduce settlement times and operational errors. Because using smart contract technology requires the translation of all contractual terms into logic, it

may also improve contract compliance by reducing ambiguity in certain situations.

As smart contracts continue to evolve, inherent risks may emerge that need to be mitigated. For example, when setting up a smart contract, the parties may decide not to address every possible outcome, or they may include some level of flexibility so they do not limit themselves. This could lead to smart contracts with vulnerabilities or errors that could lead to unexpected business outcomes. Parties may find it difficult to renegotiate the terms of a deal or modify terms due to an unforeseen error. Also, incomplete or flexible contracts can lead to settlement problems and disputes. Perhaps most importantly, however, at the date of this publication, smart contracts have not been tested thoroughly in the court system. Nevertheless, smart contracts offer a compelling use case for blockchain adoption.

Blockchain technology offers the potential to impact a wide range of industries. The most promising applications exist where transferring value or assets between parties is currently cumbersome, expensive and requires one or more centralized organization. A specific activity attracting significant interest is securities settlement, which today can involve multi-day clearing and settlement processes between multiple financial intermediaries. Certain financial services experts believe the financial services industry is on the verge of being disrupted: advances in innovative technologies such as blockchain are expected to transform the industry and its workforce by automating many of the activities currently performed by humans.

Since all businesses track information and face the challenge of reconciling data with counterparties, blockchain technology has the potential to be relevant to everyone. The first major adoptions, however, may transform business processes and old legacy systems that are cumbersome to maintain.

The table below illustrates industries where interest in blockchain technology and its potential transformative benefits has been high, as demonstrated by significant investments from both venture capital firms and large enterprises.

Financial services	Several stock exchanges around the world are piloting a blockchain platform that enables the issuance and transfer of private securities. Additionally, multiple groups of banks are considering use cases for trade finance, cross-border payments, and other banking processes.
Consumer and industrial products	Companies in the consumer and industrial industries are exploring the use of blockchain to digitize and track the origins and history of transactions in various commodities.
Life sciences and healthcare	Healthcare organizations are exploring the use of blockchain to secure the integrity of electronic medical records, medical billing, claims, and other records.
Public sector	Governments are exploring blockchain to support asset registries such as land and corporate shares.
Energy and resources	Ethereum is being used to establish smart-grid technology that would allow for surplus energy to be used as tradable digital assets among consumers.



CHAPTER - 2

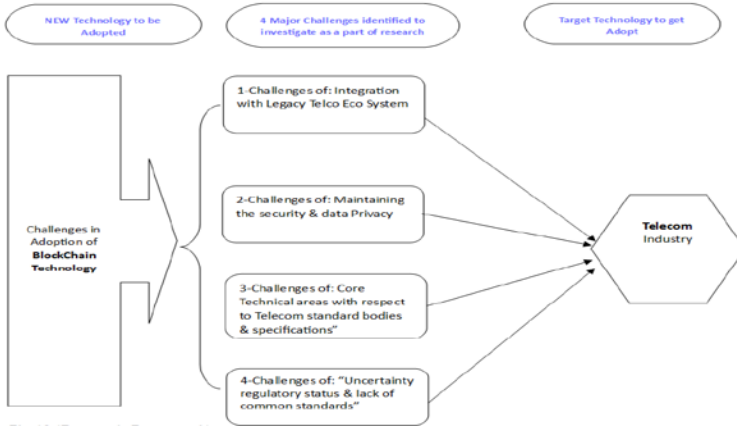
Block Chain Technology In Telecom Industry

The telecommunications industry is within the sector of ICT called as information and communication technology and it is made up of telephone companies and internet service providers and plays the crucial role in the evolution of mobile communications and the information society. The telecommunications sector comprises companies that make communication possible on a global scale, whether it is through the phone or the Internet, through airwaves or cables, through wires or wirelessly. These companies created the infrastructure that allows data in words, voice, audio or video to be sent anywhere in the world. The largest companies in the sector are wireless operators, satellite companies, cable companies and Internet service providers.

The Technology adoption is the choice to acquire and use a new innovation. And in extent by which a given technology becomes accepted and incorporated into approved social practices, also the stage at which a technology is mentally accepted by an individual or an organization. In order for a technology to be used, it should be adopted first. There are a number of adoption models available in the field of Information Systems. These models predominantly look at the behavior aspects leading to adoption. Challenges means Difficulties faced while trying to reach or adopt a goal/target and either Target to be reached by creating applicable plan, or a threat for the company which must be planned, monitored and executed by high management.

Innovation in turn, classifies the different technological innovation levels into: principal, secondary or accessory. Principal innovation concerns the transformation of an invention into products or processes, new or

improved. On the other hand, secondary or accessory innovations are the subsequent changes that introduce corrections in the principal innovation and that occur during the experimental or definitive production or sales stages.



Based on our objective and as this research involves the study & investigation of the challenges while adopting the new technology (Block chain) in to the telecom sectors and our Target population are the

- Telecommunication experts
- Solution architects
- Telecommunication industry decision makers.

So the above mentioned target population is very limited to telecom industry and particular to certain management levels hence this study will be collecting data through Interview method, because it will be more effective in terms of understanding the perceptions of target. regulatory status & lack of common standards.

A Blockchain's 'empowered' trust improves coordination between different accomplices, because of a mutual perspective on exchanges and liabilities. This thus allows the end of outsiders, bringing about cost reserve funds. Encourages a solitary perspective on information rather than the requirement for solidification crosswise over different unique frameworks. Additionally, takes into consideration dependable review trails because of the historical backdrop of all exchanges being accessible in the record.

Usage of keen contracts in meandering and different cases considers close prompt charging, in this manner prompting improved income affirmation and extortion decrease. Potential to encourage new plans of action for income age for Communication Service Provider who are searching for new roads to expand both top and main concerns. A Blockchain can go about as the record that empowers, for instance, a M2M economy to thrive dependent on the basic Qualitative Approach was chosen to carry out this research to develop opportunities by investigating the Blockchain adoption challenges in telecommunication industry stage accessible, in which M2M exchanges can be recorded. It would thus be able to go about as the empowering agent for an IoT biological system.

Which will be based on the end to end telecom management protocols & processes of a mobile network product & Operators where ITU standard & other telecommunication regulatory bodies guidelines are taken into considerations After the hypothesis' foundation, examine structure, definition of the starter plan, the arrangement structure and its specialized determinations were approved and did investigation through Interviews. The information gathered out of each meeting was broke down and used to create the outcomes.

The outcomes results will demonstrate that Blockchain innovation technology is relevant to the Telecommunication space domain of the product line & operator line of telecommunications industry with the challenges which are mentioned in the objectives, and results clear indicates & can map Which will be based on the end to end telecom management protocols & processes of a mobile network product & Operators where ITU standard & other telecommunication regulatory bodies guidelines are taken into considerations After the hypothesis' foundation, examine structure, definition of the starter plan, the arrangement structure and its specialized determinations were approved and did investigation through Interviews.

The information gathered out of each meeting was broke down and used to create the outcomes. The outcomes results will demonstrate that Blockchain innovation technology is relevant to the Telecommunication space domain of the product line & operator line of telecommunications industry with the challenges which are mentioned in the objectives and

results clearly indicate & can map with respective Challenges in terms of Maintaining the security & data Privacy” during adoption of Blockchain technology in telecom industry .

Results likewise bolster that receiving a few Blockchain arrangements over the association will make to create many challenges to existing infrastructure and at the same time add value by making another venture information engineering model, molded around the uprightness of changeless, auditable information and procedure controls. Also results shows that there is enough number of technical Challenges in terms of Core Technical areas with respect to Telecom standard bodies & specifications during adoption of Blockchain technology in telecom industry , The outcomes likewise demonstrate that receiving Blockchain innovation in a multi-seller condition has testing and positive effects on authoritative conduct, hierarchical culture and proficiency and will be having the Challenges of Integration with Legacy Telecom Eco System during adoption of Blockchain technology in telecom industry & challenges with respect to the Uncertainty regulatory status & lack of common standards” during adoption of Blockchain technology in telecom industry. with respective Challenges in terms of Maintaining the security & data Privacy” during adoption of Blockchain technology in telecom industry Results likewise bolster that receiving a few Blockchain arrangements over the association will make to create many challenges to existing infrastructure and at the same time add value by making another venture information engineering model, molded around the uprightness of changeless, auditable information and procedure controls. Also results shows that there is enough number of technical Challenges in terms of Core Technical areas with respect to Telecom standard bodies & specifications during adoption of Blockchain technology in telecom industry , The outcomes likewise demonstrate that receiving Blockchain innovation in a multi-seller condition has testing and positive effects on authoritative conduct, hierarchical culture and proficiency and will be having the Challenges of Integration with Legacy Telecom Eco System during adoption of Blockchain technology in telecom industry & challenges with respect to the Uncertainty regulatory status & lack of common standards” during adoption of Blockchain technology in telecom industry.

Blockchain solutions will have to be integrated with legacy Telco systems, which may require development of specialized solutions. OSS/BSS integration. Blockchain technology stack' integration with operators' internal systems may require middle ware layers in operators' technology stacks. This transition could be facilitated by digitization of more functions in operators' network stacks. Third-party integration. A centralized interoperability solution may be required to integrate with other operators and third parties (to verify users' access credentials, for example). Operators will need to assess whether the cost of integrating Blockchain technology distributed ledgers offsets their benefits. The need to implement centralized authentication systems, for example, could negate the advantages of decentralized ledgers over other data architectures.

The throughput of the database which is the quantity of exchanges every second that the database can deal with, the entrance time of the database and extricating some essential data about each square, just as estimations of its entrance/search time. The idleness of the database which is the time between the exchange inception and its endorsement and regulation in a square. The hidden stockpiling of Blockchain is with just restricted backings for information get to. Also, Blockchain information are exceedingly packed before put away to hard circle, making it harder to have an understanding of these profitable informational collection. The deferral brought about by the preparing required for the agreement of the hubs engaged with achieving the accord. Making full repetition in the connections between the diverse framework components to ensure interconnectivity if there should arise an occurrence of a solitary connection disappointment. The limit (data transfer capacity) of the connections utilized in the interconnections of the arrangement must satisfy the exchanges rate and the traffic between the center hubs of the arrangement.

The help and upkeep expenses of the organization and support of the Blockchain database. the legally binding contemplations a broadcast communications administrations supplier needs to take showing to sellers and providers that a typical Blockchain database will be utilized by different merchants too without focal organization from a particular merchant over the database, the requirement for exhaustive audits for the shrewd contracts includes that can be utilized to computerize the procedure

and furthermore should be commonly concurred between all the procedure partners to guarantee that they genuinely mirror the business rationale of the procedure.

In light of the investigation, it gives higher security and client responsibility because of the utilization of private keys rather than individual certifications, which restricts people from performing exchanges in the interest of one another. This will guarantee the full responsibility of every individual or element over their record and its exchanges, which limits clashes among groups and encourages compromise.

The sealed attributes and unchanging nature to hacking nature of the database qualify it to go about as the novel operational history storehouse of the considerable number of activities that have been performed under the procedures it encourages and that history turns into the sole wellspring of actualities if there should be an occurrence of question or struggle since it contains an auditable trail of marked exchanges. Likewise, the upgraded strength offered by the Blockchain design, as there is no single purpose of disappointment, which is the situation when utilizing a brought together social database, giving the association higher shortcoming –resilience, and higher business coherence measures.

In light of the investigation of the outcomes it is can be reasoned that the essential inalienable attributes of Blockchain innovation as permanence and disintermediation can resolve administration the executive's challenges as trust between various merchants, clear responsibility and less clashes in the media communications segment. Another Key suggestion is concentrating how new undertaking information engineering models can rise when an association receives Blockchain arrangements in various areas and in part moving current center procedures and functionalities performed by customary ERP and CRM frameworks to Blockchain based frameworks.

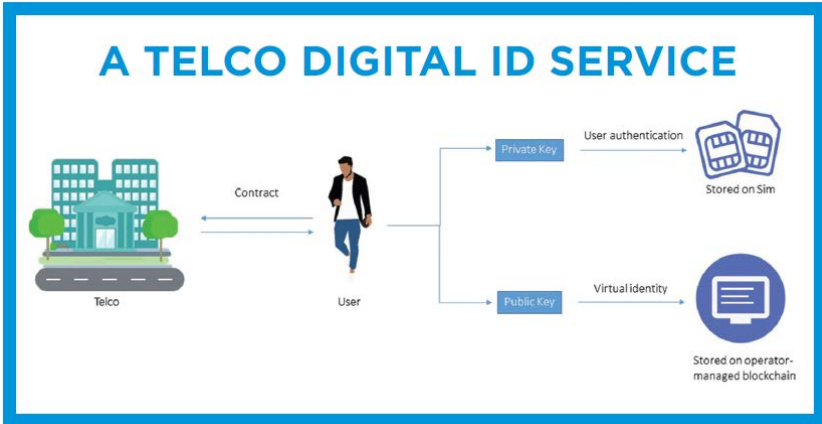
2.2 Regulating Block Chain Based Telecom Applications:

Since Bitcoin was the first application of blockchain technology, it has shaped the public perception of what blockchain is. However, Bitcoin is best thought of as a particular implementation of blockchain technology designed for a specific use case, namely to support value transfers between

pseudonymous parties without going through a trusted intermediary. It is an example of a public blockchain (also called open or permissionless). This means anybody can join the network as a node and store a local copy of the ledger. Some worry that such public blockchains are beyond the reach of the law. Take Bitcoin – developers make the Bitcoin software publicly available as open-source software. Thousands of Bitcoin nodes around the world then download and run the software on their local machines. Now imagine you are a regulator trying to impose anti-money laundering regulations on the Bitcoin network. Who do you target with your regulation? Who do you enforce against? Fining individual node operators wouldn't shut down the rest of the network.

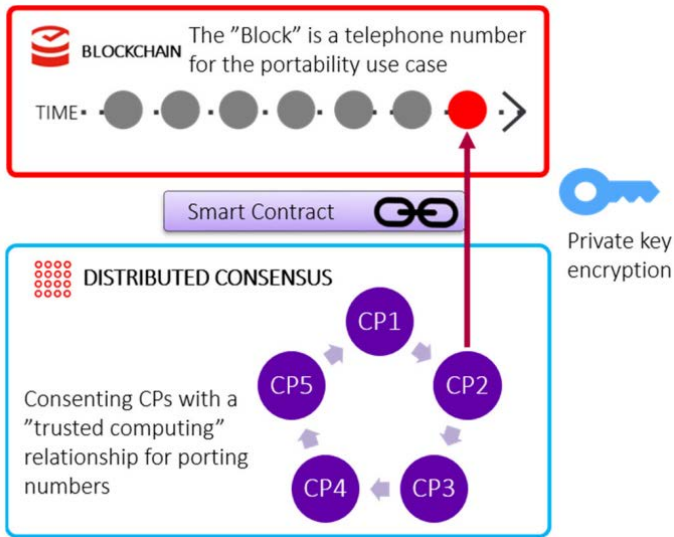
In some respects, the regulatory challenge is similar to that presented by peer-to-peer file-sharing services, like BitTorrent. Software developers make the BitTorrent protocol and client software available for download. Thousands of users around the world then download and run the software on their local machines and can make their files available for others to download. Files are stored in small pieces across many different machines, instead of on centrally controlled servers. Since Napster emerged in 1999, such networks have been used for the unlicensed dissemination of copyrighted works. As there is no central party that controls the content, it is difficult to effectively prevent copyright infringement. Sending notice-and-takedown letters to individual file-sharers doesn't affect the rest of the network.

Nonetheless, courts and legislatures have found ways to regulate copyright-infringing peer-to-peer file-sharing. For example, instead of targeting individual users, many European jurisdictions require ISPs to restrict their subscribers' access to websites that index so-called magnet links to copyrighted works, like The Pirate Bay.

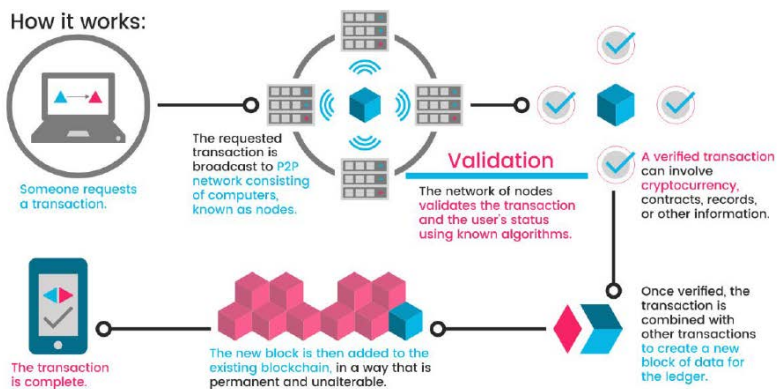


Generally speaking, fears of blockchain systems being somehow immune to regulation are overblown.⁸ First, blockchain technology can be applied in a variety of ways to create applications with different properties. It is unlikely that the blockchain components deployed in telecoms will resemble public blockchain systems like Bitcoin. Instead, operators will use private blockchain systems (also called closed or permissioned), where copies of the ledger are controlled by a closed group of vetted participants. For example, a consortium of carriers could act as the nodes that collectively control the blockchain. They could design and manage the application so as to comply with relevant regulations.

Second, even completely open blockchains like Bitcoin are not immune to regulation. Instead, regulators can control their use by identifying and then targeting any centralised or concentrated activities within the value chain. For example, many Bitcoin users rely on intermediaries that provide an interface to the blockchain system, such as online wallets like Blockchain.info, or online exchanges like Coinbase. These services are provided by companies that can be regulated.



Finally, for particularly high-risk cases, courts could order internet service providers to perform deep packet inspection and filter out certain unwanted blockchain traffic – though this may raise privacy concerns. In sum, there are various ways to regulate systems that use blockchain technology. Consequently, the more pertinent question is not whether regulators can regulate blockchain, but whether they should, and if so, how. It is too early to answer that question in the abstract. The specific regulatory and policy concerns will differ for each blockchain application – although some specific concerns can be foreseen.



The Telecom Regulatory Authority of India (TRAI) is claiming a world first in using blockchain on a large scale in the telecoms sector. The

application is set out in a draft regulation that aims to curb the problem of unsolicited communications, or spam, which TRAI first started to tackle in 2010 with a “do not disturb” registry, which has a lot of subscribers – TRAI says 230 million are registered. But the problem was not contained because “unscrupulous elements” started obtaining customers’ consent, often surreptitiously, or resorted to the use of unregistered telemarketers that call or message from a 10-digit number. Recently, the incidence of fraud calls has also been on the rise. The new regulations require that consent be explicitly recorded by a third party and be activated only after subscriber confirmation. Furthermore, the subscriber is given the option to revoke his or her consent, if it’s abused or is no longer relevant.

Blockchain is the key to making it work, says TRAI, as it has proven useful where the objective is to cryptographically secure information and make it available only on a need to know basis. “Yet none may deny their actions or tamper with records, once recorded on the distributed ledger, which uniformly enforces compliance.”

However, a software engineer has taken issue with the use of blockchain for this application, saying it hasn’t been tested at scale anywhere in the world, and that a private and permissioned blockchain network is not secure. Shirsendu “Troy” Karmakar challenges several assumptions in TRAI’s proposal in an article that can be read at bit.ly/2Qnwcws.

Meanwhile UK regulator, Ofcom, is inviting organisations to trial the porting and management of millions of telephone numbers using blockchain and ledger technology. Ofcom says about 1 billion landline telephone numbers are available in the UK, either already in use or reserved for allocation, and are issued in blocks to telecoms operators, which manage the numbers and movement (porting) of them into and out of their control. Existing systems used for this process will need to change as networks move to an all-IP (internet protocol) infrastructure and moving to blockchain has the potential to improve customer experience when moving a number between providers, lower regulatory and business costs, and provide more effective management of nuisance calls and fraud.

2.3 Integrating Iot With Block Chain in Telecom Operations:

The Internet of Things (IoT) is a rapid growing industry doomed to transform homes, cities, farms and more efficient. As per Gartner, by 2020,

there will be more than 20 billion connected things through out there globe, covering a market that will be worth north of \$3 trillion. But the turbulent growth of IoT will introduce several challenges, including analyse, connecting, securing, and advising so many devices. It will be very challenging for the present architecture underlying the Internet and online services to guide vast IoT environs of the future.

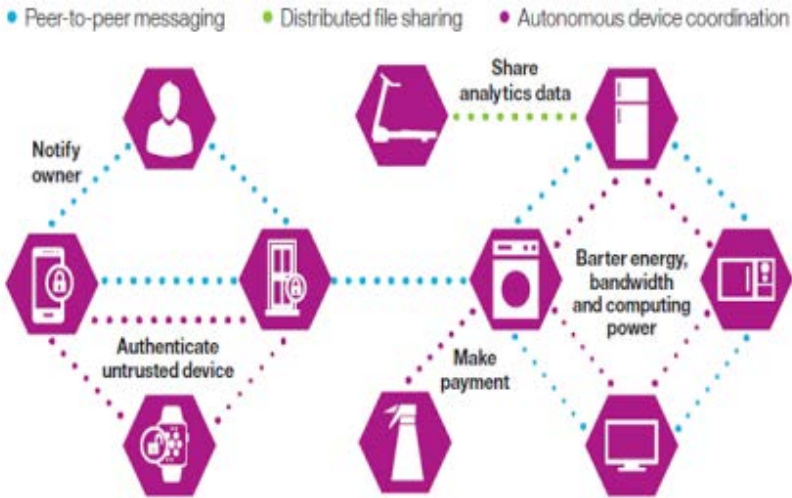
The band model has worked fully in the past decades, it will become suspect when the number of network nodes grows into the millions which result in achieving billions of transactions, because it will experimental increase computational requirements and also by delay the costs. With help of Blockchain technology will be able to create secure mesh networks, where IoT devices will interconnect in a reliable way while avoiding threats such as device spoofing and impersonation. Implementation of theIoT function solutions without a centralized control, this approach must be support three fundamental functions.

- Peer-to-peer messaging
- Distributed file sharing
- Autonomous device coordination

Several companies are already embedded blockchain to use to power IoT networks. One example is Filament, a start-up that provides IoT hardware and software for industrial applications such as agriculture, manufacturing, and oil and gas industries. Device badge and interchange is secured by a bitcoin blockchain that clutch the unique identity of each compete node in the network. There are several clear benefits to the idea of building smart contract machines which able to communicate and operate via blockchain.

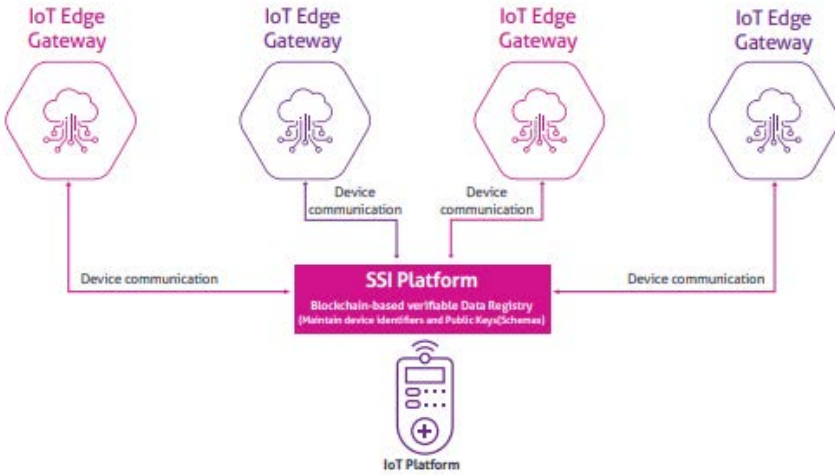
Firstly, there is the issue of overlook. With data transactions business taking place between different networks held and oversee by multiple organizations, a permanent, abiding record means care can be tracked as data, or physical goods, pass between points in the supply chain. Blockchain records are by their very nature clear – activity can be tracked and analysed by anyone authorized to connect to the network.If existing things goes wrong, degradation occur, data leaks where it shouldn't, then

the blockchain record makes it easier to analyse the weak link and, hopefully, take corrective action.



Secondly, the use of encryption and storage means that data can be trusted by all parties involved in the supply chain. Machines will record, securely, details of transactions that take place between themselves, with no human inattention. Without the protected keys giving write-access to the blockchain, no human will be able to override the record with incorrect data. Thirdly, the —smart contract facilities provided by some blockchain networks, such as Ethereum, allow the formulation of agreements which will be executed when surroundings are met.

This is likely to be extremely useful when it comes to, for example, authentication one system to make a payment, when conditions intimate that delivery of a service has been administer. Fourthly, blockchain endeavour the possible of greatly improving the overall security of the IoT environment. Much of the data generated by IoT is highly exclusive – for example, smart devices. Allowing access to data from IoT accessory to be handled through blockchains would mean an increased layer of security that any destructive actor would have to bypass – one that would be protected by some of the most booming encryption standards available.



The confluence of accounting and blockchain could create a fully new accounting system in which each and every transaction executed is publicly available and verified. Henceforth, blockchain could be used to prevent and detect obtained transactions. Because blockchain keeps the record of a forte transfer, any type of unauthorized can be detected by blockchain. To conflict financial reporting fraud, such as overemphasis of revenues by means of channel round-tripping, the transactional data in blockchain could provide valid evidence showing any potential asymmetry involving revenue recollection. In addition, the continuity, reserved, and immutable of a blockchain ledger could prevent management from creating false transactions or backdating options. The liquidity of blockchain will make it easy for juristic accountants to access and examine the material transactions. Henceforth, the risk of receiving checks without sufficient funds could be avoided.

Therefore, blockchains not only boost the chance of determining fraud, but also pressure management to reduce and control. Sharp contracts encoded with accounting and business rules could also provide effective controls of business processes in order to prevent fraud. Smart contracts can be implanted with approach access control criteria that allow only authenticated users to create transactions. A well-made blockchain should have an accurate and dynamically controlled system to designate the roles of linking to the blockchain, initiating transactions, and creating benefits.

In addition, the applicable criteria could be encoded in smart contracts to ensure all conditions have been met before recognizing revenue. Moreover, smart contracts could add reason into accounting processes by combining big data and predictive analytics.

Integrating with big data, smart contracts could layer on top of the predictive transformation to achieve an energetic risk-aware measurement of companies' performance. Woefully, not every fraud scheme can be automatically prevented by blockchain. For example, dishonestly schemes are hard to detect in both traditional accounting and blockchain accounting systems. Roaming which own subscriber of one network 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 that is VPMN, Visited Public Mobile Network.

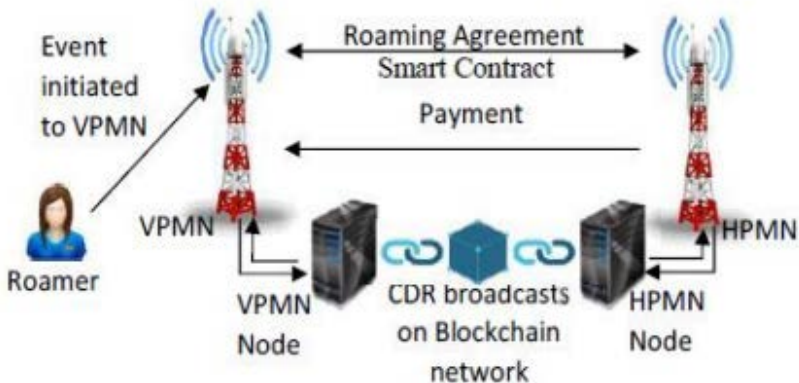
Telecom operators suffer a fraud loss due to ever increasing number of International Revenue Share Fraud (IRSF) cases. When a request for call to process is initiated by a roamer, VPMN drive a query about the roaming related information of that roamer to the Home Location Register (HLR) of HPMN through signalling link. VPMN response to this signal by sending the Call Detail Record (CDR) to their billing system and to HPMN so that they settle the account with VPMN as per the cost. Often Telco's outsource the transmission of CDR files and its conversion into billing traffic according to subscriber's subscription to the third party, called Data Clearing House (DCH). When HPMN unable to charge to the subscriber who is on roaming, to use the resources of VPMN, but still liable to pay to VPMN.

Longer detection time: The time required between the penetration of the fraud, detection and measures to combat it are deployed is determined by the time involved in sending the CDR information from the VPMN to the HPMN, and the time employed to investigate the potential existence of a fraud attack. Because of this HPMN longer time to notice frauds because it has appear outside of its network, in the network of VPMN and there have been delays in the information exchange between VPMN and HPMN.

Longer response time: After detection of the fraud, in such case HPMN doesn't have control on VPMN network. So, it takes longer time to respond.

Technical difficulties: When unauthorised 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 range in the networks of HPMNs and VPMNs, there are more technical difficulties for prevention, detection, and automatic response systems to initiate actions against fraud.

Implementation of a legal blockchain could replace the traditional ways of sending CDR. All the CSPs, which have undergone roaming.



Agreement, can broadcast CDRs on permissioned Blockchain network. Addition to this an IoT device in the network will connect to the HPMN and VPMN. Which keep track of location, HSS, and subscription plan. That IoT device will keep an update of a subscriber's activity. When subscriber creates a call process. VPMN will get every data directly from that IoT device or server and the process time will get reduced. Reduced in signalling time will lead to serving more people.

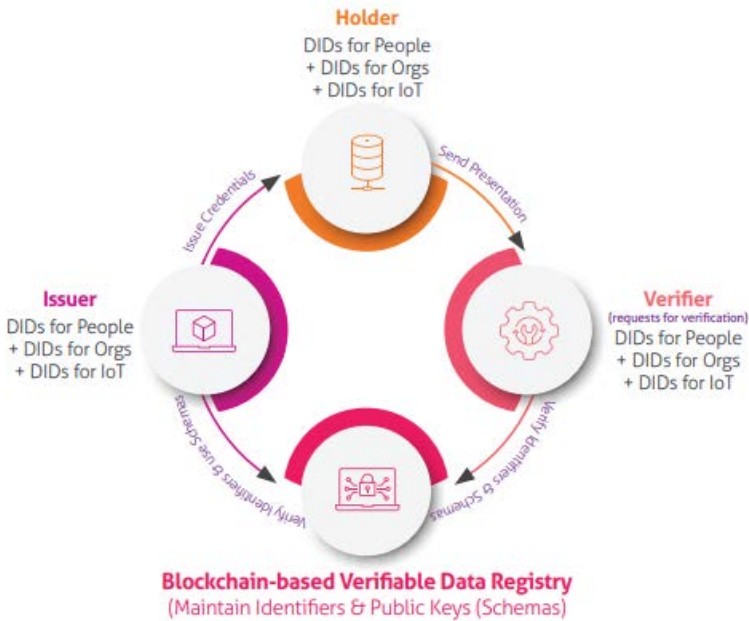
Permissioned nature of blockchain will allow only authorized access to the network, so there will be no chance of data leakage. A Hyper ledger blockchain could be used to restrict the transfer of unwanted blocks of the blockchain to designated nodes of VPMN and HPMN act as miners to

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 this whole process 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. This helps to achieve certified and smooth settlement transition between HPMN and VPMN, without occurring any fraud. Even, in this scenario, since CDRs being transferred through blockchain network via broadcasting, so it makes the role of DCH irrelevant. It helps telecom operator to save even more costly as this process does not require a third vendor.

India seeing the ascent of brilliant growth in IoT by keen innovations. What's more, telecom operator are giving an IoT based solutions for their customer. It is anticipated that by 2020 there will be 200 billion associated gadgets, which could come about into expanded likelihood of gadgets and presenting more surface to digital assaults. An IoT biological community is a joining of numerous interconnected gadgets associated with a brought together centralise hub, which thusly is associated with the IoT platform. IoT platform devours the information produced by these brilliant gadgets to understand this information.

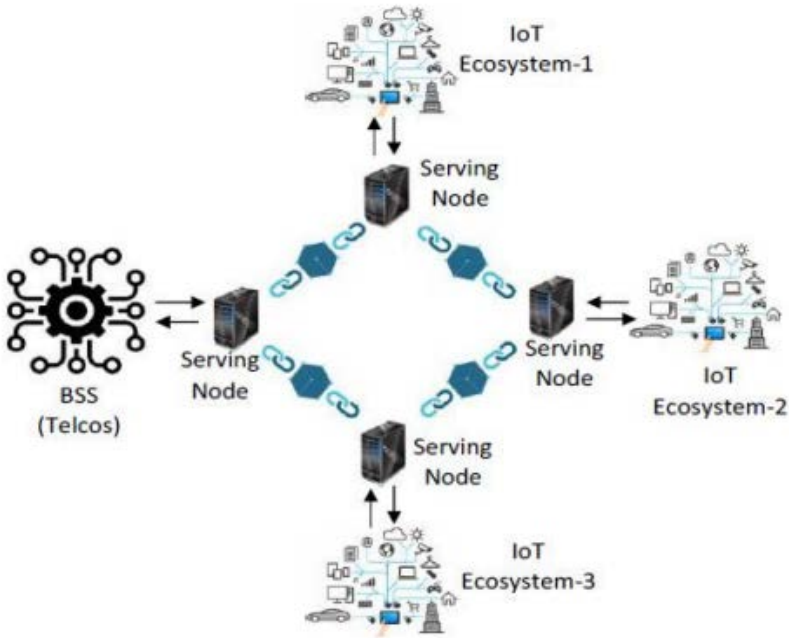
To build up this system of internet is required, which is taken into account by Telco's. IoT ecosystem is highly centralized and completely relies on the internet for any sort of communication amongst connected devices which makes it vulnerable to the high level of risk if security is not prioritized. An ecosystem for IoT needs a heavy of processing, power and storage space to authenticate and identify all the connected devices through a centralized server, so can only support small-scale network. Normally problems arise like Packet loss, Irrespective of the distance between two devices, all the communication, and transfer of information has been executed through the internet, results in packet loss and makes eco-system expensive. Packet loss is often correlated to the QoS of the ISP.



The loss in packets is equal to lose in revenue for the service providers. Cloud servers are used in current IoT ecosystem which makes network highly vulnerable to a failure at this point can disturb the entire network. The causes could range from power outages to database errors to faulty software updates to overloaded servers. Cloud services are provided by multiple manufacturers and since there is no any single platform to connect all the devices interoperability and compatibility issues arise. This is very dangerous because of increase in dependency of IoT in some sensitive sectors like health care.

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. It is necessary to secure IoT devices emerged increasingly after a massive cyberattack on the internet which exploited several connected devices to do their masters. The secure and stable-proof nature of crypto currency blockchain can be Utilized by the consortium to ensure the Security of the inter-connection between various IoT devices. A blockchain technology industry has the possible to move forward in determine the scope and operations of a smart contracts protocol layer

across several major blockchain systems/ecosystems. Through this system, the limit to interoperability and security within IoT can addition the existing IoT platforms with a blockchain back-end to add value to IoT, supply chain, and trade finance.





Basically, the concept behind using blockchain to avoid fraud, increase network transparency and allow many parties to perform confirmation in order to secure the validity and skill of transactions. In the current situation, people are not using this technology potentially. The whole courage of dissolution of management and care is nullified. Alternatively, a blockchain should be expand among different, relatively absolute parties such as suppliers, clients, and banks. These parties could become autonomous verifiers charged with strike criminal transactions, especially those transactions involving outside parties. These pieces of information make up a network of —sourced-evidencell that can be used to confirm the validity of activity booked on blockchain systems.

There are plenty of benefits adopting a blockchain in the core and auxiliary operations of a Communications Service Provider, as mentioned above. CSPs should consider the long term view of blockchain and their potential

to add value to the enterprise in both their current and new business models. Adoption of the blockchain is not easy there are some challenges, as with any new technology that holds the promise of significant disruption. Anyhow, CSPs would do well to work combine together to facilitate the full realization of the benefits, just as many of the global financial institutions are currently adopting the solution.

Key challenges with IoT implementation and its recommended solutions

Problem 	Solution 
Secure federated devices	Use encryption and decryption process
Authorize and authenticate devices	Use security for high assurance
Security glitches	Enable patches managed by updates
Establish secure communication	Use TLS or DTLS communication
Data privacy and integrity risk	Use fingerprinting or encryption-based data
Secure web, mobile, and cloud applications	Use proper hub architecture
Ensuring high availability	Ensure un-interrupted data access for authorized users
Predict vulnerabilities and incidents	Detect, measure, manage and predict

Working independently will limit the potential of blockchain, as disintermediation, robustness, and the need for trust at the intersection of many stakeholders drives real value. Organizations such as the GSMA, which represents the interests of many mobile CSPs globally, could equally take a more active role in exploring and promoting blockchain use cases in the industry. Various companies such as Orange and Verizon, amongst others, have already invested in start-ups in the blockchain area to explore the synergies and potential use cases. Many more players are researching potential use cases in-house. It is time for everyone to agree on a unified approach to enable the meaningful realization of benefits.

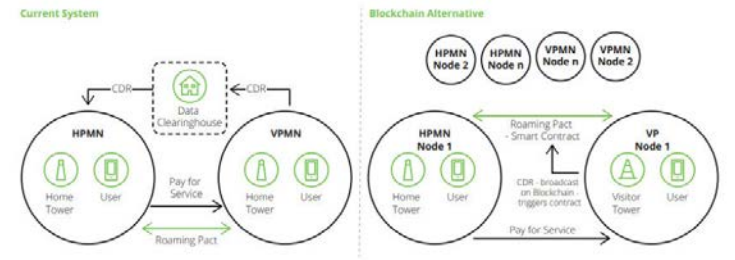
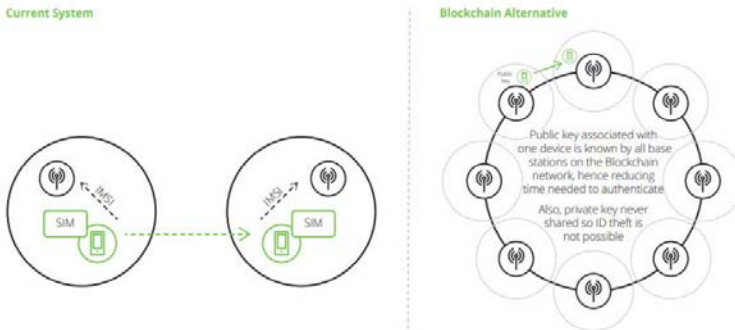


Fig. 2. Roaming Fraud prevention illustrative presented



Smart contracts, which are one of the key features of blockchain technology, are used to automatically implement rules and agreements between access points and to ensure the availability of real-time network resources. Networking and real-time networking rules are the current issues that need to be addressed before mass adoption of 5th generation networks. The blockchain platform allows new generation of access and management technology for network selection. It supports the activation of 5G network potential and provides a common platform with seamless connectivity. 3GPP and non-3GPP can be implemented using block

blocking, and operators can connect to devices on multiple local hotspots and Wi-Fi based on permission.

With the search for improvements in the telecommunication network and the deployment of the 5G network, the connectivity network is expected to grow with the highest CAGR. Applications for IoT devices include a smart city, intelligent home, connected car, connected cars, smart farming, smart entertainment and much more. There is no doubt that this list will grow further in the near future. Frost and Sullivan predict that by 2020 the market for smart cities will reach \$ 1 trillion. It is estimated that there will be 200 billion connected devices by 2020, which may increase the likelihood of devices being vulnerable to attacks. Separate hardware challenges (such as longevity), the core elements in the development of IoT devices are Connectivity, Privacy, Compatibility, and Security.

Benefits	Challenges
A blockchain's 'enabled' trust improves co-ordination between various partners, due to a shared view of transactions and liabilities. This in turn permits the elimination of third parties, resulting in cost savings.	Since a blockchain retains all historical data, the size of an established blockchain at each node might become unsustainable. Instead, a mechanism to archive historical data needs to be looked at. Several alternatives are currently being explored in this regard by various players in the blockchain ecosystem.
Facilitates a single view of data instead of the need for consolidation across various disparate systems. Also allows for reliable audit trails due to the history of all transactions being available in the ledger	Conforming to existing data standards in terms of both structure and transport for sharing of information could prove to be an initial hurdle.
Implementation of smart contracts in roaming and other cases allows for near-instantaneous charging, thus leading to improved revenue assurance and fraud reduction.	Clear regulatory frameworks need to be defined for the implementation of agreements as digital, smart contracts
Potential to facilitate new business models for revenue generation for Communication Service Provider who are looking for new avenues to increase both top and bottom lines.	
A blockchain can act as the ledger that enables, for example, an M2M economy to prosper based on the common platform available, in which M2M transactions can be recorded. It can thus act as the enabler for an IoT ecosystem	

The current ecosystem for IoT is highly centralized and completely relies on the internet for any sort of communication amongst connected devices which makes it highly vulnerable if security is not prioritized. Traditional systems are subject to several points of failure such as Packet loss, Cloud services Interoperability issues, Single point of failure.... etc. 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 captured into a real-time monitoring system for IoT systems. With the implementation of blockchain technology in IoT ecosystem, the Centralized model can be replaced by Distributed Digital Ledger (DDL) for all the transactions, makes extremely secure peer-to-peer self-managed network which overcomes some of the IOT challenges.

The presented use cases for blockchain technology implementations are just a small but valuable part of the variety of possibilities which blockchain provides to telecom industry. The adoption of blockchain technologies in telecom industry could have potentially benefits in three areas: Efficiency improvements; cost reduction; and fraud mitigation. Efficiency improvements streamline multiparty transactions by automatizing and expediting the process while guaranteeing the accuracy of the settlements between parties (thus avoiding duplication of verification processes). The benefits can materialize in different forms depending on the type of industry and the type of interactions/transactions required.

For industries with regular and low value interactions with their customer base, such as telecom, blockchain can verify and automate transactions, with increased transparency for the end customer. The higher the number of low value transactions, the greater the potential of blockchain. The higher the number of players, the higher the number of cross-transactions, hence whenever multiple parties are involved, blockchain plays at its best.

The Cost reduction potential is linked to the capability to eliminate intermediaries and reduce labour intensive processes through automatization. This is higher in industries with complex and labour intensive internal processes, like banking. Middle men can be eliminated as verification of transactions is automated and guaranteed through blockchain. This applies to telecom international roaming transactions and resulting international voice settlement where blockchain can replace the expensive mediation of clearing houses.

Fraud mitigation is mostly associated to high delinquency ratio such as identity theft and similar fraud. The food industry can greatly benefit from blockchain by enabling trusted tracking of food lifecycle to ensure the integrity of the cold chain in transportation, helping reduce the high

volume of fraud related to the sale of expired, contaminated or counterfeit food. Blockchain-addressable security related concerns are also related to long verification processes, as the longer the time, the more exposed the process is. International money transfers between banks is an area facing this problem and so too is roaming settlement between telecom players, which currently lose more than \$38 billion annually in fraud costs, according to Deloitte.



Blockchain is currently leading the way in telecom innovation and is changing the economic social landscape of digital communications worldwide. It accommodates telcos biggest need to make their service offerings elastic according to market changing demands. Blockchain technology can resolve the telcos high pressure to cut down the cost, to enable new revenues streams, service efficiencies, and also keep a check on fraudulent practices while allowing a superior customer experience. It eliminates the traditional complex and long chain of inter-related operations that work jointly to deliver services to customers. Being a decentralized technology, blockchain completely eliminates the role of expensive infrastructure as well as the need for central authorities or intermediaries. It increases the speed and efficiency of the digital exchange of data between people, departments and provides quicker, efficient and seamless transmission of information.

Blockchain looks instrumental in enabling interoperability between internal as well as external systems for telecom companies. This can bring down infrastructure as well as compliance. Blockchain has the potential to disrupt business models by increasing transparency and effectiveness in the telecom network and its processing. Blockchain decentralized ledger documents fully each transaction that occurs across a distributed or peer-to-peer network, either public, private or hybrid. In addition, blockchain (recognized as a trusted technology) plays an important role in many areas that conventional systems are technically limited to resolve, such as Service convergence, Real-time transactions, Industry integration, Usage of 5G capabilities, Internet of Things (IoT), Augmented Reality (AR), Virtual Reality (VR), Machine-to-Machine (M2M), Issues related to overabundance of contents, Data traffic explosion, Mobility, Security and many more... where devices connected to the internet automatically orchestrate their interactions The usage of blockchain based-applications by the telecommunications industry is gaining momentum and eventually will become the norm. The clock is ticking.



CHAPTER - 3

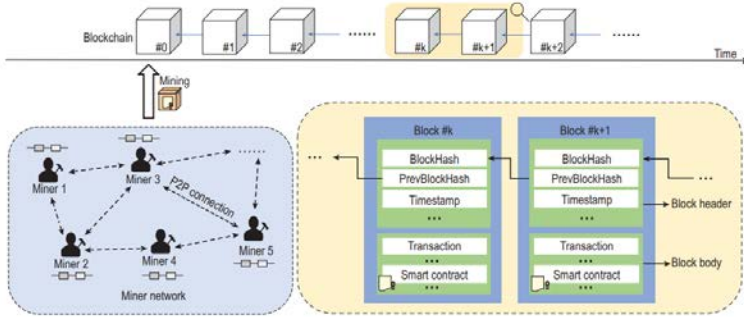
Blockchain In Wireless Telecom Communications

With the deployment of fifth-generation (5G) wireless networks worldwide, research on sixth-generation (6G) wireless communications has commenced. It is expected that 6G networks can accommodate numerous heterogeneous devices and infrastructures with enhanced efficiency and security over diverse, e.g. spectrum, computing and storage, resources. However, this goal is impeded by a number of trust-related issues that are often neglected in network designs.

Blockchain, as an innovative and revolutionary technology that has arisen in the recent decade, provides a promising solution. Building on its nature of decentralization, transparency, anonymity, immutability, traceability and resiliency, blockchain can establish cooperative trust among separate network entities and facilitate, e.g. efficient resource sharing, trusted data interaction, secure access control, privacy protection, and tracing, certification and supervision functionalities for wireless networks, thus presenting a new paradigm towards 6G. This Chapter is dedicated to blockchain-enabled wireless communication technologies.

We first provide a brief introduction to the fundamentals of blockchain, and then we conduct a comprehensive investigation of the most recent efforts in incorporating blockchain into wireless communications from several aspects. Importantly, we further propose a unified framework of the blockchain radio access network (B-RAN) as a trustworthy and secure paradigm for 6G networking by utilizing blockchain technologies with enhanced efficiency and security. The critical elements of B-RAN, such as consensus mechanisms, smart contract, trustworthy access, mathematical modeling, cross-network sharing, data tracking and auditing

and intelligent networking, are elaborated. We also provide the prototype design of B-RAN along with the latest experimental results.



After summarizing and evaluating the merits and demerits of existing works, we present a unified framework of B-RAN as a trustworthy and secure paradigm for 6G networking by utilizing blockchain technologies. By establishing cooperative trust via blockchain among separated resource hosts as well as heterogeneous network entities, B-RAN facilitates cross-network resource integration and sharing and promises enhanced wireless accessing, roaming, sharing and security across networks or subnetworks. Acting as an open unified framework, B-RAN supports a plethora of services and applications beyond radio access and data transmissions, such as IoT, mobile edge computing (MEC), distributed learning, vehicle networking and energy trading.

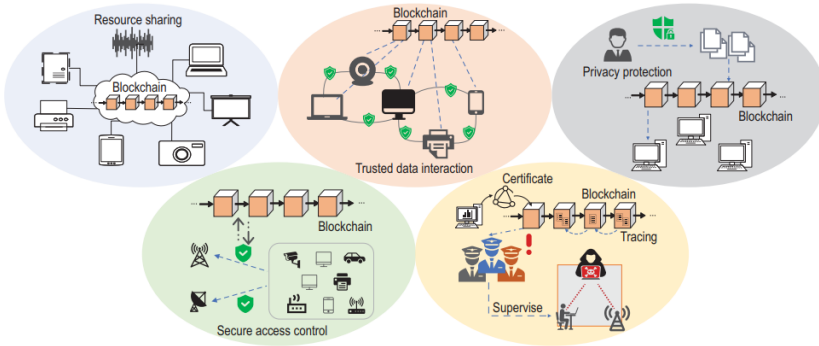
The underlying blockchain can establish a multifold trust relationship for B-RAN among multilateral groups with any trusted party. In this way, B-RAN pools and shares varied network resources across subnetworks to form a multisided platform (MSP) that leverages the power of positive network effects. In this work, we present B-RAN in a full picture and investigate the application prospects of B-RAN in future 6G networks. We elaborate on the critical elements of B-RAN, including consensus mechanisms, smart contract, trustworthy access, mathematical modeling, cross-network sharing, data tracking and auditing, and intelligent networking.

Blockchain is expected to be the next game changer in the wireless communication area by not only industry but also academia. The number of research works related to blockchain in several academic databases has

continued to grow in the recent decade. Among them, there are a few pioneering works that attempt to incorporate blockchain into wireless networks. An extensive discussion on the opportunities brought by blockchain to empower 5G systems and services was presented. provided a survey of blockchain technology applied to smart cities supported by information and communication technology. A new concept of the blockchain radio access network (B-RAN) was proposed for future wireless communications and potential functionalities of blockchain applied in resource management and network access were investigated.

Reviewed some efforts on integrating blockchain and machine learning for communications and networking systems and discussed some significant challenges of such integration, envisioned the potentials of blockchain for resource sharing in 6G and presented some cases in different application scenarios. So far, most existing research works focus on applying blockchain to one or several specific communication scenarios, for instance spectrum sharing, but there lacks a panorama of comprehensive and deep emergence of blockchain technologies and wireless networks. Meanwhile, critical issues of blockchain, such as security, latency, throughput, scalability, cost and power consumption, have to be investigated for the adaptability and applicability of blockchain in 5G and future 6G wireless networks.

This Chapter present a comprehensive investigation of the most recent advances and challenges in incorporating blockchain into wireless communications, and more importantly establish a unified framework of the blockchain radio access network for upcoming 6G networks as a novel paradigm shift. We first provide a brief introduction to the fundamentals of blockchain, including its concept and architecture, mining and consensus protocols, smart contracts and possible security risks. Then, we provide a comprehensive survey of state-of-the-art works on integrating blockchain into wireless networks from several aspects, including resource sharing, data interaction, access control, privacy protection, tracing, certification and supervision, and highlight the motivations of such integrations and the significant benefits from blockchain.



Low-cost alternative consensus protocols, such as PoS, are even more vulnerable. If something is at stake, it is at risk of being lost, whereas if nothing is at stake, the adversary has nothing to lose and attempts to launch nothing-at-stake attacks and work on multiple branches simultaneously. That is how a nothing-at-stake attack arises, recognized this issue and proposed an algorithm, namely Slasher, to prevent this attack by requiring validators to provide a deposit that will be locked for a period. A similar case occurs in the coin-age accumulation PoS, in which an attacker can accumulate coin age by hoarding his coins to increase his influence in the blockchain. Author suggested introducing a cap on the coin age to resist this attack.

Traditional cyber-attacks, such as the distributed denial of service (DDoS) attack, replay attack, man in-the-middle attack, Sybil attack and eclipse attack, still exist in blockchain. The DDoS attack occurs when multiple blockchain nodes are flooded with invalid requests and their normal operations may be abruptly interrupted. The replay attack is to intercept the data packets of communicating parties and relay them to their destinations without modification, while in man-in-the-middle attacks, attackers can intercept those data packages and inject new contents. Author presented an example of applying the man-in-the-middle attack to raise double spending in a private Ethereum blockchain. Besides, a malicious entity could create many fake identities to launch a Sybil attack, where a plural of faulty information is injected into the network. Unlike Sybil attacks aiming at the entire blockchain network, the eclipse attack only cheats on one network target and forges a false view of blockchains.

3.1 Resource Sharing In Blockchain For Wireless Telecom:

The explosive growth of various mobile services demands a large quantity of network resources, e.g. spectra and infrastructures, which are generally limited and have to be shared for better utilization and efficiency. In practice, however, resource sharing is often deterred by the separation between resource hosts, who may lack incentive or have cost and security concerns, making coordination and cooperation between network entities infeasible. On the other hand, with the new functionalities of cloud processing, MEC, software-defined networking (SDN) and network functions virtualization (NFV) in 5G systems, there are increasing types and quantities of network resources, e.g. computing and storage resources as well as network slices, which make resource management and sharing quite challenging. Blockchain and its inherent characteristics can effectively promote collaboration and alleviate the trust and security concerns among separated network entities, thus leading to more efficient resource sharing.

There has been intensive research around applying blockchain to spectrum sharing. Author explored how to implement spectrum management in combination with blockchain and discussed the pros and cons of different spectrum sharing mechanisms. Author proposed a spectrum sharing system between operators based on consortium blockchain to provide reliable privacy and security guarantees. In Ref, a blockchain verification protocol was proposed to enable and secure spectrum sharing in moving cognitive radio networks without constant spectrum sensing. Author proposed a blockchain-empowered spectrum sharing framework that can effectively motivate primary users to share their under-utilized spectrum and realize efficient spectrum allocation with low complexity. Moreover, Author used blockchain to construct an unlicensed spectrum management framework for semi-distributed wireless networks and solved the spectrum contention. Author introduced an intelligent network architecture to deal with the unlicensed spectrum sharing between operators and users via smart contracts. In addition, a new blockchain structure with corresponding consensus algorithms was introduced in Ref to autonomously manage unlicensed spectrum and decrease the CapEx and OpEx of network deployment.

The wide use of cloud processing and MEC makes computing and storage capacities valuable network resources, which can be efficiently managed by blockchain. Author proposed a blockchain-based computation offloading framework that enhances the collaboration among entities in sharing computing resources. Author proposed a blockchain-based MEC architecture and used a three-stage Stackelberg game to model service bidding, negotiation and transactions among different entities. In Ref, two double auction mechanisms were utilized to encourage blockchain entities to share their computing power. Furthermore, Author introduced a consortium blockchain for resource transactions in vehicular edge computing and to defend against malicious behaviors. Author utilized blockchain to construct an attribute-based encryption scheme for secure storage and sharing of medical records. In Ref, a blockchain-based arbitrable remote data auditing scheme was proposed to provide reliable network storage services.

Blockchain presents a secure and efficient way to manage heterogeneous devices and infrastructures in 5G and IoT networks. Author explored blockchain to fulfill sovereign, autonomous and trusted infrastructure sharing in 5G small cell networks. Author considered using blockchain as a secure, distributed cyber infrastructure for the future grid and proposed a prototype to optimize energy infrastructure allocation and improve energy efficiency. Author proposed a method to use blockchain to control and configure IoT devices, and attempted the identity management for interconnected devices. Author presented several blockchain-based solutions to mitigate the issues associated with the management of numerous constrained devices. In Ref, a private-blockchain-based architecture for the management and monitoring of IoT devices was introduced. Author constructed a blockchain-based IoT architecture to organize and share IoT data and devices.

Enabled by SDN and NFV in 5G systems, network slicing, as logical assembling of diverse physical network resources, has an inherent sharing property. Author presented the concept of the blockchain network slice broker to promote slice leasing, and later in Ref, the feasibility of blockchain network slice brokering was analyzed in an industrial automation scenario. Author proposed a novel network slicing brokering solution named NSB chain, which enables infrastructure providers to

allocate network resources to the intermediate brokers through smart contracts. Similarly, Author designed a signaling-based distributed on-demand framework called distributed blockchain-enabled network slicing that promotes dynamic resource leasing between different service providers to support high-performance end-to-end services.

3.2 Trusted Data Integration In Blockchain For Wireless Telecom

With the upsurge of diverse wireless traffic and connection density, data from varied sources need to interact and collaborate to provide services together . However, the lack of trusted relationships among data holders participating in the mobile network makes it difficult to secure data interaction processes and verify data authenticity an reliability . Recently, researchers have been using blockchain to establish mutual trust between diverse devices and create a trusted channel for secure data interactions. The efforts of using blockchain to support trusted data interactions in wireless networks have mainly been in two directions: to ensure the credibility of each network identity and to improve the authenticity of the transmitted data.

To ascertain identity credibility, each entity can obtain its credibility value before entering the network by letting blockchain participants analyze a number of indicators (e.g. its historical behaviors), and then the permissions will be granted based on the evaluated value to the entity. In the trust management mechanism in Ref, only the nodes with a specific trust degree can interact with other nodes, while malicious nodes will be detected and expelled. Author designed a consensus mechanism for blockchain-based V2X networks, in which the validation of data interaction is conducted based on vehicles' credit degrees. In addition, by combining distributed identities with the underlying layer of blockchain, Author managed to enhance personal privacy and control of digital identities. Moreover, Author proposed a trustless system model for intelligent vehicles using blockchain and a certificate authority in vehicular ad-hoc networks.

Group intelligence perception and consensus mechanisms could be utilized together to ensure the accuracy and authenticity of the data. Author took advantage of the mutual authentication protocol and user-defined

sensitive data encryption in a blockchain-based trusted data management scheme in edge computing. Author proposed a decentralized trust management system for vehicular networks based on blockchain by using a Bayesian inference model to evaluate the credibility of traffic messages. Also, Author proposed a proof-of event consensus concept for vehicular networks that uses passing vehicles to verify the authenticity of traffic data collected by roadside units.

3.3 Secure Access Control In Blockchain For Wireless Telecom

The continuous densification of wireless networks and increasing heterogeneity of massive devices bring many security risks to access control in mobile communication systems. Specifically, there are mainly three categories of security risk: device security risk caused by malicious device intrusion, system security risk due to the single point of failure and data security risk resulting from data leakage.

Built on its inherent nature, such as tamper resistance, decentralization and fine-grained auditability, blockchain presents a promising remedy to address these security risks in wireless networks. Device access control Given the massive number of various devices in the mobile communication network, there are inevitably malicious devices attempting to compromise the security of the system. Several works have considered using blockchain to prevent malicious device intrusion. Author adopted a customized smart contract to defend against DDoS attacks and rogue device attacks. Author designed an access control architecture called Control Chain, which provides a secure way to create relationships for network entities and assign them attributes. Moreover, Author proposed an access control framework containing three smart contracts to safely add, update and delete network entity identities.

In addition to malicious device intrusion, the traditional access control mechanisms also face the risk of single points of failure due to the fact that they are based on centralized entities. The characteristics of decentralization and joint maintenance in blockchain can readily prevent the single point of failure. Some researchers have tried to integrate blockchain with access control mechanisms to solve this concern. Author proposed an attribute-based access control scheme for IoT, which utilizes blockchain to record the distribution of attributes to avoid single points of

failure and data tampering. Moreover, Author devised an identity-based robust capability token management strategy, which employs smart contracts to register, disseminate and revoke access authorization.

Nowadays, users have significant concerns around data security, whereas in traditional centralized access control mechanisms data security remains at a low level, as centralized entities may manipulate and leak user data as they wish. Some studies have introduced blockchain technology in access control to solve data security issues . Author realized the security and anonymity of IoT data by deploying fair access in UTXOs to implement blockchain-based access control. Moreover, Author suggested an access control scheme called Cap Chain, which employs the anonymity of the blockchain to hide key information for data sharing and delegation to ensure data security. Also, Author designed a novel blockchain enabled gateway, which acts as an intermediary between users and IoT devices, thereby enhancing data security in IoT access control.

3.4 Privacy Protection In Blockchain For Wireless Telecom

When different entities communicate with each other through wireless links, the openness of wireless transmission and mobility of wireless devices may bring many privacy issues. For example, malicious entities may intercept, relay or even tamper with the transmitted messages, which usually contain private entity identities or confidential data. Therefore, privacy protection in mobile communication networks has received increasing attention. With imbedded asymmetric encryption, blockchain is expected to provide both the privacy protection of entity identities and the privacy protection of confidential data.

The pseudonym mechanism is often employed in blockchain to protect identity privacy by concealing the user's identity in communication systems. In Ref, attempts were made to use blockchain to protect privacy, where each node uses a unique public key that can be retrieved from the blockchain to communicate with other nodes. Also, Author utilized pseudonyms in a private blockchain to hide users' identity, where each user may create multiple pseudonyms with data related to these pseudonyms. Similarly, Author designed dynamic key management in a vehicular communication system where users must periodically change their pseudonym set, as well as all the cryptographic materials related to

this pseudonym by contacting the blockchain miners. In Ref, all the activities of certificate authority are recorded in the blockchain transparently without revealing sensitive identity information of vehicles, so that public keys can be used as authenticated pseudonyms for communications. Moreover, Author applied permissioned blockchain into smart grid networks and used a group signature technique to secure identity privacy.

Apart from identity privacy, some researches focus on the privacy protection of confidential data of users in wireless networks. The asymmetric encryption methods were used to encrypt user data recorded as blockchain transactions to provide privacy protection for data confidentiality. In another example, permissioned blockchain is used to retrieve the related data and manage the accessibility of data, while raw data is stored locally by each data provider in industrial IoT. Author proposed a scheme in which the mining node is chosen according to the average consumption data and individual private data will not be disclosed for power grid communications. Different from the aforementioned mechanisms, Author presented a blockchain-enabled IoT gateway to enhance privacy and security, by which users can manage their privacy preferences and determine whether personal data can be forwarded to an IoT device.

3.4 Tracing,Certification,Supervision In Blockchain For Wireless Telecom

Blockchain is able to provide a full range of credible records and security guarantees for tracking network entities via the mandatory operations in consensus mechanisms and smart contracts, which ensure the integrity and security of the data and transactions in blockchain. In Refs, blockchain was proposed to enhance the traceability of IoT devices. Author devised an asset tracing method in which a mixed blockchain structure is adopted. Author designed a new token to enhance the traceability of blockchain data. Author used smart contracts to track and manage industrial transactions in manufacturing. Author proposed an identity authentication scheme based on blockchain secret sharing and dynamic proxy and used it to track the collaborative authentication process.

By adopting blockchain, mobile service providers (SPs) are able to preserve and certificate devices and data transparently and reliably. Author introduced a blockchain-based certification service that uses smart contracts to seal biomedical database queries and results. Author built a public key infrastructure (PKI) certificate system based on a permissioned blockchain and solved mutual trust problems in multi certificate-authority (multiCA) applications. Moreover, in Refs, blockchain was proposed to reinforce the security of device certificates in PKI systems. Author proposed a digital certificate system based on blockchain, implementing anti-counterfeiting and verifiable digital certificates. Author designed a blockchain-driven certification system to achieve efficient and secure certificate queries and validations.

Blockchain naturally caters to the requirements of information supervision. It was born with the capabilities of securing regulatory data and improving the efficiency of supervision and administration. Author proposed a blockchain supervision model for e-government based on a threshold ring signature algorithm. Author proposed a vaccine production supervision mechanism based on a two-layer blockchain. Moreover, Author used blockchain to create an edge computing infrastructure for workflow supervision in government bidding and significantly secured government plans and policies. Author designed a blockchain-based autonomous transaction settlement system for IoT e-commerce, which allows all network participants to jointly supervise the settlement process.



CHAPTER - 4

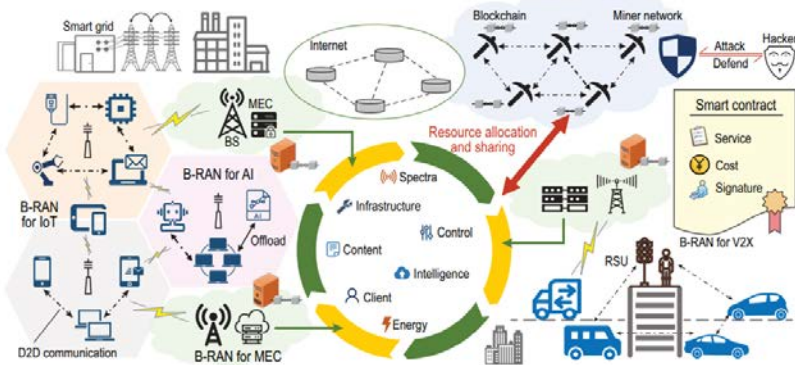
Wireless 6G in Blockchain Technology

In this section, we propose B-RAN as a unified framework of blockchain-enabled wireless communications for 6G networking. Upon the depiction of the B-RAN paradigm for 6G, we provide an indepth discussion on the critical elements of B-RAN, including consensus mechanisms, smart contract, trustworthy access, mathematical modeling, cross network sharing, data tracking and auditing, and intelligent networking. We also provide a prototype design of B-RAN along with the latest experimental results. Accompanying the prosperity of blockchain in the recent decade, many studies have investigated underlying blockchain technologies and their advanced applications in wireless networks, e.g. 5G and IoT, as reviewed in the previous section.

However, most existing works fetch blockchain into specific scenarios separately without considering the panorama of deep and comprehensive incorporation of blockchain into wireless communications. In fact, future blockchain-empowered networking in 6G should be considered from a systematic point of view to establish an integrated system. The trust issues cannot be solved merely by introducing blockchain, but should take the complicated distrusted nature of different network layers into account to eventually form a trust foundation for 6G networks. Further more, most existing studies have not investigated.

The critical issues of blockchain in wireless environments, such as security, latency, scalability, cost, power consumption and so on. There is also a lack of mathematical models to characterize blockchain based wireless networks as well as the corresponding experimental results. Therefore, it is imperative to address these issues and integrate advanced blockchain technologies into a unified framework for upcoming 6G. The concept of B-RAN offers a novel paradigm for large-scale, heterogeneous

and trustworthy wireless networks . B-RAN acts as an open and unified framework for diverse applications to achieve resource pooling and sharing across sectors and presents an attractive solution for future 6G networks. B-RAN unites inherently untrustworthy network entities without any middleman and manages network access, authentication, authorization and accounting via trustful interactions.

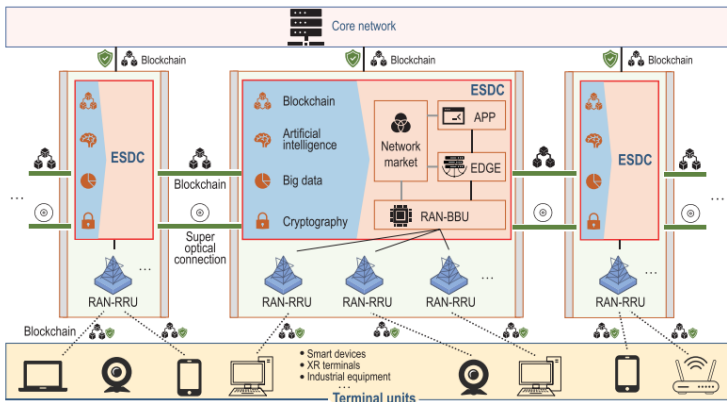


Via B-RAN, an MSP is established to connect different parties and facilitate resource and data sharing in a cooperative, flexible and secure way. B-RAN cannot only dynamically share computing, caching and communicating capabilities, but also deliver and spread intelligence across subnetworks. Federated-style learning can further optimize under-utilized resource allocation and network services in B-RAN. As a blockchain-as-a-service (BaaS) platform, B-RAN has distinctive security properties and is expected to provide enhanced functionalities of data exchange, privacy protection, tracking, supervision, etc.

The edge super data center (ESDC) consists of powerful baseband units (BBUs) and edge servers (EDGE) and adopts a number of innovative technologies such as blockchain, AI and big data. An ESDC along with a number of remote radio units (RRUs) acts as a super base station, i.e. an enhanced counterpart of eNodeB in 5G, and supports not only wireless services but also various local applications and the network market. Within an ESDC, blockchain guarantees endogenous safety with the help of cryptography, and assisted by AI and big data, facilitates many important functionalities such as secure access control, tracking and supervision of mobile terminals. Multiple ESDCs, which may belong to different parties,

are interlinked via super optical connections for high-speed data exchange, and wherein, blockchain enables trusted and reliable interactions among them.

In addition to ESDCs, blockchain also interconnects massive dissimilar terminal units (through RRUs), edge nodes and core networks, defining and governing their rights and obligations, and eventually achieves the network orchestration through on/off-chain smart contracts. More specifically, in an IoT scenario, B-RAN can establish mutual trust between IoT devices and access points (APs) in a distrusted environment through the underlying blockchain, and provide a scheme for future IoT/IoE in a multioperator network . This establishment of trust can avoid possibly selfish behaviors between untrustworthy devices and promote cooperation among individual IoT networks. By re-organizing multiple individual networks into a joint multi-operator network based on blockchain, B-RAN can efficiently integrate and utilize cross-network resources, such as spectra, APs, IoT devices and user data. Thus, in B-RAN, the IoT devices are not restricted to services from one subscribing SP, but can obtain resources and services across networks via effective incentive mechanisms.



Another imbedded application of B-RAN is blockchain-empowered MEC that can realize multiparty resource scheduling for an open and distributed network while providing privacy protection and data security for users. B-RAN enables direct communications between network users and MEC servers from different operators flexibly without relying on intermediary

agents. The storage and computation resources among MEC participants can be fully utilized by B-RAN to reduce the vacancy and redundancy of network management and achieve the efficient configuration of resource sharing and scheduling.

As the survey in the section entitled ‘Mining and consensus’ demonstrates, PoW exhibits strong robustness at the expense of great resource consumption. Since mobile devices are resource constrained, traditional consensus mechanisms (e.g. PoW and its variants) are not suitable in the mobile environment. Also, the confirmation delay is often unbearable for latency-sensitive wireless services. The drawbacks of great resource consumption and high latency become the major obstacles of traditional consensus mechanisms in a mobile environment. Besides the potential applicability of low-cost consensus protocols, such as proof of stake (PoS) and proof of activity (PoA), an identity-based consensus mechanism named PoD was developed for B-RAN.

Given the fact that B-RAN is comprised of a tremendous number of devices, the PoD utilizes a unique hardware identifier (ID) that is commonly used to distinguish different devices. Based on the unique ID, every device only needs to perform the hash query once for each slot. The device that obtains a hash query less than the target threshold will be granted as the winner of the current slot. PoD significantly reduces resource consumption by restricting the number of hash operations. In this case, the uniqueness of the ID is crucial to the safety and effectiveness of PoD. To achieve this, we should introduce and use more secure features as identifiers, e.g. location, radio frequency (RF) fingerprinting, hardware security module (HSM). As an example, RF fingerprinting utilizes the imperfections of transmitter hardware to construct a unique fingerprint that identifies the device.

Moreover, we can embed the HSM into the devices in B-RAN to prevent ID forgery and counterfeiting. As the unique device ID and other indispensable information is put into the device’s HSM, the users can only perform verifications without modifying the information in the HSM. Attackers can hardly alter the built-in device ID safeguarded by the HSM physically or digitally. The HSM may even erase the key information and render itself permanently inoperable if misbehaviors are detected. In addition, a novel satellite-aided blockchain consensus protocol was

devised . It makes full use of the advantages of wide coverage and ubiquitous connectivity to innovate the consensus protocol and can help construct a highly scalable space-terrestrial blockchain structure.

In each round of this consensus, the satellite is responsible for periodically generating oracles and multicasting them to the terrestrial blockchain network. An oracle is a random number used to select the only winning miner in that round, who has the right to create the unique and valid new block and broadcast it to other miners via the blockchain network. This method of selecting the winner does not require massive hash queries, thus greatly reducing the energy consumption during the consensus process. The simulation results show that the proposed consensus protocol can achieve higher throughput than PoW while maintaining the same security as PoW.

In addition, the delay of terrestrial P2P networks is usually long-tailed due to the large number of hops , while the propagation delay of satellite communication is almost fixed and more controllable. Therefore, this consensus protocol can also be an option for B-RAN in the space-terrestrial 6G networks. Moreover, in consensus mechanisms, one can also construct useful tasks instead of requiring participants to perform meaningless hash queries. For instance, large-scale resource allocation and scheduling in B-RAN is such a suitable mining task. Borrowing the principle of proof of learning (PoL) , participants in B-RAN can deploy diversiform intelligent algorithms to provide solutions to these tasks as a machine learning competition. The maintainer who offers the best solution to the scheduling scheme will be elected as the winner for the next round. Such machine learning competitions could be employed to provide solutions for manifold, complex tasks and optimize various schemes in B-RAN.

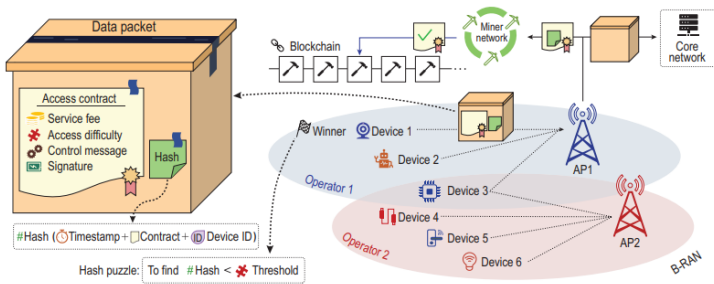
4.1 Smart Contract at Wireless 6G In Block Chain Technology:

The underlying blockchain and mechanisms in B-RAN guarantee system security and efficiency for resource sharing, data exchange and user access. The verifiable software codes in smart contracts ensure the consistent and automatic program execution for these services across the B-RAN network, and prevent backdoor viruses from being planted in the B-RAN system. Here, we introduce two smart contract-based mechanisms

for enhancing the security and efficiency of B-RAN. Fast smart contract deployment (FSCD) is an advanced mechanism proposed for accelerating and securing the service in B-RAN . By implementing the concept of template in smart contracts, the root contract in FSCD defines the service terms in detail, which is later automatically applied to all services. FSCD can effectively validate and trace service requests. Furthermore, it prevents forged and malicious requests from being accepted by blockchain, and thus reduces the potential risks involved in service request procedures. Moreover, the hash time locked contract (HTLC) can be utilized in B-RAN to enforce the fair resource exchange between SPs and clients.

The HTLC allows users to carry out trust-free payments outside the blockchain in an ‘off-chain’ payment channel by forming a ‘restraint’ between two transactors. Because of the ‘restraint’, the breaching party is doomed to play its unprofitable role in the HTLC-based resource exchange. In this way, the HTLC credibly reduces the risks (e.g. identity spoofing risks) between SPs and clients and enhances the safety of resource trading. Although B-RAN demonstrates its security and efficiency, a few issues remain unsettled.

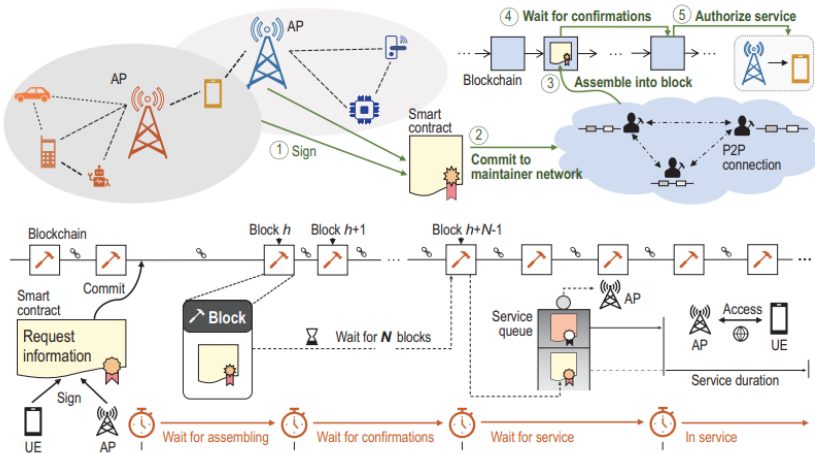
B-RAN is an MSP coordinating a host of networks or subnet works but approaches to safely isolate private information between them are still being investigated. Also, pre-computing attacks are difficult to prevent in PoD, where an attacker can use future timestamps to find a valid block in advance. Robust and efficient smart contract designs are imperative for conducting automatic penalties of violations.



It is expected that the 6G network will contain a massive number of heterogeneous devices that belong to multiple untrustworthy parties. These devices may compete for limited resources for self-interest and

simply ignore the pre-defined protocols, leading to a possible tragedy of the commons. Specifically, for grant-free access through shared links, such as IoT uplink, massive devices share a common access link without requesting permissions or dedicated resources. Because of the absence of trust, a selfish device may deliberately shorten its backoff period in random access to reduce access latency.

As the number of selfish devices increases, there will be disastrous congestion in the network, To eliminate mistrust among client devices and address the congestion in grant-free scenarios, a trustworthy access scheme named Hash Access was propose, along with its mathematical analysis and within the B-RAN framework. Each device is required to solve a hash puzzle by finding a hash value below a given threshold before transmitting packets. Otherwise, the device is denied access in the current slot. The hash puzzle is formulated by the current timestamp, its unique ID and the access contract. Owing to the pre-image resistance of the hash function, the answer to a hash puzzle can be easily verified but hardly forged. It is almost impossible for a rogue device to generate a fake hash value. Therefore, an enforced random backoff is embedded in the Hash Access scheme to reduce collisions, which can hardly be skipped by any device.



In this way, the Hash Access scheme enforces devices to obey the rule of access, so as to prevent selfish behavior of rogue devices and establishes trust between client devices. In addition, the threshold in a hash puzzle

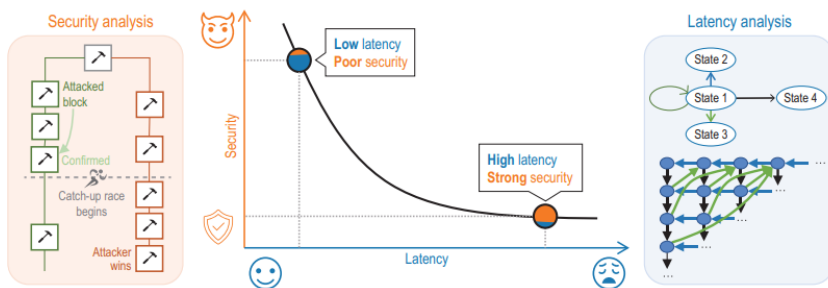
determines how hard it is for each device to access, which can be adjusted accordingly to control the traffic in B-RAN. Furthermore, Hash Access ensures that the uplink resources are shared fairly, which promotes multi-party cooperation and helps to integrate the cross-network resources and efficiently offload traffic.

In addition to the misbehavior of malicious IoT devices discussed above, there are many other device access security risks in different layers of a wireless network as investigated in the section entitled 'Secure access control'. Secure and robust device access control approaches for 6G networks are to be developed. B-RAN provides an ideal platform to integrate various access methods and protocols into the 6G architecture from a systematic point of view via establishing cooperative trust and security among heterogeneous entities that may have potential security risks. Very few works have noted that service latency will be a crucial problem for B-RAN as a price of decentralization, the length and controllability of which, unfortunately, is still unknown. As another critical aspect of B-RAN, security has not been thoroughly looked into yet. Therefore, an analytical model is urgent to explore the characteristics of B-RAN (such as latency and security) and to provide insightful guidelines for real-world implementations further.

we made an original attempt to mathematically model B-RAN and analytically characterize its properties and performances. Specifically, we modeled the block generation via a Poisson process and verified it by real data. We then established a queueing model embedded by a continuous time-homogeneous Markov process for BRAN. Based on the queueing model, we presented a general state transition graph, evaluated the service level latency in the average sense and revealed the impact of critical parameters on the B-RAN latency by further deriving tight upper and lower bounds. Meanwhile, we assessed the security level of B-RAN by considering the attacker's strategy.

From the above analysis on latency and security, we discovered an inherent relationship between them, which can be described by the latency-security trade-off curve. On the one hand, the request latency of B-RAN is quasi-linear to the block generation time, and it grows as the number of confirmations for verification or the block generation time increases. On the other hand, more confirmations are required to reduce

the probability of a successful attack. The confirmation number becomes the key factor in balancing the service latency and system security in B-RAN and shall be carefully selected. It is worth pointing out that such a trade off characterizes the achievable performance of BRAN comprehensively. Our analytical model provides meaningful inspirations for designing blockchain-based wireless networks with both enough security against malicious miners and affordable access latency.



Rather than an oligopoly, B-RAN recruits a large number of SPs and clients, enabling significant resource sharing across subnetworks. As the number of clients increases, more SPs will join out of economic incentives. With more SPs, the improved quality of service (QoS), in turn, attracts more clients, creating a positive feedback loop based on network effects.

As well as recruiting more SPs and clients, B-RAN functions as an MSP, a platform letting multilateral groups (SPs, clients, and others in B-RAN) on board and enabling direct interactions between them. Such multi sidedness leads to various sources of revenue in B-RAN. These assets or services from different participants are commodified and put into a vast resource pool in B-RAN and then virtualized via smart contract, promoting further resource sharing and pooling. Here we summarize several important kinds of resources in B-RAN.

1. Spectra. The spectra in B-RAN are virtualized as digitized spectrum assets. A spectrum asset can be defined as an exclusive usage right within the assigned time duration to transmit on a frequency range in a given coverage area. The utilization of spectrum assets from multiple spectrum holders will be more efficient and flexible than that of a single-operator network.

2. **Infrastructures.** Infrastructures in B-RAN include all types of APs and base stations (BSs), MEC and cloud servers, backhubs, etc. Infrastructures belonging to different hosts can be shared across SPs and individuals via computation offloading, data storage, or network access services. Such coordination can significantly reduce utilization redundancy and improve network efficiency.
3. **Devices.** Mobile client devices can be exploited to collectively gather data and extract information for large-scale services of SPs or other applications, while various IoT/IoE devices can be involved in crowdsensing. Also, the growth of client numbers will attract more SPs to BRAN and further achieve economies of scale. Client resources can benefit multilateral groups and motivate B-RAN to continue growing.
4. **Content.** Content in B-RAN can be media files, software, documents, applications, live streaming, etc. Not only will SPs provide content delivery services, but clients will also be encouraged to participate in providing content. Under the security and privacy protection of B-RAN, the content will be tamper-proof and accessed only by authorized users in delivery.
5. **Control.** Control rights over multiple devices can be viewed as resources in B-RAN. Network devices with functionality for packet forwarding or smart devices used as home appliances will function at the control command of all permitted users with a sharing key. With the underlying blockchain, a more trustworthy and reliable control can be implemented in B-RAN.
6. **Energy.** Energy in B-RAN is usually electricity energy coming from fossil or renewable energy resources. Devices with sufficient idle energy can conduct a discharging operation for energy supply demand payment. Energy prosumers and consumers can interact with each other securely and fairly in B-RAN.
7. **Intelligence.** Intelligence in B-RAN represents trusted learning models and capabilities, such as computing, caching and communicating, to perform learning algorithms. In B-RAN, learning models can be performed in a federated manner on heterogeneous devices and the data confidentiality of such collaborative learning process will be

ensured. Reliable intelligence will be distributed efficiently in B-RAN.

The following is the basic procedure of how B-RAN works to help a user equipment (UE) request services from an SP.

1. In preparation for access, the UE and SP should first enter a service-level agreement (SLA) containing details including service types and compensation rates. The service terms and fees will be explicitly recorded in a smart contract authorized by the digital signatures of both sides.
2. The smart contract is committed to the blockchain network, waiting for the blockchain maintainers to verify its validity.
3. The blockchain network maintainers finish the verification of the smart contract and will record it in a new block after the current round of consensus is reached.
4. The block is accepted into the main chain after a certain amount of blocks as confirmations built on top of it. The smart contract is then confirmed secure and qualified to enter the service queue.
5. When finishing the services of preceding requests, the SP will deliver the access service to the UE according to the request information in the smart contract.

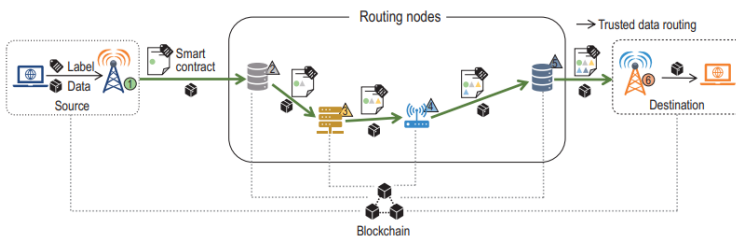
It is worth noting that the superiority of B-RAN regarding efficiency lies in the network pooling principle that requires flexible offloading and sharing between subnetworks. In the previous example, the UE has established trust with SPs and the UE can thus access and use resources pooled by other SPs in B-RAN. The trading and roaming charges would be calculated and settled periodically by smart contracts. In this case, the maintainers in B-RAN can use some intelligent algorithms to allocate and distribute the pooled resources for higher network efficiency. As a result, mobile devices may access suitable SPs belonging to the subnetworks that likely provide higher-quality coverage for the UEs in their current locations.

Data tracking and auditing ,In the era of big data, the expeditious growth of data has brought many challenges for enterprises, societies and

governments. Data breaches occur more frequently than ever and are now causing serious security risks. Wireless networks, due to openness and mobility, are more vulnerable to data leakage and malicious intrusion. The increasing demand of data security and user privacy calls for necessary data tracking and auditing approaches to detect data leakage and prevent unauthorized access and usage of sensitive data. Some countries and organizations have issued relevant regulations on data usage to curb data leakage and ensure data tracking and reliable auditing.

The current network data tracking and auditing methods are mostly based on deep packet inspection (DPI) and traffic analysis. DPI based schemes often require manual discoveries of traffic characteristics and a large amount of data processing, and traffic analysis may also suffer from real-time performance and deployment efficiency, which make them difficult to scale with the rapid growth of big data. Note that data marking techniques can also be used to trace network flows, e.g. in Refs, two watermarking schemes were designed for data traceback and analysis in mobile networks.

Recently, several studies have shown the feasibility of using blockchain to fulfill or facilitate data tracking and auditing for cryptocurrency, health care and food supply chains. Yet, blockchain-enabled data tracking and auditing approaches for wireless networks are still open. In B-RAN, data are delivered through several relay paths via a number of devices and infrastructures.



A blockchain consisting of entities from multiple parties can record the routing path of data in a trustworthy and transparent way and thus is suitable for tracking and auditing data. By incorporating the data marking technique, a data tracking and auditing scheme in B-RAN is designed. The scheme lets routing nodes, which may be from various manufactures and operators, participate in B-RAN and report their sight of routing data to

the blockchain via smart contracts. To protect the authenticity of data and its origin, the data source is required to generate an immutable digital label for its transmitting data using the trusted platform module (TPM) inside its device

Smart contract records the data label and information of the source. In addition, each relay node has to add its digital signature and commit the latest contract to the blockchain, which forms a trusted routing path consisting of smart contracts. Thus, the relaying path of data is jointly audited by the multiple parties in BRAN and can hardly be forged or modified since the data paths are secured by the blockchain. Also, this scheme can facilitate the data review and violation monitoring conducted by regulatory authorities.

B-RAN can provide an intelligent resource provisioning mechanism to manage network resources in a distributed learning approach. The maintainers in B-RAN can monitor the resource conditions and optimize under-utilized resource assignment through machine learning technologies. As discussed in the section entitled ‘Consensus mechanisms’, the intelligent consensus of B-RAN provides credible prospects for spectra and infrastructure sharing, which helps network operators better serve customers. Additionally, energy trading, computation offloading and storage sharing can also be achieved in B-RAN.

Because of its distributed nature, B-RAN inherently supports federated-style learning. B-RAN can exchange trusted models and share the capabilities that are necessary for machine learning, resulting in high efficiency of federated-style learning. As the underlying blockchain establishes multifold trust relationships for B-RAN, network entities can share intelligence in an open, compatible manner. Also, B-RAN can track the entire process of the data procedure for trust considerations, enhancing the interpretability and credibility of machine learning. Therefore, B-RAN will promote the development of federated-style learning and eventually achieve strong trusted intelligence.

In turn, B-RAN also improves network quality and provides intelligent services. In response to clients’ requests, B-RAN maintainers can schedule and assign services via a distributed learning approach, leading to an

adaptive smart network. BRAN can collect users' data to adjust real-time service quality, while service scheduling is performed as a federated learning task among different network entities. Clients can also select and use the appropriate signal transmission medium such as millimeter wave, visible light, infrared and terahertz wave, depending on the specific scenarios.

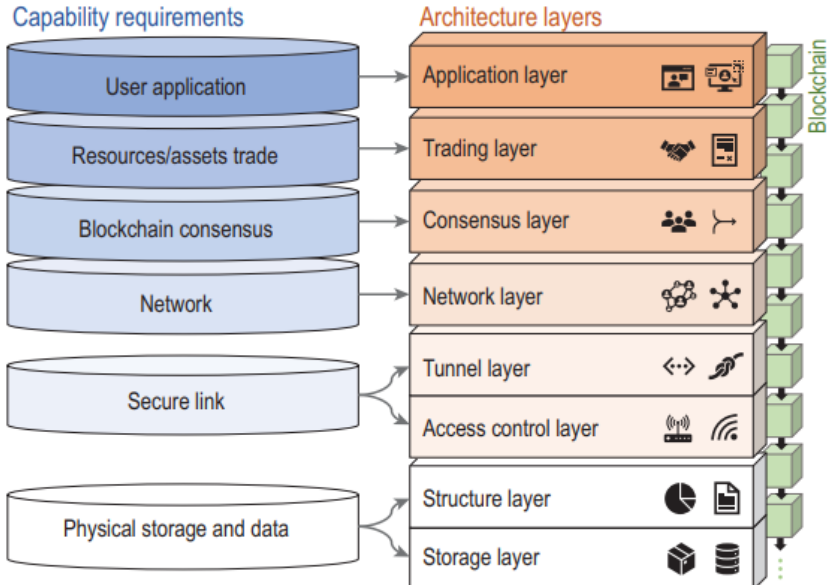
Also, B-RAN can monitor the network status and utilize distributed learning to avoid traffic congestion and achieve fast fault locations. Via deep learning from historical data, B-RAN can predict the trend of traffic and prevent traffic congestion. To achieve a balance between limited network resources and service quality, data packets need to be prioritized to ensure optimum experience for network operators and users. This can be achieved by utilizing AI technology. With the proliferation of devices and users, fault location has ushered in new challenges due to the spatial correlation of alert messages and the interaction between failures via machine learning algorithms, such as the learn vector quantization neural network and the deep neural evolution network.

In order to implement the proposed design and better test its performance, we assess the basic capability needs in B-RAN and construct a corresponding prototype. The capability needs cover six aspects, including physical storage and data structure, secure link, network, blockchain consensus, resources and assets trading, and user applications. Based on the evaluated needs, we further design the corresponding architecture layers for the prototype. We introduce the access control layer, tunnel layer, consensus layer and trading layer into our architecture. Apart from these, we also use several traditional network system layers (i.e. storage layer, structure layer network layer and application layer) to support basic operations of our prototype. Considering the unique application scenarios of B-RAN, we further incorporate the mechanisms FSCD, HTLC and Hash Access into the architecture to improve the overall performance of the prototype system. We now provide more details about the basic capability needs and the design of the architecture layers

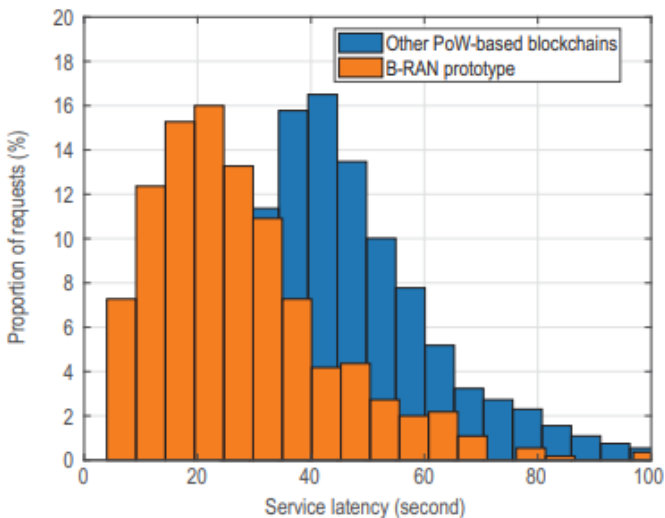
1. Physical storage and data. All the blockchain data or information associated with B-RAN such as the ordered transactions, digital actions and cryptographic keys form the structure layer. Such data are stored by servers or any active electronic devices in the storage layer.

Not all devices will store a full copy of a blockchain, as some mobile devices can store partial information as lightweight nodes.

2. **Secure link.** A secure link between different sides is established in B-RAN. By leveraging the principle of HTLC in the tunnel layer, the payment channel between terminals and APs is trust free. Transmission reliability is also ensured by flow control and error detection in the access control layer. Link duration, fees and even physical transfer media are regulated by smart contracts.
3. **Network.** Subnetworks with various structures in B-RAN form the network. The nodes and the links between them in the network layer are responsible for nodes discovery and communication and synchronize with each other to maintain the distributed network.
4. **Blockchain consensus.** The consensus in B-RAN is responsible for generating and validating the blocks and ensuring participants reach a consensus about the broadcast transaction
5. **Resources/assets trading.** The execution of resources/assets trading is performed with the underlying rules in B-RAN to keep the fairness between SPs and clients. Such fairness is ensured by smart-contract-enabled service-level agreements in the trading layer.
6. **User application.** User applications on top of the blockchain are designed for clients to interact with the blockchain and smart contract. Application programming interfaces in the application layer will also be provided for developers to implement some other desired functionality apart from access services



we have identified the critical trust related issues in wireless networks that impede the evolution of current 5G networks towards more efficient and secure 6G networks. Upon a brief introduction of the fundamentals of blockchain, we comprehensively investigated the recent research works on applying blockchain to wireless networks from several aspects, including resource sharing, trusted data interaction, secure access control, privacy protection, tracing, certification and supervision.



Then, a unified B-RAN framework was proposed as a trustworthy and secure paradigm for 6G networking by utilizing blockchain technologies with enhanced efficiency and security. We elaborated on the critical elements of B-RAN, such as consensus mechanisms, smart contract, trustworthy access, mathematical modeling, cross-network sharing, data tracking and auditing, and intelligent networking, and provided the prototype design of B-RAN along with the latest experimental results.

4.2 Applications Of Wireless Blockchain Technology:

There are a large number of hardware devices in the network of telecom operators, which are widely distributed in the core network, transmission network, data network, access network and other fields. Currently facing the following problems : the number of equipment, variety, manufacturers, batches, it is difficult to form top-down transparent penetrating management ; The whole process technologies of automatic collection, trusted storage, record traceability and intelligent analysis of inspection data are still incomplete, and data analysis is difficult. The underlying data storage based on blockchain, combined with IoT, AI and other technologies, can provide equipment inspection and equipment life cycle management services for operators to improve the quality and efficiency of inspection.

From the level of provincial companies and groups, provincial companies inspect the equipment as required and record it on the block chain ; The group obtains the trusted data on the chain and checks the implementation of equipment inspection in real time ; From the perspective of operators and equipment vendors, the equipment management platform interacts with the business system of operators through interfaces, synchronizes equipment fault information and equipment risk information in real time, predicts faults in advance and processes them in time

Wireless spectrum resource is an essential cornerstone to support wireless communication data transmission, which belongs to the important strategic resources of the country. With the exponential explosion of communication data, the shortage of wireless spectrum resources and low spectrum utilization have emerged. However, there are still problems such as the lack of unified record of user frequency information, the leakage of

node privacy, and the lack of sufficient trust mechanism for the sharing transaction of spectrum resources.

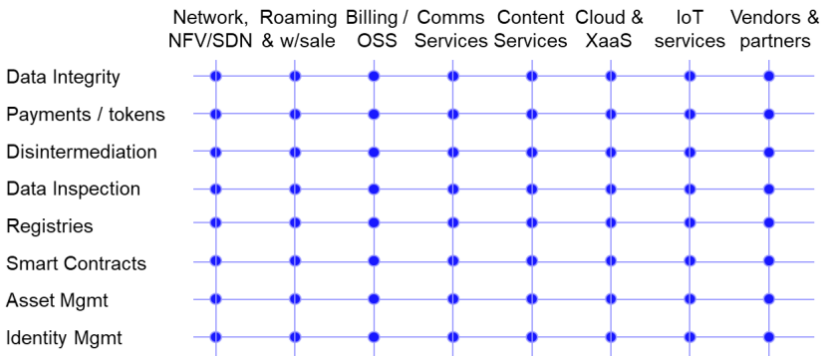
The dynamic spectrum sharing based on blockchain can make use of the distributed book structure provided by blockchain to make the circulation records of spectrum trading transparent, untampered and traceable. All participants in the blockchain can supervise the information and establish the trust relationship between the chains of spectrum trading. Based on the consensus mechanism of block chain, the authentication information and spectrum resources are effectively bound and registered before the spectrum transaction, so that the whole network node can verify the validity of the authentication information at the same time, and thus identify the owner of the spectrum assets. By establishing a new and reliable spectrum resource rights system, it provides a strong guarantee for maintaining spectrum sovereignty. The rules are established in the spectrum transaction, and the intelligent contract code representation is used instead of the contract to realize the chain payment and improve the automation level of the transaction.

Equipment identity management is a typical application of blockchain penetrating into the Internet of Things. Blockchain can provide each Internet of Things equipment with a unique digital identity ID, register the ID onto the chain, and record all information of the digital identity through the jointly maintained accounts, so as to realize the identity authentication, access control, anti-counterfeiting and traceability of the equipment. By constructing the equipment identity management system based on blockchain as the background accounting system, the equipment identity can be obtained and verified by the implementation of the blockchain intelligent contract consensus, and the mapping relationship between the identity of individual entities and the identity of the equipment at the end of the ownership can be established, so that the equipment end can also verify whether the identity of the requester has access rights in the authorization mode, and realize the bidirectional credible and safe traceability verification between the equipment end and the user.

International roaming service is one of the many services that telecom industry mobile Internet service providers or operators can provide. From the perspective of international roaming settlement mechanism, the generation process of international roaming charges is more complex,

involving domestic operators and roaming operators. At present, there are more than 700 operators in the world. The opening process of roaming business between operators is complicated and there are many risk points. If the roaming business is opened, it is necessary to establish mutual roaming relationship, negotiation of roaming protocol and roaming settlement. Blockchain technology can meet the challenges of safety and efficiency of operators of international roaming settlement business.

Using the characteristics of blockchain technology in trusted value exchange and tamper proof, a trusted and mutual authentication roaming protocol file and financial settlement file system can be shared between operators and their roaming partners. At the same time, call list verification and bill reconciliation settlement are made. All roaming public reference records are chained to realize traceability, safety and transparency, improve settlement efficiency, and reduce the complex dispute settlement and arbitration mechanism caused by inconsistency.

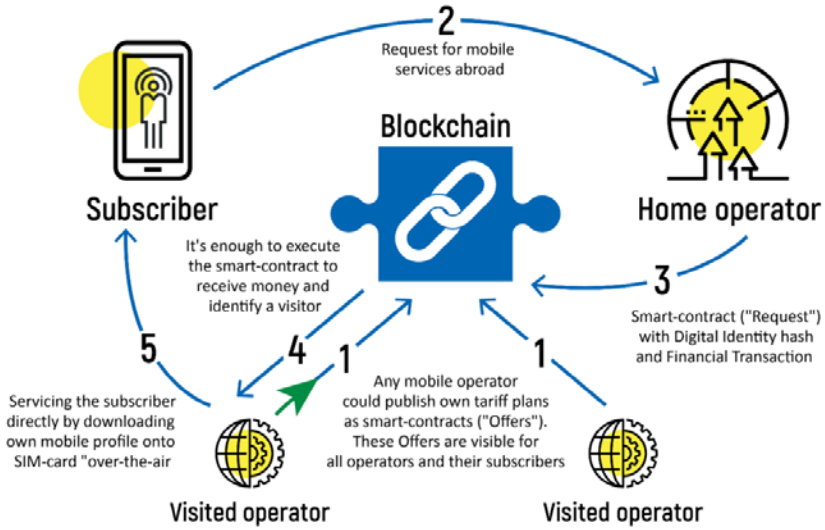


With the wide popularization and application of big data, the value of data resources is gradually valued and recognized, and the demand for data circulation and sharing is also increasing. Driven by the active promotion of national policies and the drive of local governments and industry, telecommunication operators have actively arranged and practiced the circulation and sharing of telecommunication data, but there are still the following problems: lack of standardization and completeness in data transactions, and the core issues such as data confirmation and data pricing have not been fully solved; Data security and privacy protection requirements are increasingly prominent, lack of technical means.

The existing centralized way of data circulation lacks credibility in the telecommunications industry. Building a decentralized data circulation and system based on blockchain technology, sharing metadata, sample data, data acquisition requirements, data transactions and ownership transfer information; Before the generation or circulation of data resources, the confirmation information and data resources are effectively bound and registered to provide technical support for the maintenance of data sovereignty ; The intelligent contract rule code is used to replace the contract, realize the automatic acquisition of online payment and data access rights, and improve the level of transaction automation.

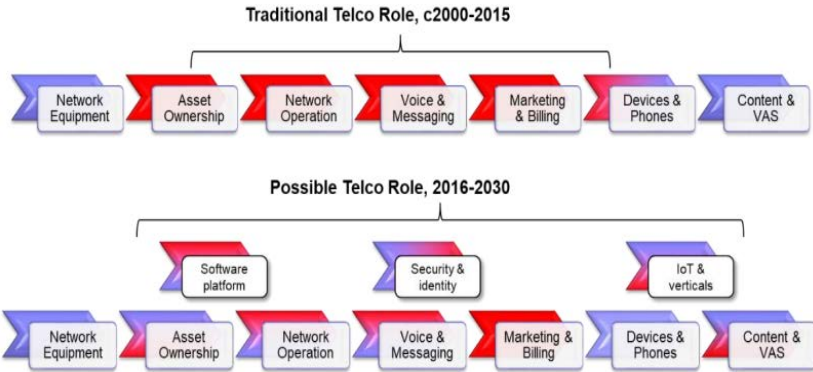
With the popularization and deepening of the Internet of Things technology in the industry, human society is entering a new era of “ Internet of Things, ” but there are still many problems that restrict the Internet of Things to play its potential ability, including numerous access devices, and the security and credibility of the equipment itself and its collected data are difficult to guarantee. The ability to centralize data storage devices and users and control devices can easily cause privacy and security concerns; There is no effective cooperation mechanism between industry applications, and the value transfer of application data is still difficult.

The combination of blockchain technology and Internet of Things technology can achieve the effect of dual-sword combination, including but not limited to expanding the opening capacity of IoT platform and establishing data stores based on blockchain technology, and promoting the high-speed flow of Internet of Things data. Blockchain IoT platform adopts a unified data model record to ensure consistent understanding of data between different applications ; Blockchain is used to record data fingerprints, encryption mechanism and privacy authorization mechanism to ensure user privacy and data asset security. It can also maximize the connotation of sharing economy in smart home Internet of Things, environmental protection Internet of Things, vehicle networking, computer room leasing and other scenarios.



User 3A (authentication / authentication / billing), interconnection and interoperability, and cost settlement are three major obstacles affecting the global cloud network integration of operators. Blockchain technology helps to achieve business collaboration between cloud and multi-network from authentication to charging. For cross-network connection, blockchain + AI identifies massive hardware and parameters, and analyzes the performance and fault of interconnection and interoperability in real time; For cross-cloud docking, blockchain + AI automatically records and analyzes the cloud data throughput and interface behavior, and provides a credible basis for cloud collaboration and settlement; For cloud network integration, cloud network business based on the alliance chain, the alliance enterprise “cloud + multi-network” sales authorization certification, accounting traceability.

In the MEC at the edge of the mobile network, due to the limitations of the computer room and environment, the hardware resources of MEC are often limited, and there are some devices around MEC that have strong processing capabilities, such as mobile phones / cameras / personal computers. These resources may be used to strengthen the ability of MEC. Local network servers connected by MEC, or some personal computers in the local network, have certain storage and computing resources.



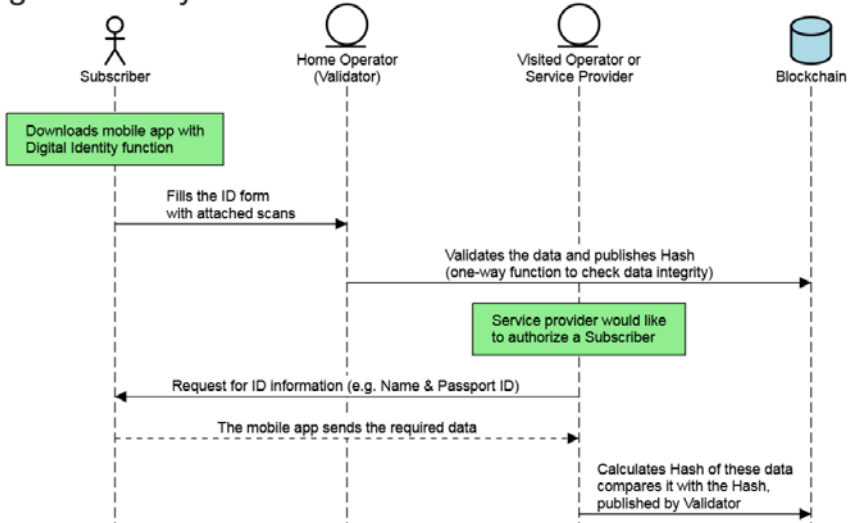
Using blockchain technology, the resource network of “infinite nodes” can be constructed by aggregating all kinds of idle resources, so as to aggregate into a powerful resource pool and optimize the real-time deployment and utilization of resources distributed in each node, which can effectively help MEC deployers to save costs and improve efficiency. The combination of MEC blockchain technology can provide rich computing resources for sharing, for video broadcast, local caching and other services, GPU resources can also be used for AI training. Operators of MEC can make returns by means of chain integration or chain payment. After the transaction, MEC can operate the corresponding resources on the access blockchain.

By gathering resources such as industry, university and research, supporting universities and research institutes to build blockchain innovation laboratories and research centers, closely tracking the development frontiers of international blockchain technology, building a basic blockchain technology research and development platform, accelerating the innovation and evolution of core technologies such as asymmetric cryptography, consensus algorithms, intelligent contracts, and reducing the difficulty of landing blockchain technology applications.

At present, the development of blockchain industry is seriously fragmented, and there is no industrialization-oriented blockchain standard system. In the new track of blockchain, operators ' collaborative progress is the trend, and BSN provides a good opportunity for deep cooperation among the three. BSN is a platform for operators to cooperate closely with blockchain industry, which helps to jointly explore the application value

of blockchain in digital assets, telecommunications assets, and new generation network construction.

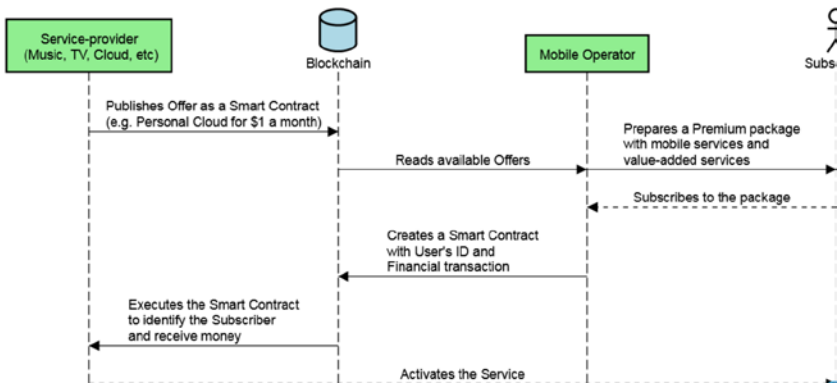
Digital Identity as a new revenue stream



Through co-construction and promotion of BSN blockchain network deployment, the high cost problem of LAN architecture for alliance chain applications is changed. Relying on existing network resources and provincial and municipal data centers, urban public nodes throughout the country are established to form a blockchain service platform serving the whole country, so as to reduce the development, deployment, operation and maintenance, interoperability supervision costs of blockchain applications.

Aiming at the application scenarios of telecom equipment management, dynamic spectrum management and sharing, digital identity authentication, international roaming settlement, data circulation and sharing, Internet of Things, cloud network integration, and multi-access edge computing, this paper organizes and implements representative blockchain technology application projects, establishes models, forms a replicable and easy-to-operate blockchain technology application demonstration platform, and promotes the integration and development of blockchain technology and telecom industry.

Hundreds of Value Added Services for Mobile Operator



CHAPTER - 5

Security Of Block Chain In Telecom Operations

The current signaling technology used by telecommunication operators to communicate on the authentication of roaming users is no longer as effective as it used to be. There are several reasons for this including authentication delays, security concerns, and cost. With respect to authentication delays, users will sometimes have to wait for periods of between 5 to 15 minutes until they get authorization for roaming service. In the age of near real-time response expectations, this delay is too long.

Furthermore – and ever more critical – is the fact that the existing encryption method used by the industry for roaming purposes – SS7 encryption – has been compromised. In fact, it was shown to be hackable via brute force over a decade ago. Obviously, a new and more secure approach is needed. The third reason for upgrading roaming authentication is cost. Telecommunications companies are paying large monthly fees for their existing authentication services, but these services charges are not cost effective, nor do they meet the requirements they were designed for.

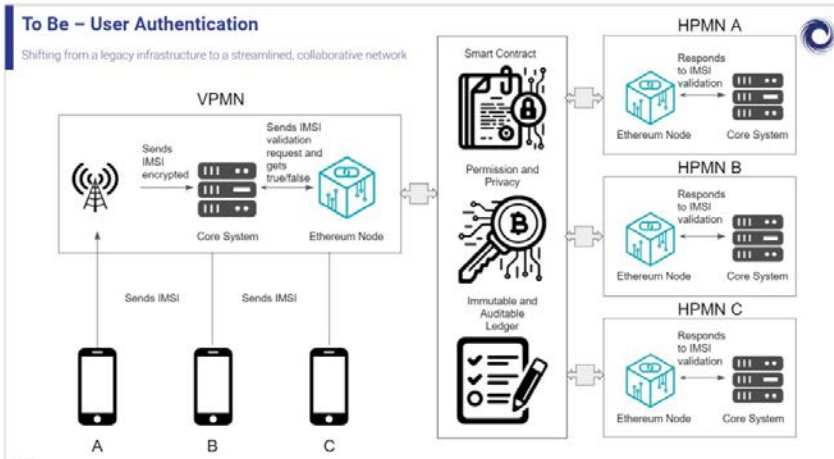
A proposed solution is to make use of a blockchain-enabled communication network to facilitate the provisioning of services by telecommunication operators for users roaming between networks. This blockchain-based facility would be secured using modern encryption methods (SHA-3, for example) with each operator holding a public/private key pair. The idea is to create a registry of public keys for each operator on a permissioned basis so that each

operator has access to other operators. This registry would thereby facilitate direct/encrypted communication of service authorizations for roaming requests – allowing for a common, secure, and traceable improvement from the current method.

The primary stakeholders are the telecommunication operators whereas the beneficiaries are both the operators and their customers. The GSMA (Global System for Mobile Communications) is a global trade body that represents the interests of mobile network operators worldwide and would likely be one of the organizations to serve as a primary driver for mobile carriers.

	1. User identifies itself to the VPMN	2. VPMN's VLR requests confirm. from HPMN's HLR	3. HPMN to confirm user's accessible services	4. HPMN confirms accessible services to VPMN
Process Step Description	a) The user turns his/her cell phone on while being in the visited country b) The cell phone communicates its IMSI number to the VPMN's Visitor Location Register	a) VPMN encrypts IMSI number b) The VPMN's VLR sends encrypted IMSI to the HPMN's HLR	a) HPMN decrypts IMSI number b) HPMN confirms within its database the services that its user should have access to while abroad c) HPMN encrypts the returned value for user's accessible services	a) HPMN sends encrypted user's accessible services to VPMN b) VPMN decrypts the accessible services propagated by HPMN
Actors	- User - Visited Public Mobile Network	- Visited Public Mobile Network - Home Public Mobile Network	- Home Public Mobile Network	- Home Public Mobile Network - Visitor Public Mobile Network
Network Participants / Consensus	- VPMN Node	- VPMN Node - HPMN Node	- HPMN Node	- HPMN Node - VPMN Node
Assets in Play	- IMSI Number	- Encrypted IMSI Number	- Encrypted IMSI number - Decrypted IMSI number - 1/0 per service requested by user - Encrypted values for user's accessible services	- Encrypted values for user's accessible services - Decrypted values ^
Business Rules (Smart Contract)	- Creation of record for user (consumer) - Identification of corresponding HPMN based on IMSI	- VPMN hashes the IMSI number - VPMN communicates encrypted IMSI to HPMN	- HPMN decrypts IMSI number - HPMN submits decrypted IMSI to off-chain database - HPMN maps user's accessible services - HPMN encrypts accessible services	- VPMN decrypts user's accessible services - VPMN confirms to off-chain database the services to be provided to user
Transaction on Ledger		- VPMN propagates encrypted IMSI number on ledger	- HPMN propagates encrypted accessible services	- VPMN confirms activation of user services

To add to the workflow above, here is a high-level schematic that describes the interfaces and some of the underlying components. By using a blockchain-based solution, carriers benefit from shared schemas and standardized transaction processing (via smart contracts) that provide better security and faster response times than the current solution.



Offering and supporting roaming telecom capabilities is an important service component for telecommunications companies but it must be profitable for the carriers in order to manage and maintain such services. Any such provisioning must also provide a seamless and low cost/no cost experience for mobile users. Inter-carrier policies, along with the transaction and billing overhead involved with roaming, however, have become quite complex. This combination presents difficult challenges for carriers, especially when it comes to reconciling roaming services charges between operators. The requirements for a global solution that might improve on the current approach are, not surprisingly, quite strict.

Any provisioning and reconciliation solution must not only manage multiple relationships, it must also manage complicated financial relationships with varying laws and regulations in different countries and regions around the world. From an internal carrier standpoint, supporting roaming capabilities with existing approaches has become quite difficult due to these financial and business workflow complexities, this is especially true when combined with the user expectations regarding

service interoperability. When looking at a new roaming reconciliation system, a number of concerns arise.

A few of the more important concerns include:

1. Sharing sensitive business data with other companies
2. Protecting against spoofing and user fraud
3. Processing large volumes of data

To solve the problem, various companies involved with mobile roaming have formed a consortium that proposes to specify a telecommunication roaming service solution that can communicate and share sensitive data directly within a blockchain network. In particular, the solution addresses the use of both Layer 1 (decentralized ledger) and Layer 2 (state channels) components, in order to provide both immutability and record keeping along with enhanced throughput and scale needed to support real-time global telecommunications. Via this consortium, roaming contracts and business flows can be developed, propagated, audited, and enforced. These business flows and contracts are expressed via smart contracts within a blockchain solution.

Among other transactional needs, the proposed smart contracts address the following areas:

- Matching the roaming call log with a fee list along with performing a service fee calculation
- Forwarding the call log of the user to the home carrier from the visited carrier
- Creating and sending an invoice for service charges and sending to the home carrier from the visited carrier
- Confirming receipt of invoice(s) and call logs by the home carrier
- Reconciling sent and received invoices and creating a balance of payments account with other carriers
- Making payment of open balances, carrying balances forward, and/or disputing any transactional elements

with an improved roaming solution, Telco's will be able to better correlate a user's non-home carrier usage with a user's contract to provide greater

transparency and faster service response and accommodation. The benefits for users are that they get great service flexibility and decreased service fees, which, in turn, will increase their usage. For telecommunication companies, the benefits include reduced costs, increased customer loyalty, and improved fraud prevention.

- Network-related data and registry information can be exposed on a permissioned basis within the blockchain network whereas private transactions and data can be encrypted and processed via zero-knowledge proof algorithms.
- The consensus algorithm(s) used can be optimized to reflect the permissioned nature of the network as well as meet the needs of the contemplated throughput. The proposed algorithm is currently based on proof-of-authority consensus, which allows for only trusted parties to have roles in validating and verifying the transactions.
- Data processing can be minimized by transmitting only relevant data to roaming operator node.
- Transparency and Trust: Trust between roaming partners will be secured by both the “mutual monitoring” and “tamper-resistance” nature of a blockchain solution. Carriers can run and maintain nodes within the same network and therefore have a role in generating consensus for transactional records as well as validating and verifying each transaction block. Multilateral deals that incorporate and enhance with transparency and trust will also be possible.
- Smart Contract Visibility: Multilateral contracts can be executed and managed in a more transparent and faithful manner. Primary flows between parties will be automated and facilitated by smart contracts.
 - Visiting carrier: Getting user info in order to services → supply network service → write call-log to blockchain
 - Home carrier: Confirm call-log and invoice from visiting carrier → settle accounts and pay/receive payments.
- Real-Time Processing: Another significant advantage of moving to a blockchain-based solution is the ability to process transactions in real-time and maintain more current roaming balances between carriers.

(Although the performance of blockchain networks is often criticized, permissioned/private network in conjunction with the use of state channels are designed to handle the type of throughput contemplated here.) This real-time capability enables carriers to more readily know what is going on with cross-carrier traffic as well as stay on top of their business and revenue and expense forecasts and actuals.

- **Cost Reduction:** All the above benefits will allow carriers to reduce costs related to confirmation time, the adjustment process, and other post-transaction reconciliation that currently takes place. Doing the cost adjustments concurrently with the service provisioning will eliminate a significant amount of overhead and post-service activity. The commonality of the solution and the leverage gained by visible contracts expressed as executable code will also prove to be a significant savings for carriers.

The benefits of an IOT trust system executed via blockchain technologies are many. Here are just a few of the benefits.

- **Decentralized Ecosystem** — Using a decentralized blockchain solution reduces the opportunity whereby a single party can establish or define trust within an ecosystem. Consensus algorithms along with an immutable ledger improves the collection of data as well as assures submitted information cannot be altered.
- **Open Ecosystem** – A solution via blockchain would likely by nature be more open, thereby allowing new parties to contribute criteria used for trust decisions. This openness would also allow for and facilitate dynamic changes in trust attributes.
- **Standard Protocols / Shared Data Formats** – The decentralized nature of blockchain technology means that all parties use the same protocols and data schemas and have access to the same data. This standardization is largely overlooked benefit in that integration and ETL work – which is common with interconnected systems – is largely eliminated.
- **Increased Longevity** – The decentralized operation of an IOT device trust network would conceivably increase the longevity of a solution in that it would be independent of any one party. Centralized hubs and

registries are at the mercy of their owners and different incentives and motivations can alter the direction and purpose of a system. Decentralized systems are more adept at tempering single source motivations.

- **Reduced Attack Service** – A distributed network can in many cases reduce the attack surface for many types of security attacks. An example is Denial of Service (DoS). The more nodes in the system, the less effective a DoS will be.

Transacting parties also gain additional benefits via the flexibility and open nature of the network and data. Any party that is making use of IOT trust attributes within the system can define what is trustworthy based upon their needs, the specifics of the transaction, and the identity of the other party. They can use any of the information that is available to them as they see fit, without necessarily relying on a central or authorizing authority. Now certainly there are possible downsides in that this flexibility may open up security issues for those less adept although we expect some standardization via smart contracts and other mechanisms that will set forth industry best practices for varying trust levels and authorities.

- **Network Structure and Consensus** – One of the primary decisions would be how to structure the network – on a distinct permissioned blockchain, on a permissioned sidechain anchoring to a public chain, and/or some other type of hybrid approach whereby some data is public and used as a catalog/registry where other information is exposed on peer-to-peer basis. A related concern is the consensus algorithm to use and the node structure – first node operator, submitter, registrant, and verifier.
- **Third Party Access, Security, and Data Size** – Related to the point above – network structure and consensus – is how open the network will be to allow participation by new parties. It's one thing to access the data. It's another to be able to update information both with respect to security concerns as well as with data size and growth. The number of devices currently in use along with the estimates point to very large numbers. Adding additional attributes for each device increases the data size exponentially.

- Record Attribution and Identity – Another decision is how to establish trust in the submitted information with respect to the submitter’s identity. Given the underlying cryptography, the submitter can be trusted to have the right credentials to post but there is and will be a question as to how to ensure the submitter is who they claim to be. This is no different than many current Web 2.0 solutions as well as blockchain solutions, just something that needs to be addressed – given the premise that records provided a “trusted” view of the device.
- Network Incentives – Rounding up the top list of challenges is how to create the right incentives for operating a network. A decentralized network is far different from a centralized hub when it comes to economic models, revenues, and costs. It’s entirely conceivable that device manufacturers and network operators would support much of the costs for such a network either by funding development and/or maintaining nodes. Extending this operational capability to other parties (such as corporations who might want to use the data as part of their security authorization) would certainly extend the network reach and capabilities (assuming the inclusion of additional trust attributes). How the incentive and operational cost structure might work in this scenario is something that is not readily apparent and would need certainly need some study and attention.

Blockchain technology promises to enable a variety of decentralized services where the participants do not have to have to create or establish prior trust toward other participants. Ethereum in particular via its support of Turing-complete smart contracts may be well suited to bring about solutions to the data-related challenges facing telecommunication providers. When it comes to privacy by design, GDPR addresses pseudonymization and anonymization techniques.

As any data stored on blockchain may constitute personal data, developers and companies which are likely to be subject to GDPR must limit the kind or amount of personal data stored on blockchain, and come up with new methods to anonymize data by utilizing some state-of-the-art technologies such as Zero Knowledge Proofs for the minimization of possible conflict with GDPR. In terms of “the right to be forgotten”, personal data related to subscribers should be kept separate from the blockchain in an “off-

chain” data storage because of the immutability characteristic of blockchain, with only its cryptographic hash value or evidence on blockchain platform. By doing so, personal data can be erased in case of subscribers’ request or specified grounds for deleting their information without impacting the integrity of the blockchain.

Blockchain networks can be used to establish a record of data events and transactions. While the data of the event itself (i.e. the user, the particular use or notification) may not be included in the transaction record, a notation as to its occurrence might establish an immutable record its existence. For example, a telecommunications service provider might generate and store ‘customer insights’ about individual and/or groupings of their subscriber customers – after collecting, processing and analyzing data provided by subscribers. In the course of this offering, they would notify individual or groups of customers of the availability of the new insight and offer to ‘return’ or ‘send’ such insight to the customers. These notifications might then be recorded into the Ethereum blockchain as having taken place at a time – with a link to permissioned records that would provide specific details on the notifications and their derivation.

Subscribers could either accept or decline such offer, where such indication might also be recorded on the blockchain as an event. If an offer is accepted, the telco service provider would send the insights, along with transaction metadata, to the respective customer. The sending mechanism may be by way of use of mobile phone text messages, in text or file formats, customer’s emails, cloud-based service accounts, or other mechanisms. The insight information is then stored in encrypted format in a repository – such as the mobile phone, SIM card, any other online or offline device, or a cloud storage – using the subscriber’s public key as the lookup key.

When an individual wish to ‘read’ the insight data, they would access the insights via the key, decrypt it using their private key (which would have been pre-installed or otherwise a prior provisioned to the individual), and privately consume it. (This access and decryption event might also be recorded on the blockchain.)

Any individual may wish to sell or trade the whole or part of the insight information to a third party or may wish to simply share it with a friend or

other party. The individual's indication of their wish to share, sell, or trade their insight information, along with some metadata describing it for the purpose of discovery by a third party, would also be recorded as an event. Such an indication could also be broadcast or similarly shared in a blockchain-based 'marketplace' like system.

If any individual or a third-party institute who participates in the blockchain-based 'data marketplace' finds a description of insight information that it may be interested in, a sharing-request, buy-signal, or trade-signal may emanate and run through the marketplace. All such signaling may also be recorded via a blockchain record. There may be third-party aggregator or broker who may aggregate insight information from multitudes of subscribers and sell or trade aggregated such information on behalf of the subscribers who offered up their insight information as well as any third party in demand of such insight information.

The telco service provider may act as such an aggregator or a broker. Any share, sell, or trade activities are all recorded into the blockchain. The telco service provider may not directly sell the insight information in decrypted format. It may only direct the prospective customer to a link whereby the customer would be able to retrieve the stored insight information.

In the scenario described above, individual subscriber may benefit by

1. becoming better informed about their own self (characteristics, preferences, behavioral tendencies, actual activities, etc).
2. being able to share such information either freely to selected parties or at a profit to parties who have demand for such insight information. Blockchain technology may be used as a way of giving the ownership of the data or the value originating from it back to subscribers or users, which is impossible in the centralized architecture that has been dominant in internet services for the past decades.

The telco service provider may benefit by

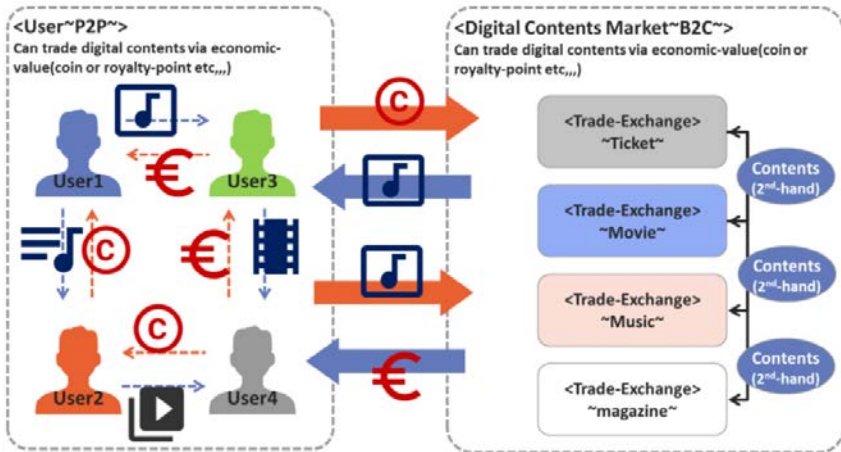
1. forming a new relationship with its subscriber where the subscriber may feel better served,
2. thereby expecting to compete more effectively against its competitors

3. directly drawing newer revenues from transaction fees charged to customers of insight information in the marketplace. The authorities may benefit by being ensured that telco service subscribers' data privacy and property rights may be upheld in more transparent and immutable ways than before.

Here is a description as to how a content distribution platform might work using blockchain technology:

- Create mechanisms for registering and providing unique IDs for content via a nonfungible tokens (NFTs) or other digital ID formats.

- Support other types of distributable/promotable property that can benefit from a trackable and incentivized distribution system.
- Create smart contracts that support transfer of ownership rights (all or partial) and for other rights including distribution, promotion, creation of derivative works and other traditional IP rights. (The NFTs will allow for tracking and usage attribution.)
- Create smart contracts that calculate the distribution of royalties and other revenues between content creators, owners, distributors, promoters, and others in the value chain.
- Support mechanisms to aggregate royalties and allow for payment via cryptocurrency and/or other acceptable currency forms.
- Provide credits to consumers for consuming and/or rewarding content along with ways for users to increase their credits.
- Create mechanisms for tracking implicit rewards (i.e., attention/views/responding to surveys) as well as explicit rewards (tips, bonuses, direct fees, etc.)



- Telcos can use existing cryptocurrencies and/or tokens as the digital currency that would be used in the system.
- Telcos can provide methods for content registration and authentication, rights transfer, usage payments along with payment distribution, reconciliation, and settlement.
- Digital content could be stored in telco-managed storage networks in a secure manner with copy protection.
- Ethereum and similar blockchain platforms that support tokens and smart contracts can be used for registering content via tokens along with recording transfers, usage, and other actions for that token within the system.
- Ethereum can provide smart contract which can be used to support a variety of intellectual property transactions including transfer, copy, limited counts of access, limited length of access, and many more.
- Ethereum by itself cannot guarantee the copy protection of the contents as it manages only the rights associated with the token when the content is associated with the token. Content could get separated from the token (by copying it directly from the user device and then introduced into the content stream as an unauthorized copy). Fingerprinting and content analysis could help reduce unauthorized content.

- Scalability will also likely be an issue although as with other use cases, improvements to the Ethereum mainnet as well as Layer 2 solutions shows promise in resolving this concern in the not too distant future.

5.1 Constructing Economic Incentives For B2b Service Partnerships in Telecom

Constructing economic incentive models is difficult. Crowding out of desirable behavior in different forms occurs due to economic incentives and enforcement of incentive rules requires a good understanding of the underlying population of participants. Whereas the latter is hard for large ecosystems, in a business setting, it is significantly simplified since there are incentives to do business with one another:

All parties have things other parties want and typically informal relationships for a majority of business relationships are long-lasting establishing a significant “trust” factor. However, this “trust” factor is only at the executive level of the pyramidal hierarchy and not at the operational level where it matters. This means that trust is formally only established at the legal contract level and not at the operational level, even within companies. This very fact leads to significant business goal misalignments amongst companies and even within companies.

Given the above, let us construct a simple, yet generally applicable incentive model that will meet our needs for the Service Provider and the Service Recipient:

1. Upon self-verified completion of a service task with a well-defined business outcome such as installing and activating a new receiver in a home, a service provider is paid $X\%$ of a previously agreed service fee $\$Z$ in real-time, with $X > 50\%$, or $< 50\%$ depending on the nature of the service and business relationship. No price discount is provided by the service provider to the service recipient for Net + 0 payment terms. $Y\%$ of the service fee such that $X\% + Y\% = 100\%$ is put into an escrow function to account for a period of A days, where A days represents a normal payment period such as 30 days, or 90 days. After the A day period is passed, the escrowed amount is paid out to the service provider through a token to fiat exchange function. The percentage Y of the service is called the economic stake of the service provider and the percentage X is the stake of the service recipient .

2. The service recipient receives the completion of the service task in the agreed-upon KPIs such as MTTR, Complaint Rate, etc. and agrees to the above payment terms. In addition, as we will see below, we need the function of a Business Outcome Validator or Auditor. Auditors function as independent validators of business outcomes. The Auditor population should be large and anonymous, or at least pseudonymous, to the business ecosystem participant. The use of auditors can be triggered by a variety of business conditions related to the state of a business outcome. However, in a service scenario, they will be used either if a complaint about a service task has been filed or a completed service task is audited as part of a service provider agreement.

Similar incentive rules that are applicable to a service provider and a recipient are also applicable to the Auditor:

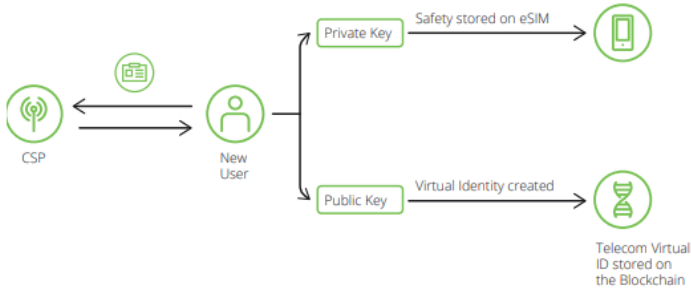
1. The Auditor will be compensated for their service through a token reward. The size of the reward depends on the value-at-risk; however, should be significant enough to incentivize participation, e.g. one could either make a living off this service or significantly supplement an already existing income source. There are two available options to realize this:
 - a) Service recipient and provider contribute in equal parts tokens that are tied to fiat currency to an escrow function. In this case, it is recommended that both parties provide a percentage of the annual value of a service contract.
 - b) Each time an auditor is rewarded, the token reward is “minted” by the platform. We will discuss what we mean by the platform when we talk about implementations.
2. For Auditors to have “skin in the game”, they will have to escrow a token stake that is significant enough, on the one hand, to deter malicious behavior by the auditor, on the other hand, low enough that it does not deter participation. There will be several instances, see the next section, where Auditors will have to escrow a token stake to economically participate in the business ecosystem. Care must be taken such that the rewards and stakes/penalties of the incentive system are set in such a way that they do not incentivize the wrong behavior as happened in the case of Staples. This will require some

experimentation through pilot studies to find the right configuration of the above model before applying such an incentive model more broadly in a business ecosystem.

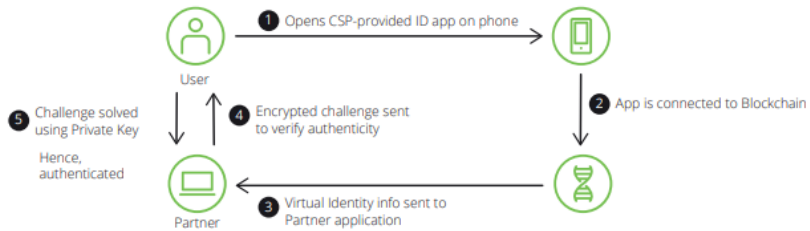
Economic & Customer Experience Benefits: We have constructed an incentive model and consensus algorithm, that aligns business goals of B2B service partnerships in the Telecom industry around specific business outcomes that are independently verifiable in a tamper-proof and collusion resistant manner. We believe this model to be a significant improvement for the Telecom industry to achieve significantly higher quality service outcomes at lower costs than before.

Security Benefits: We have performed a game-theoretic security analysis of the economically incentivized consensus model and shown this model to be a highly secure process. In addition, we discussed platform security in the same game-theoretic analysis framework. Lastly, we gave implementation considerations in terms of high-level requirements to implement the model on a permissioned Blockchain platform with economically incentivized consensus and capable of support business logic through smart contracts.

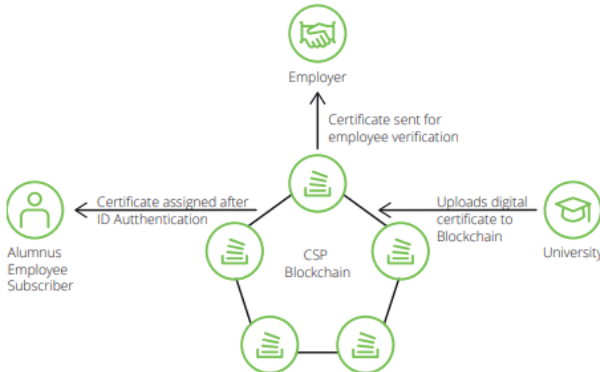
Blockchain And Cloud Computing In Engineering Application



ID Authentication

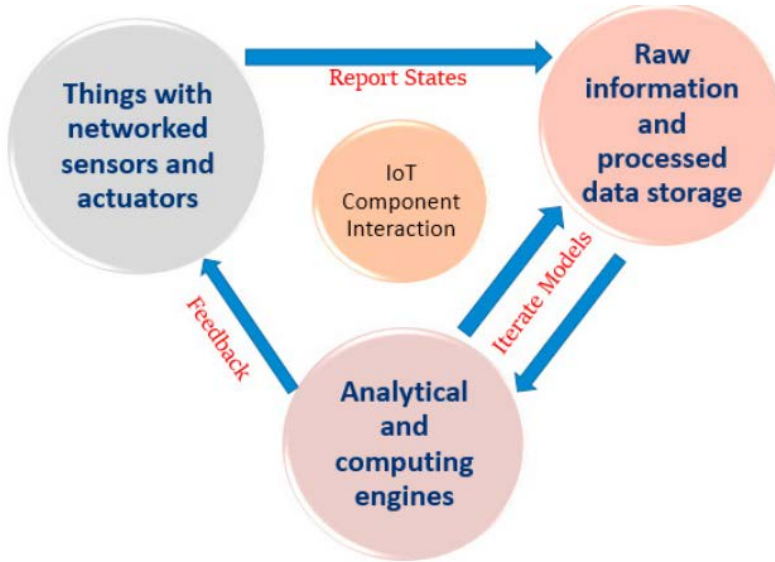


Data Management

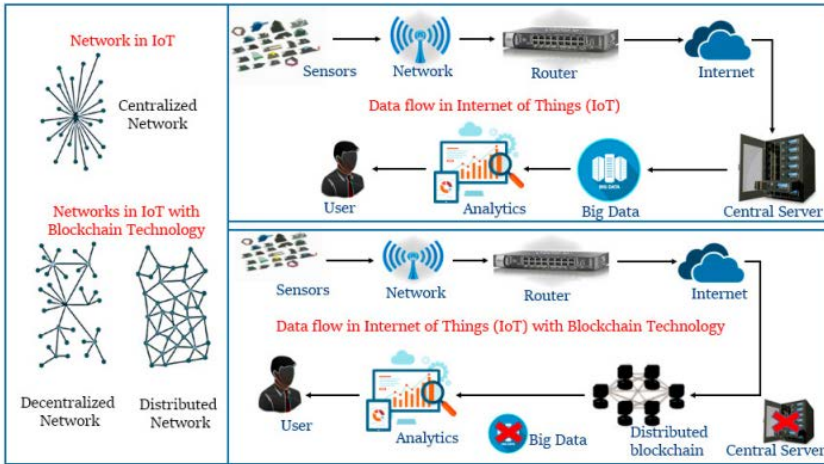


- **Regulatory Benefits:** The economic benefits and improved customer experience, in turn, will likely ease regulatory burdens currently in place due to the systemic quality issues in the industry.
- DID's are pseudonymous not fully anonymous. However, as long as no PII is used in the above use case and no mnemonics are derived from PII, the privacy of individuals and institutions data is guaranteed.
- Security is based on standard cryptography for encryption and authorization protocols such as OAUTH or DID-AUTH.

1. Platform: In order to ensure tamper and collusion resistance, a Blockchain stack that allows for business logic execution through smart contracts and has an economically incentivized consensus algorithm with a mathematical proof of security. We recommend a Proof-of-Stake consensus algorithm since the platform nodes should be permissioned, in contrast to for example Bitcoin or Ethereum, through the platform itself should be open.



2. Digital Identity: We recommend integrating a proven Decentralized Digital Identity Provider such as uPort, Sovrin, Blockstack or Microsoft for to provision platform identity and, in order to reduce complexity, leverage the Decentralized Identity Foundation's Identity Hub reference implementations¹⁰ for identity integration. To reduce the platform failure points, we recommend a decentralized access control system by leveraging the aforementioned identity systems as an access control layer.
3. Incentive Model: The incentive model can be created through a smart contract system built upon a Blockchain stack that allows one to freely define tokens and their value based on the business needs and easily build any desired business logic.

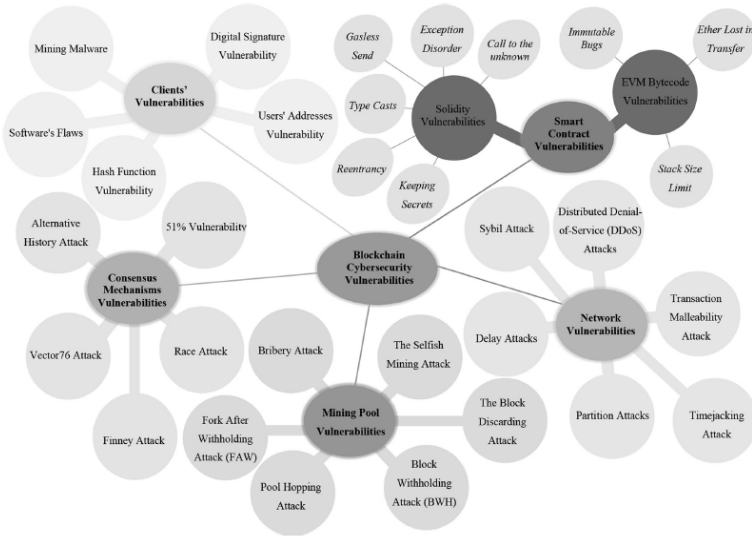


4. Consensus Model: The consensus model can be created through a smart contract system built upon a Blockchain stack that allows one to freely define consensus rules and easily build any desired business logic. The model can leverage the provided digital identity system integration to enable unique identification of participants.
5. Exchange Facility: Since we are dealing with economic value, there needs to be an exchange facility built using smart contracts that allows one to exchange tokens to fiat currencies and vice versa leveraging escrow accounts at banks that require a multi-signature approach to unlock funds related to platform token stakes. This facility needs to be defined and controlled by the platform governance body and should best be run by a 3rd party such as a bank.

We classify BT threats and vulnerabilities into the following five categories:

1. Client's vulnerabilities
2. Consensus mechanism vulnerabilities
3. Mining pool vulnerabilities
4. Network vulnerabilities
5. Smart contract vulnerabilities

Each of the threat and vulnerability types is discussed in the following sections.



5.2 Clients Vulnerability:

All BTCs' asymmetric cryptography is based on elliptic curve cryptography (ECC). The addresses in BTC are derived from public keys of ECC, and the authentication of the transaction uses digital signatures, which are generated by the ECDSA. The use of ECC is inadequate, because it does not have the requisite randomness, which might compromise the user's private key. A random value must be used with the private key to create a digital signature, where the random value must be different for each transaction. For example, in BTC blockchain, 158 unique public keys were found, which used the same random value (nonce) in more than one signature, which made it possible to compromise the users' private keys.

The operation in some of the blockchain networks, such as BTC blockchain, relies on cryptographic primitives to ensure the correctness and accuracy of the operation. With the rapid development in the computational power and advanced cryptanalysis, these primitives have become breakable. One of these primitives is the hash function. For example, SHA256 is the hash function used in BTC blockchain, which is vulnerable to different cybersecurity threats, such as preimage and collision attacks. A preimage attack is when the attacker is given an output Y from hashing an input m ; the attacker attempts to find an input m^* so that

hashing m^* equals Y ; however, the attacker's attempt to find two inputs providing the same hash is considered a collision attack.

The potential impact of performing the preimage attack on BTC blockchain might lead to uncovering an address or the complete failure of the blockchain, while the impact of the collision attack might be stolen to destroy coins or repudiate payment.

Although enormous computation power is needed to perform such attacks, attacks might be possible if the adversary has quantum computing or dominates a huge mining pool.

Cryptojacking is when the adversary installs the malware on the target machine or mobile device to utilize its computational power to mine a block, which consumes a large amount of electricity and might compromise the target's system functionality. In February 2018 alone, researchers launched a cryptojacking campaign, which affected more than 4000 websites, including the UK and US government pages; the other campaign targeted millions of Android devices. Author proposed a deep-learning image-based analysis for malware detection. In addition, a critical infrastructure security company found cryptocurrency mining malware on the European water utility operational network, which had a huge impact on the systems.

There are different types of flaws in blockchain users' software, such as runtime, concurrency, and hard fork flaws . Flaws in the blockchain users' software, which is used in the blockchain network, might lead to the exposure of users' private keys. In 2014, Blockchain.info, which is a hybrid wallet provider, made a mistake during their software update in that when their users generated a new key pair on their local computer by using the affected software, the ECDSA inputs were not adequately random, which meant that an adversary could operate the software to compromise the users' private keys by only viewing the public address .

Addresses in BTC blockchain are vulnerable to identity theft threat because these addresses are not certified. For instance, a man-in-the-middle attack might be performed by an adversary to change the target BTC address to the adversary address. The adversary might vandalize the target website to obtain payments destined for the target. The impact of the attack is disastrous, because, in the BTC blockchain, it is impossible to return the payment if the nodes in the network accept and register it in the ledger.

5.3 Consensus Mechanisms Vulnerabilities:

Establishing mutual trust in BT is based on the shared consensus mechanism. However, the attackers might control the whole blockchain network by exploiting the 51% vulnerability, which is built in the mechanism. For example, if a single user or a group of users have more than 50% of the total hashing power in the blockchain networks, which are based on the PoW mechanism, then the user or the group of users can exploit the 51% vulnerability. Therefore, gathering the mining power under a few mining pools might lead to this issue. Recently, GHash.io alone dominated 54% of all BTC network processing power for a day . In addition, the blockchain networks, which are based on the PoS mechanism, also have the 51% vulnerability.

The vulnerability can be exploited when a single miner has more than 50% of the total coins in the network; a 51% vulnerability leads to a 51% attack, which allows the attacker to do the following :

1. Injecting deceptive transactions
2. Manipulating the blockchain network
3. Outstripping all other users in the blockchain network
4. Performing a double-spending fund
5. Stealing other users' assets

Alternative History Attack:

In this attack, the attacker sends a payment transaction to the target while he or she mines another blockchain fork, which includes a deceptive double-spending transaction. After the confirmation, a product or service will be received by the attacker from the target. If the attacker succeeds in

finding more blocks than the genuine chain, he or she propagates his or her malicious fork and recovers the coins; otherwise, he or she must extend his or her malicious fork to reach the fork of the honest miners. If the attacker cannot catch up with the other nodes, the attack will fail.

Finney Attack:

In this attack, one transaction is pre-mined in a block, and a duplicated version of this transaction is sent to a user by the attacker. After the transaction is accepted and the receiver delivers the product, the attacker propagates the block, which contains the initial transaction. Thus, the transaction, which is sent to the user, will be invalid, and the attacker will succeed in producing a double-spend transaction.

Race Attack:

This attack is easy to launch in blockchain networks, which are based on the PoW mechanism; this is mainly because an attacker can exploit the time between the creation transaction and the confirmation transaction to carry out the attack. Before mining the confirmation transaction, the attacker has obtained the creation transaction results, which leads to double spending.

Vector 76 Attack:

This attack originally came from the BitcoinTalk forums, where a user named Vector76 described an attack against the MyBitcoin e-wallet, which resulted in double-spending issues. In this attack, the attacker does not need to mine two consecutive blocks; one block is sufficient to perform this attack. The attacker needs to observe the blockchain network to determine the timing of the propagating transactions of network nodes and how they are broadcasting over the network. The attacker then identifies the nodes that are earlier in the propagating transactions than the target and sets up a direct connection with the target. After that, the attacker initiates a transaction that makes a legitimate deposit into the target and mines it into a block, without broadcasting it to the network. The attacker mines the block like other nodes, except that he or she adds an extra transaction that is not broadcast. When the attacker succeeds in initiating a valid block, he or she does not broadcast it until some other nodes mine a block.

Once a node mines a block, the attacker immediately broadcasts his or her block to the target, and if the target receives the attacker block before the other block, the target will accept the attacker block, and the transaction will gain one confirmation. In this situation, the blockchain and the target and other nodes connected to the target will be forked mainly because the target that passed on the transaction quickly will consider the attacker block legitimate, whereas the other nodes in the network will consider the other fork valid. The attacker directly transfers the coins to a different address that is controlled by the attacker, and the target will generate the transaction because the target believes that it is a legitimate transaction.

The attacker also double spends the inputs by transferring the coin to himself or herself. The network nodes that did not receive the attacker's first block will accept the transaction as a genuine transaction, and they will include it in the next block. If the attacker's first block wins when the blockchain has forked, the attacker will not lose anything; however, if the first block loses, then the deposit to the target will become invalid, although the withdraw transaction will still be valid.

1.4 Mining Pool Vulnerabilities:

Block withholding Attack:

In this attack, the attacker joins a mining pool to assist the pool members in mining blocks; however, the attacker will never broadcast any block to decline the pool anticipated income. This attack is also called a 'Sabotage Attack' because the scoundrel miner does not obtain anything but causes everyone to lose. Although the attacker does not gain any revenue from this attack, assert that the attacker might be able to earn income from this attack.

Bribery Attack:

This attack is based on bribing miners to mine on precise forks or blocks. The attacker can validate random transactions and publish them because he or she has paid to dishonest nodes to verify them. The attacker might gain the majority of the computing resources by using three ways of bribing, namely out-of-band payment, negative-fee mining pool, and in-band payment. In the out-of-band payment, the computing resources owner is directly paid by the attacker to mine the attacker's blocks. In the

negative-fee mining pool, the attacker creates a pool by rewarding the higher return. Finally, in in-band payment, the attacker pursues to bribe the blockchain itself by making a fork, which includes free bribe money to any miner endorsing the attacker fork.

Pool Hopping Attack:

In this attack, the attacker mines based on the appeal rate. If the rate is high, the attacker mines; otherwise, the attacker leaves the pool. The attacker utilizes the information about the number of the submitted shares in the target mining pool to understand how many shares have been submitted and how many blocks have been found. Using this information, the attacker stops mining in the target pool and contributes elsewhere. The central idea behind this attack is that the attacker chooses various pools to mine to gain maximum income.

Block Discarding Attack:

In this attack, compared with the honest nodes, the attacker must possess an adequate number of network connections and dominate multiple slave nodes to increase his or her network superiority. Once the attacker is informed of newly mined blocks, he or she immediately publishes his or her own block, which must be faster than the rest in the network; therefore, when a node publishes a block, the attacker can instantly propagate his or her own blocks to discard honest nodes' blocks.

Selfish Mining Attack:

In this attack, a group of attackers conspire to create a mining pool to negate the honest miners' work and acquire better income for themselves. The attackers mine in their private blockchain and broadcast it based on the length difference between the public and the private blockchains to influence the rewards.

Fork After Withholding Attack:

The fork-after-withholding (FAW) attack income is equal or greater than a block withholding (BWH) attack income, and the attack is four times more fruitful, usually per poll, than the BWH attack. This attack has two types: single-pool FAW attack and multipool FAW attack. This attack combines the selfish mining attack and the BWH attack. In the single-pool

FAW attack, the attacker joins the target mining pool and performs the attack against it, whereas, in the multipool FAW attack, the attacker aims to increase his or her income by expanding the attack against several pools. The attacker computing power is divided in this attack into infiltration mining and innocent mining. When the attacker infiltration part locates a full PoW, the attacker keeps the block and does not broadcast it. Based on the next steps, the attacker might publish his or her private block to the manager of the target pool, hoping that a fork is created identical to the selfish mining attack or the attacker discards the block, which is identical to the BWH attack

5.5 Network Vulnerabilities:

Partition Attacks:

In this attack, the attacker isolates a group of nodes from the rest of the BTC blockchain network, and the network is partitioned into disjoint components. The adversary hijacks the most specific prefixes, which host each of the isolated nodes' IP address to redirect the traffic destined to them. The traffic is intercepted by the adversary when he or she is on the path and determines which connections cross the partition that the adversary attempts to create. If the connection does not cross the partition, the adversary drops the packets; otherwise, the connection is contained within the isolated nodes. The adversary tracks the exchanged messages to determine the leakage points; these are nodes in the isolated group, which maintain connections with the external nodes and the adversary cannot intercept. The adversary finally isolates the leakage points from other nodes in the isolated group.

Delay Attacks:

In the previous attack, the adversary needed to gain full control over the target's traffic to perform the attack effectively. In contrast, the delay attack can cause significant delays in block publishing even when the adversary intercepts only one of the target's connections. First, the attacker alters the content of specific messages to delay the block delivery; this is achievable because of a lack of integrity checks and encryption of BTC messages. In addition, the adversary makes use of the fact that nodes first send block requests to the peer that propagated each block and wait for 20

minutes to deliver it before requesting it from another peer. Thus, the adversary delivers a block to a target node by a 20-minute interval, which makes the target unaware of the most recently mined blocks and makes the target unable to contribute to the network.

Distributed denial of service Attacks:

Nowadays, the distributed denial-of-service (DDoS) attack is one of the most common and inexpensive attacks on the Internet . Despite being a peer-to-peer technology, BT is still vulnerable to the DDoS attack. The BT networks, such as Ethereum and Bitcoin, have frequently undergone these attacks. For instance, 40 BTC services have suffered from 142 DDoS attacks over 2 years, and the targets have included 7% of all popular operators . Most of these attacks targeted large mining pools and currency exchange services because of a larger revenue possibility. These attacks have forced firms such as BitQuick and CoinWallet to shut down their service after a few months of their start

Sybil Attacks:

In this attack, the adversary sets up fake assistant nodes and attempts to expose part of the blockchain network. The adversary might use a group of exposed nodes to perform the attack to isolate the target and disconnect the transactions created by the target, or the attacker will make the user choose only the blocks that are maintained by him or her . The adversary with malicious nodes will surround the target. The target will think that he or she still connects to the network through different honest nodes; however, the reality is that the target has a limited access to the network because the adversary controls all the nodes to which he or she connects. Once the adversary surrounds the target, he or she can refuse to relay the target's transactions. Besides, the adversary can feed misleading information to the target of the network state . A successful Sybil attack can incapacitate the consensus algorithm functionality and cause potential double-spending attack .

Time Jacking Attack:

This attack is a specific attack on the BTC blockchain network. The network time in this network is maintained by full nodes. The network time is acquired by obtaining a version message from the neighboring

nodes. The median is calculated, and if the median time of all neighboring nodes exceeds 70 minutes, the network time counter returns to the node system time by default. When the adversary is connecting to the target node, he or she attempts to reveal imprecise timestamps. Once the adversary modifies the node network time counter, the misled node might adopt a substitute blockchain. This attack will isolate the target node from the network or decrease the transaction confirmation rate on the whole network.

Transaction Malleability Attack:

Transaction malleability is a vulnerability in the BTC blockchain network that enables the adversary to alter the TXID without revoking the transaction. Modifying the TXID will deceive the victim into believing that the transaction has failed, although it is later confirmed. Currency exchanges are the common targets for this attack. The adversary withdraws from an exchange and then republishes the same transaction with a different TXID, and one of them will show on the network. Because of delays, it is highly probable that the altered transaction will win rather than the original withdrawal. The currency exchange will not locate the original transaction on the network and will think that the transaction has failed if the exchange relies on TXIDs only. Thus, the adversary can continuously withdraw. Mt. Gox was one of the largest exchanges in BTC history; it declared bankruptcy due to losing coins valued over US\$450 million. The attackers performed a transaction malleability attack to steal coins from the exchange, which forced the exchange to freeze users' account and halt withdrawals.

5.5 Smart Contract Vulnerabilities:

Two of the major vulnerabilities of Ethereum are discussed in the following subsections.

Ethereum Virtual Machine Vulnerability:

The ethereum virtual machine (EVM) is a virtual machine that runs the bytecode, which is the result of compiling the source code of a smart contract. Each operation in the EVM expends a specific amount of gas. The gas represents the code execution cost.

Solidity Vulnerabilities:

Solidity is the smart contract high-level programming language in Ethereum, which the programmer uses to write the smart contract source code. There are six known vulnerability types in the smart contract source codes that are already exploited and represent the highest portion of the smart contracts' vulnerabilities number. Most of these vulnerabilities emanate from a misalignment between the programmers' insight and the Solidity semantics.

Ethereum Smart Contract Coding flaw represents the third-highest impact of the incident type. The main cause is due to the reentrancy vulnerability in smart contracts, as shown in the case of the DAO incident in 2016. Reentrancy is a kind of vulnerability exhibited in Ethereum Smart Contract only. As the name suggests, an attacker first deposits an amount X to a multiparty smart contract. The attacker then executes a function to withdraw an amount Y , which is more than X , before the balance of funds deposited and withdrawn has been settled. The effect is the attacker essentially stealing the money of other parties in the contract. Our study reveals that incidents related to Ethereum Smart Contract flaw have risen from being one incident in 2016 to two incidents in 2017 to four incidents in 2018.



PART – 2
CLOUD COMPUTING IN
ENGINEERING APPLICATION

CHAPTER - 6

Introduction To Cloud Computing

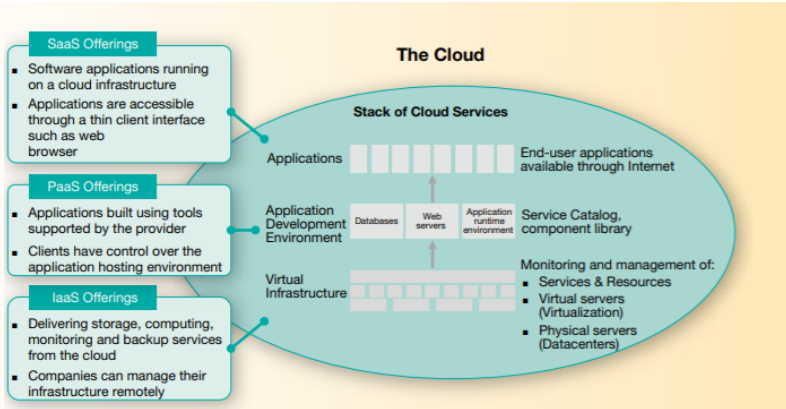
Cloud Computing has its roots in Grid Computing and Utility Computing. Grid Computing has been playing a vital role in scientific research. Scientists work on scientific applications using High-Performance super-computers employing parallel processing. Virtualization started at the OS-level, using mainframe logical partitions for multitasking. After this, companies were able to provide shared computing capacities to multiple processes with different configurations on the same systems. Later, companies like Amazon introduced virtualization in commodity computers, in order to provide services over the internet. As the internet data-transfer speed increased, it was visualized that these computing capacities can be provisioned at a larger scale through the internet. IT companies saw promise and opportunity in this internet-enabled compute utility model.

So, cloud computing started its maturity journey for IT enterprise, and the SPI (SaaS, PaaS, IaaS) model was born. End-users were able to consume services using software-as-a-service, developers were able to develop code and applications in the cloud using platform-as-a-service, and SMBs (Small and Medium Businesses) were able to rent computing capacities, storage and networking, from the cloud provider, using infrastructure-as-a-service. This created a boom in the IT sector service-provisioning and business-agility, leading to a growth in the cloud services market. Telecom companies follow this new provisioning model, and started developing solutions from/for the cloud. Cloud computing has become a revolutionary concept in IT and Telecom, reshaping the business models, service offerings, and hardware/software provisioning, thereby unleashing new revenue generating services.

Cloud computing has become one of the highly used terms in the industry by companies, developers, and the end users. There is an immense research going on cloud computing in the industry and academia. Many companies, from SMBs (Small and Medium Businesses) to large, are shifting towards cloud implementations of their on-premises systems. These companies are required to think of multiple aspects of a cloud like application design [4], cloud-provider maturity, security, dimensioning, scalability etc. Testing their systems in the cloud requires a clean relocation of their current applications to the cloud. Cloud computing has multiple facets when it comes to industry segmentation.

For example for mobile applications, mobile clouds are being developed, and to cater for security private clouds are being developed. The telecom sector questions if the maturity of the cloud can be used for telecom application delivery. Nowadays we are witnessing a shift of telecom service providers and vendors to the cloud. We have researched and analyzed these trends, telecom sector concerns, cloud options for specific telecom product, and ways to deal with the migration problems.

In recent years, the increasing costs of setting up and maintaining IT infrastructure have been a cause for concern for enterprise CIOs . Cloud computing provides businesses with a cost efficient and elastic solution for offloading maintenance, freeing up budget, and improving IT productivity and responsiveness. The rising interest in cloud computing has resulted in several telcos entering this space. Although operators have been late entrants, they have established a strong presence by leveraging their in-place assets and focusing aggressively in this market. The primary focus of telcos has been on IaaS2 , even if many also provide significant SaaS3 applications. However, PaaS4 has been largely neglected by most operators. Our analysis indicates that cloud computing presents several attractive commercial opportunities for telcos which should be tapped in a phased manner, without delay, in order to maximize returns.



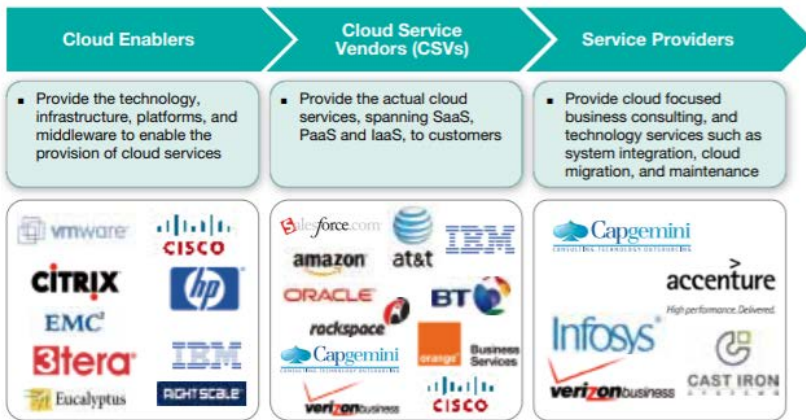
Although the IaaS proposition would be most fruitful for operators, other opportunities across SaaS, service delivery innovation, and PaaS will also offer significant potential. We recommend that telcos differentiate themselves by offering niche services which require industry and region-specific customization. For example, a strong focus on specific industry verticals such as finance and healthcare will help them gain an edge over the competition. In terms of service delivery, telcos are best equipped to adopt virtual private cloud deployments and broker approach .

Customized offerings for large enterprises and SMEs will further strengthen their position and enable them to become frontrunners in cloud computing. Cloud computing is the latest technology trend in which IT infrastructure and software programs are accessed over the Internet or private networks. Cloud offerings can be largely categorized as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) . These services are delivered via three main models: public cloud , private cloud, and hybrid cloud . Enterprises of all sizes are being increasingly drawn to cloud computing. Benefits such as reduced IT costs, pay-per-use, better resource utilization, and elastic scalability are driving its uptake. The percentage of CIOs interested in cloud computing has grown rapidly from 5% in 2009 to 37% in early 2010.

Interest in these services is driving increased enterprise spending, and as a result, cloud computing presents an attractive revenue potential for technology players and telcos alike. While the benefits of cloud computing make it attractive for customers, concerns such as data security, privacy, and compliance have slowed down the pace of adoption. For instance,

strict privacy laws that place limits on the movement of information beyond the borders of the European Union, have hindered the evolution of cloud computing in Europe.

After carefully weighing the benefits and risks of cloud computing, several operators have advanced into this lucrative market. However, the key challenge ahead for these operators is to differentiate themselves in this highly competitive arena. In this chapter, we take a close look at the cloud computing space, qualify the opportunity for telcos, and propose some recommendations around how operators can maximize the opportunity in this market.



Several companies are competing aggressively to grab the largest share of the lucrative cloud computing market. These players fall largely under one of these three categories: enablers, vendors, or service providers. The role of some mature players, however, can also span a number of categories. For instance, both Cisco and IBM are cloud enablers as well as CSVs. Leading technology vendors such as Amazon, Salesforce.com and Microsoft have established a firm footing in this market and offer a range of services spanning SaaS, PaaS, and IaaS.

In terms of revenues, the current CSV landscape is dominated by players such as Salesforce.com, Amazon, and Oracle. Salesforce.com, the leading provider of SaaS CRM solutions, reported revenues of over US\$1billion in 2009, which is the highest amongst CSVs. The success of these leaders can be attributed to their technical prowess, early mover advantage, and the strong focus on cloud computing. Though large technology players

have emerged as leaders in cloud computing, several smaller companies such as Rackspace and Netsuite are trying to carve their niche. Telcos such as BT and AT&T have also entered this market. In the next section, we will evaluate the cloud computing initiatives and strategies of telcos.

	2003-2004	2007-2008	2009-2010	Planned
SaaS	BT Open Orchard T-Systems Dynamic Services	Telstra T-Suite Orange IT Plan	NTT Biz Security Telefónica Aplicateca TeliaSonera Business Class Cloud Services	
PaaS		T-Systems (Database and Middleware Environments)	SK Telecom Cloud Computing Platform	AT&T Telstra
IaaS		AT&T Synaptic Hosting Deutsche Telekom Zimory*	Orange Flexible Computing BT Virtual Data Center	Verizon Computing as a Service AT&T Synaptic Storage and Compute Telecom Italia NTT

Compared to market leaders such as Amazon and Salesforce.com, telco entry into cloud computing has been reasonably late. While Salesforce.com started offering services in 1999, BT and T-Systems, one of the earliest telcos to offer cloud solutions, entered only in the 2003 to 2004 timeframe . Despite the late start, several telcos such as BT, AT&T, and Verizon are competing aggressively with market leaders to establish a strong foothold. The majority of operators have taken the role of a CSV while a few such as Verizon also act as service providers. This section presents an overview of key telco strategies in cloud computing.

The cloud computing offerings of most telcos are targeted towards the enterprise segment. Enterprises and governments spend nearly US\$2.4 trillion worldwide¹⁵ on IT products and services, many of which can be delivered from the cloud. This high revenue potential makes the segment attractive for operators. Moreover, the consumer cloud space and the revenue opportunities limited. Within the enterprise segment telcos are aggressively targeting SMEs due to the growing interest in this segment for cloud-delivered software. SME share in overall cloud services revenue is expected to increase from 25% to 40% between 2009 and 2015¹⁶ . To benefit from this opportunity, several telcos offer services customized to

fulfill SME needs. For instance, “IT Plan” from Orange is a packaged SaaS solution offering a suite of office productivity, messaging, and business applications targeted at SMEs.

Telco offerings in cloud computing are centered around IaaS and SaaS with limited focus on PaaS. IaaS is the flagship offering of most operators, and in general SaaS has taken a backseat compared to IaaS primarily because telco capabilities and experiences are more aligned towards delivering IaaS. the mainstay of SaaS offerings from leading operators.

Telcos have traditionally stayed away from PaaS, largely due to its unattractiveness both in terms of revenue and demand, when compared to IaaS and SaaS. Apart from T-Systems, which offers database and middleware environment to nearly 19 customers, few operators have shown significant interest in this category. In addition to SaaS, PaaS, and IaaS some telcos such as Verizon, Orange and BT also offer professional services, helping customers identify and migrate the right applications to the cloud.

Examples	Software (SaaS)	Application Development Platform (PaaS)	Infrastructure as a Service (IaaS)	
			Servers	Storage
Oracle on Demand	✓	x	x	x
Cisco Webex	✓	x	x	x
Salesforce CRM	✓	x	x	x
IBM Lotus Live	✓	x	x	x
Salesforce Force.com	x	✓	x	x
Google App Engine	x	✓	✓	✓
Microsoft Azure	x	✓	✓	✓
Amazon Web Services	x	x	✓	✓
BT	✓	x	✓	✓
Orange Business Services	✓	x	✓	✓
AT&T	✓	x	✓	✓
GoGrid	x	x	✓	✓
Rackspace	x	x	✓	✓
EMC MozyEnterprise	x	x	x	✓
Nirvanix CloudNAS	x	x	x	✓

Partnership with technology players has been the foremost entry strategy of telcos in cloud computing. Operators have partnered with a range of vendors from hardware providers such as HP and Sun to virtualization specialists such as VMware and Citrix Systems. These partnerships have helped telcos significantly reduce their time-to market and minimize the risks associated with developing complex technical capabilities in-house. In addition to partnerships, a few operators have acquired technology companies to leverage their expertise to launch cloud services. For

instance, AT&T acquired leading application services provider US Internetworking (USi) in 2006 for US\$300 million to develop capabilities in delivering on-demand services and managed enterprise software solutions. Similarly, telcos such as BT, Verizon and T-Systems also acquired companies to develop expertise in launching certain cloud services.



CHAPTER – 7

Cloud Computing In Service Providers

Cloud providers are using Internet Protocol (IP) infrastructure where IP protocols are used for communication services. For storage and processing, cloud providers are using multiple environments to have a dynamic approach for storage and processing. Distributed databases with encryption capabilities, and highly scalable storage techniques are being used in the cloud .

All the major cloud providers are constantly increasing their infrastructure capabilities to make their infrastructure attractive for enterprises. For example, the provision of networking-as-a-service in Amazon’s Virtual Private Cloud (VPC) provisioning is a new step which will help enterprises become confident in handling their important data in the cloud.

Currently, the main task of the operators and telecom enterprises is the transformation of the next generation datacenter into the cloud . This task entails that the benefits of Cloud Internet Data Center (IDC) should be a subset of the benefits provided by their local datacenter. So the technologies used in local datacenter must be in sync with the cloud provider’s data center solution.

7.1 Virtualisation:

Cloud providers have managed to provide many levels of virtualization in their networks. For example, OS virtualization, kernel-level virtualization, files system Virtualization, and, Network or I/O virtualization. This enhanced aspect means that many types of network and software configurations/architectures can be ported to the virtualized world.

Amazon AWS has gone far in this and provides both partially virtualized and fully virtualized systems. Root access to virtual machines and ability

to let networking play its part in VM-to-VM communication means many types of applications can be ported to the Amazon Cloud. But does this mean that we need not change the application architecture in order to deploy it in Amazon Cloud.

The ability to scale out while maintaining the desired level of service is visualized through the help of load balancing. Load balancing provides availability to services within single or multi-cloud environments. They distribute the load among redundant servers based on the traffic load. On the other hand, scalability can be seen in two ways. To scale up/down means that server can be up-graded/down-graded with RAM, storage, networking capabilities, and processing power. On the other hand, scale out/in means that servers can be added or deleted from the server pool.

7.2 Virtual Private Cloud Provisioning(Vpc) Provisioning:

Many cloud providers have included the provisioning of VPC in their offerings. This was the requirement of bigger enterprises which demand IPsec enabled VPN connections to the cloud, and power over the networking capabilities. They can get a pool of IP addresses, assign their own DNS servers, maintain Access Control Lists (ACL) lists, fully control their cloud network topology, creating rules for outbound and inbound traffic, provisioning of internet gateway inside cloud to segregate traffic between multiple office localities, and having NAT in their control. These things are provided in Amazon VPC offerings too. One thing that cannot be done is the connection to VPC using an IPv6 address.

Switching technology in traditional datacenter is normally gigabit. This concern has been addressed by the cloud providers, and provisioning of high bandwidth gigabit interfaces is in place. But the full power on creating one's own virtual interfaces and thus Virtual Local Area Network (VLAN) is not supported in many clouds.

To be able to create multiple users, permissions, access domains, departmental segregation, and identity management, cloud providers have gone through provisioning of giving a separate layer to these functionalities. Since cloud can be deployed with different market segments in mind (SaaS, PaaS, IaaS etc), it is important to manage identity and access requirements on customers, and in-house staff.

Apart from on-demand computing, high performance computing is one of the most important benefits of cloud. A myriad of applications with high computing demands, such as scientific applications, can benefit from this area. Large scale experiments from high end IT processes to physics-based research can be carried out if a sufficient amount of computing resource is available, especially the one based on distributed and grid computing.

A great study has been conducted on how Aneka, an enterprise cloud computing solution, addressed scientific computing in the cloud using classification of gene expression data and the execution of fMRI (functional Magnetic Resonance Imaging) brain imaging workflow.

7.3 Cloud Vendors And Platforms:

Hoff's along with some industry experts on cloud computing in 2009 put forth a very comprehensive model of cloud computing . This model defines partitioning of the cloud into sub-areas e.g. presentation layer, APIs, applications, data, metadata, content, middleware, hardware etc.

Public cloud Service Providers:

Microsoft Azure:

Microsoft Azure provides a service on which developers can deploy their applications without worrying about the technicalities of underlying infrastructure. The environment provided by Azure is best for .NET application, and is a good option too if someone wants to deploy applications with mixed environments. Microsoft provides compute, storage, virtual network, and certain services which are specifically designed for developers . The Azure is built on Midori, which comprises of object-oriented distributed operating system.

Google App Engine:

If someone is developing applications in the Java, PHP, or Python then Google App Engine is a very good option. It is a Platform-as-a-Service provisioning, and you only have to worry about your own application and you are not concerned about the underlying infrastructure, load balancing, and scalability. It also provides Task Queue, XMPP, and Prospective Search mechanisms, in its APIs.

Cloud Name	Market Segment	Cloud Type *	Cloud Name	Market Segment	Cloud Type *
AWS	IaaS	Pu, vPr	ElasticHosts	IaaS	Pu
Microsoft Azure	PaaS, ITaaS, IaaS	Pu, Pr, vPr, Hy	Opsource Enterprise Cloud Hosting	IaaS	Pu
Google App Engine	PaaS, SaaS	Pu	JoyentCloud	IaaS, PaaS	Pu, Pr
IBMSmartCloud Enterprise	IaaS	Pu, Hy	Linode	IaaS	Pu
GoGrid	IaaS	Pu	Salesforce	SaaS, PaaS	Pu
Rackspace	IaaS	Pu, Pr	Skytap	IaaS, PaaS	Pu
Verizon Terremark vCloud Express & Enterprise Cloud	IaaS	Pu, Pr, Hy	Bluelock	IaaS	Pu
Colt	IaaS	Pu			

*Pu = Public, Pr = Private, Hy = Hybrid, vPr = virtual Private

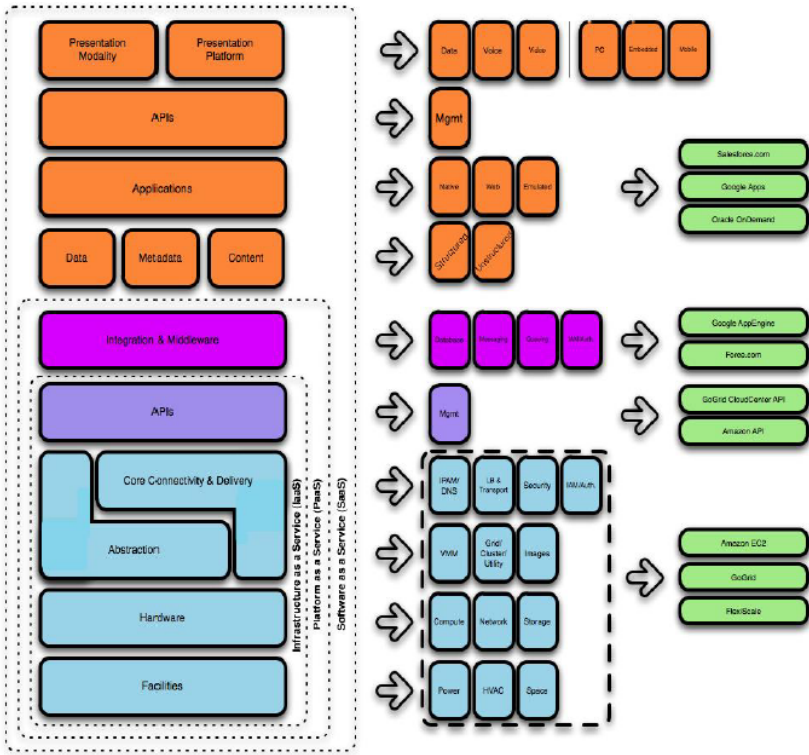
Many powerful cloud vendors provide different types of cloud platforms which can be built inside enterprise data centers to leverage the benefits of virtualization. These run inside corporate firewalls. The other variant of Enterprise Clouds are those that run in public infrastructure but they specifically introduce enterprise related dependencies in the cloud e.g. high redundancy and enterprise-class latency.

IBM Smartcloud:

IBM, with its IBM SmartCloud platform provides very solid private cloud functionality for enterprises to build upon. HP also provides cloud services to the enterprises and its latest move to provisioning of IaaS is another move towards enterprise development. IBM has partnered with Redhat, SOASTA, and RightScale.

HP,CA,Oracle and Others:

HP partnered with Microsoft, and Oracle partnered with AWS, to develop enterprise cloud solutions. CA technologies' AppLogic solution helps enterprises build cloud solutions using an intuitive graphical user interface (GUI). On the security level, UniSys Stealth Security Solution provides data protection technology. Other major players in the arena are Rackspace, GoGrid, Joyent, AT&T, EngineYard, NetSuite, Intuit, Intacct, 3Tera, Appistry, Elastra, RightScale, BMS, and Nasuni.

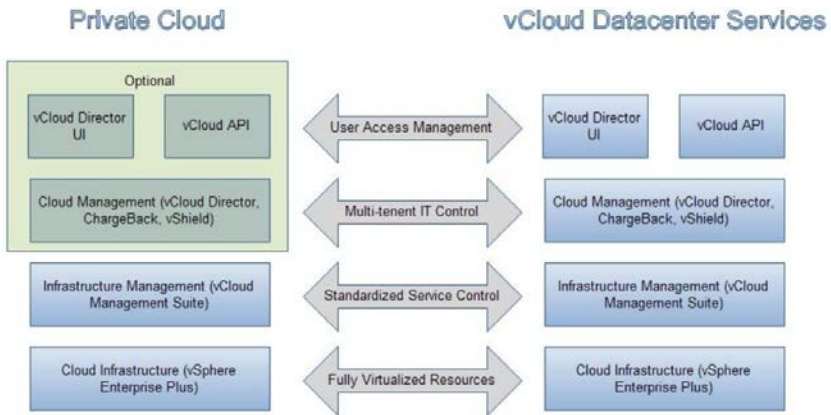


Vmware Vcloud Enabled Service Providers:

Terremark and Virtacore provide vCloud Express based public cloud. Terremark cloud is virtualized using VMware. Terremark uses its own datacenter, distributed among 160 networks, globally. Terremark gives API enabled web-based standardized architecture. There are more than 450 operating systems that can run over their VMs. Terremark also provides hardware-based load balancing which is not available in EC2. Terremark also claims to have fiber attached persistence storage.

Virtacore delivers its vCloud Express on pay-as-you-go basis. Virtacore provides high-end availability which means if our VM dies for some reason then it is automatically replicated to a new server that is automatically created by Virtacore infrastructure. VMware vShield Edge is used for firewall control. OVFformat is supported by Virtacore vCloud Express. VMware vCloud Express’s API can be enabled over Virtacore.

Verizon Terremark, Bluelock, Colt, CSC, Dell Services, SingTel, and Softbank provide VMware vCloud Datacenter enabled cloud. VMware vCloud Datacenter is used to deliver enterprise-class hybrid solution. VMware vCloud Datacenter gives Layer 2 isolation, Active Directory integration, and role-based access controls. These features are enabled in the above mentioned clouds. Terremark enables Interconnect services (Layer 1), Peering services (Layer 2), and Managed Routing services (Layer 3) within and from their data centers. All in all, these clouds enable hybrid model for clients using vCloud Datacenter.



Private cloud Service Providers:

Microsoft Hyper V Server:

This is a Windows Server 2008 R2 based x64 virtualization solution. It can host multiple operating systems. It is a virtualization platform which runs windows hypervisor in between hardware and OS (Operating System). It does not contain third party device drivers. A dynamic datacenter with private cloud implications can easily be created from it. Linux distributions can be run as guest operating system on the Hyper-V.

It has integrated virtual-switch support. It also supports live migration of VMs, VM Chimney i.e. TCP Offload, and the use of Jumbo Frames (which are good for high throughput). Currently .vhd file format can be migrated to Hyper-V. Hardware assisted virtualization should be enabled on the server on which Hyper-V based virtualization has to be applied.

Open Stack:

It is open-source software that can be used to build private as well as public clouds. It is an initiative first started by Rackspace and NASA. It has three dimensions Compute, Object Storage, and Image Service. Due to its nature of being open source, it has gathered much industry attention. Different kinds of adapters can be produced using this technology which can work with other clouds e.g. Atlas-LB, which is a Load Balancing as a Service solution.

Compute component of Openstack provides control panels, and APIs that can be used to orchestrate a Cloud. It supports seven major hypervisors, and can be built on multiple hardware configurations. Live VM management, floating IP addresses, Role Based Access, Security Groups, and Federated Zones are supported in it. It is a very powerful solution. It also supports RAW, Hyper-V format (.vhd), VirtualBox (.vdi), Qemu/KVM (.qcow2), VMware (.vmdk), and .ovf formats.

Eucalyptus:

Eucalyptus is a private cloud computing platform, which provides a very powerful API that can easily integrate with Amazon cloud. It has commercial, community, and open source cloud dimensions. If organizations want to get the benefits of AWS without its public nature, then it can implement Eucalyptus into its own datacenter and can enjoy the same kind of power as has been provided by AWS.

Open Platform Cloud:

Open Platform is a new cloud build solution in which all the components of a cloud are build using open standards and solutions. One such introduction to the market which is robust is CloudFoundary. CloudFoundary provides very powerful solution which is based on this open platform. CloudFoundary is the initiative from VMware.

Ericsson Composition Engine:

Ericsson Composition Engine3 is an Open application platform that provides an environment for service providers for management of feature interaction among IN, IMS, and internet services thereby creating converged and differentiating applications for heterogeneous platforms

and access technologies. The underlying technologies are Java EE, Linux, and Open Multimedia Platform (OMP) framework.

Ericsson Composition Engine's default runtime target platform is based on

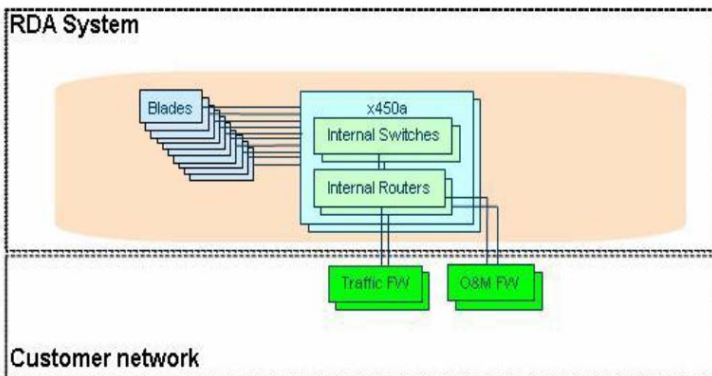
1. COTS (Commercial off-the-shelf) hardware (Sun Blade Server and Extreme switches)
2. Linux based operating system viz. RHEL 6.0
3. Java EE/SIP application server -OCCAS (Oracle Communications Converged Application Server) and/or Glassfish
4. Database (MySQL)

OMP Basis:

ECE default RDA is based on the Ericsson Open Multimedia Platform framework (OMP) and serves as a model for building server nodes with open interfaces and standard components. OMP framework is based on common hardware architecture which is defined for building the software part in order to make it target a hardware setup that can cater OMP components and proper functioning of applications.

Processor Blades:

ECE uses blade configuration with each blade configured as either traffic blade or management blade. Two server blades are always reserved for management purposes and up to 18 server blades are supported for payload purposes. Management blades are called SC (Service Control) blades and traffic blades are called PL (Payload Blades).



Highly redundant Infrastructure:

For the redundancy purpose, ECE is inherently designed and deployed by a combination of hardware redundancy, network design and software architecture.

Hardware redundancy

1. Blade server architecture with hardware redundancy
2. Power redundancy
3. Interface (active-standby)
4. Ethernet switching redundancy

Network design

1. VIP, load balancing
2. Different networks for OAM and traffic

Software architecture

1. Redundancy provided by Application Server middleware, e.g. clustering
2. SAF (Service Availability Framework) middleware
3. Database redundancy
4. Application architecture is based on strategies of architecture patterns, and data persistency patterns

AMAZON WEB SERVICES:

AWS Compute Offerings:

Elastic Compute Cloud (EC2)

EC2 provides on-demand compute capacity. This service is public cloud offering, and does not extend to private cloud. Multicast, broadcast, and multiple Ethernet switching are not supported in EC2.

Auto-scaling:

Auto-scaling service from Amazon provides an interface in which we can define conditions on when the scale out and scale in has to be applied to the cloud application. ECE in the Amazon Cloud can use this service, or it can use its own auto-scaling mechanism.

AWS Database Offerings:

Amazon provides three different types of database offerings. They are Amazon SimpleDB, Amazon Relational Database Service (RDS) and Amazon ElastiCache. Amazon SimpleDB is non-relational data store. Amazon RDS provides access to MySQL or ORACLE database, which is completely managed by Amazon. The capabilities of the database are in control of the customer, so any application that uses its own MySQL or ORACLE database in it, can also use Amazon RDS. ECE has also these two options, whether it should use its own MySQL or Amazon provided RDS service, which is specifically designed for cloud environment. ElastiCache provides in-memory cache deployment and management service. The main benefit of it is for read-heavy application workloads by improving their latency, and throughput. ECE can also use its own caching mechanisms or the ElastiCache.

Amazon Deployment and Management Offerings

Amazon Elastic Beanstalk:

Elastic Beanstalk provides an interface using which a Java application that is based on Apache Tomcat software stack can easily be deployed just by uploading the .war format file. Scalability and load-balancing of the application is automatically applied to the deployed application.

Amazon CloudFormation

It is a templates-based deployment service where cloud resources are defined inside a template file. This file is used by the Amazon to deploy resources in the cloud that are to be used by the application. It is a great automation solution that can be used by ECE deployment. It supports almost all the Amazon services e.g. EC2, RDS etc.

AWS Messaging Offerings

Amazon Simple Queue Service:

Amazon SQS enables automated workflow of distributed components of a single application. Using it messages can be passed between individual components with states preserved in queues. This ensures a highly failure resilient mechanism. Applications which are loosely coupled can use this service.

AWS Monitoring Offerings

Amazon CloudWatch:

Amazon CloudWatch is the monitoring tool used by Amazon and provided as a service for its customers. It provides information on resource utilization, latency, and performance metrics of the cloud resources. ECE can get benefit from this resource and apply its results to scaling mechanisms of the ECE in the Amazon Cloud.

AWS Networking Offerings

Amazon Route53:

It is a Domain Name System (DNS) service. It can be used for AWS resources as well as non-AWS resources over the internet. ECE can also use AWS DNS offering to address DNS issues.

Amazon Virtual Private Cloud (VPC)

Virtual machines that are available in EC2 are also available in VPC. But VPC provides the ability to connect the public part of the cloud to the private part of the company. It also gives enhanced networking support like IP address-ranges. IPv6, multicast, broadcast, multi-Ethernet switching is still not supported in VPC.

Amazon Elastic Block Store:

It is used to create storage volumes from 1GB to 1TB. It can be attached and detached to a computing node. It can be copied, transferred from one compute resource to another, and accessed at very high data rates. It is used for an application which uses persistent storage.

If applications do not have persistence storage requirements then they can use the virtual machine's local storage.

7.4 Service Provider Concerns in the Cloud:

Cloud Computing has a profound effect on Software Development Life Cycle (SDLC). Manual up-gradations to cloud deployments or even making cloud deployments is conducive to errors, so there is a strong need to automate this process along with defining clear servicing of applications . In many scenarios, it has been seen that reference deployment architecture used by the enterprise on-premises is different from the one in the cloud . For example, the organizations might have broadcast at their

network level but if they want to implement in the cloud vendor, it is strong likelihood that cloud vendor might not support it.

There are many scenarios both technical and non-technical in which an on-premise application cannot be directly shifted to the cloud. Either you are going to make a new application that will harness the cloud or you are going to port your application to the cloud. Main issues to resolve, in application design, are encryption of cloud storage and transient data, integration with cloud backup services; load balancing across geographical regions, integration of cloud security mechanisms into the applications, patches for network limitations, and identity management in clouds.

Multiplicity of applications onto single server, as in public cloud, entails a solid VM isolation in compliance with the standards. Systems have to be made which can address intrusion in SaaS applications e.g. Anomaly-based IDS (Intrusion Detection System) . Grid computing addresses some security standardization issues, for integration with NGN, but cloud computing does not have it in current offerings . Security concerns include but not limited to accidental release of protected data, user authentication, and access control. Virtualized systems come with security problems that specifically arise from miss configurations.

There are mainly three security goals for virtualized systems namely operational correctness, failure resilience, and VM isolation. An assessment has been made on undesirable information flow in virtual machines that reside in the same availability zone. Security can be integrated through the provisioning of cloud vendor's provided firewall mechanisms e.g. security groups mechanism from Amazon Cloud. The question is then how well the IT and system administrators configure these options . A number of tools are available which can address this issue.

Since cloud vendor own the infrastructure, enterprise does not have control over the commodity hardware platform on which applications are running. Recently AWS was struck by downtime . This affected large applications, owned by large enterprises like Foursquare, Quora etc, and the only excuse that came from AWS was an undisclosed problem in servers .

Security solutions in telecom address integrity of data, availability of service, accountability of offerings, confidentiality of privacy data, and

authenticity of user-access issues. So a cloud provider has to comply with all of them . Abuse of cloud computing technologies by professionals working in the public cloud is not in control of any customer, so there must be a standard to put limitations on malicious insiders. Insecurity in the APIs, shared technology and cloud software vulnerabilities, data leakage, account and/or traffic hijacking is some common threats for which we see examples in the cloud industry.

Current clouds are incapable of providing telecom-grade latency solutions . Intra-cloud latency adds up to the network or internet latency to give total systemic latency . This issue has to be addressed by cloud provider or a vendor who is providing SaaS. To curb these problems, VPNs and network overlays are being employed. One such network overlay is provided by Akamai . Latency guarantee has to be end-to-end, in order for complete QoS (Quality of Service) provisioning and edge devices have to be reconfigured with respect to cloud computing .

Since infrastructure hardware is owned by the cloud vendor, it is very hard for the enterprise to trust the vendor in many scenarios. One such scenario is when downtime or disruption in the service comes due to the hardware malfunction. At this point, the enterprise has to trust the cloud vendor that it will recover from the disaster without enterprise's intervention. Open standards are needed to reduce vendor lock-in . We have seen many such examples of this kind of lock-in in the AWS cloud. The enterprises have come up with a solution to this type of problem by backing up their application data in another cloud. This inter-cloud concept is on the verge, and enterprises are now seeing it as a requirement rather than an option.

7.5 Attractive Oppurtunities for Telco In Cloud:

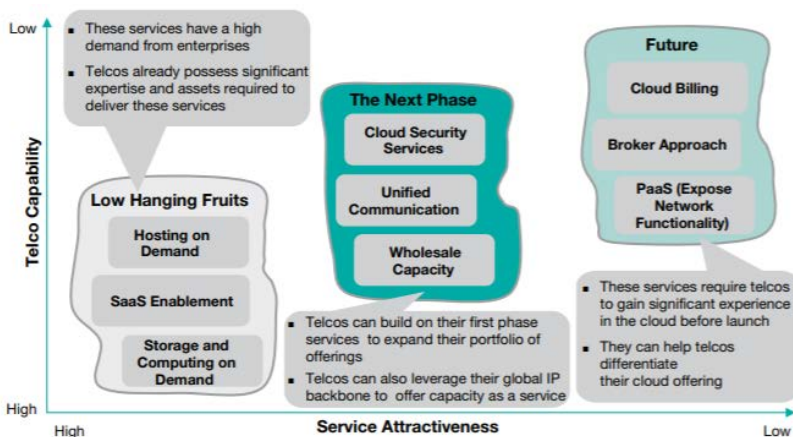
Cloud computing presents several opportunities for telcos to pursue . Analysts estimate that by 2015, telcos will have a 23%20 share in the overall cloud services market. Operator success in the cloud, however, will depend largely on selecting the right choice of services to launch. Telcos should consider a combination of factors such as the attractiveness of a service, its complexity, and the expertise required to launch before determining the services to offer.

Most importantly, operators should focus on those services for which they are well positioned to offer by leveraging their existing capabilities such

as data center expertise, managed service experience, and global footprint. Based on this rationale, the most relevant commercial opportunities for telcos can be categorized into three different service buckets: low hanging fruits, the next phase, and the future. In order to make the most of these opportunities, telcos should launch these offerings in a phased manner, starting with the low hanging fruits first. In the subsequent subsections we will detail the three service buckets.

These are the services which provide an immediate attractive opportunity for telcos and should be launched first. Not only do these services have a high demand and revenue potential but also existing telco strengths are well aligned to deliver them rapidly. Hosting on-demand, SaaS enablement, and storage and computing on-demand fall under this category.

Telcos are already proficient at providing managed hosting services for enterprises. In collaboration with technology partners, operators can rapidly virtualize their existing data center infrastructure, without excessive cost overheads, to offer on-demand hosting. Some operators such as AT&T and Orange already provide this service. Service delivery through the cloud will not only result in the optimization of telcos' existing infrastructure, but also attract a large number of customers interested in maximizing IT investment by migrating to the cloud. According to analysts, when compared to traditional hosting, cloud hosting can help enterprises save 50% in costs with an associated ten-fold increase in capacity.



SaaS has the largest share of the cloud services market and its adoption within enterprises, especially SMEs, is rising. Telcos which have not yet ventured into SaaS can quickly establish a firm footing by partnering with a wide range of ISVs and leveraging their existing infrastructure to deliver diverse SaaS applications. In addition to gaining a substantial share of the large and increasing enterprise spending on SaaS, these telcos can also improve customer loyalty by offering SaaS as a value added service.

Computing, storage, and backup along with hosting constitute the bulk of US\$5 billion²³ IaaS market. Telcos already offering on-demand hosting can cross-sell computing and storage through an integrated package. In addition to hosting, providing virtual CPU instances (to meet the different computing needs of customers) and on-demand storage and backup will result in a comprehensive IaaS solution. In order to deliver these additional services, existing data center resources can be easily leveraged, thereby, minimizing incremental costs.

This phase includes the next line of services, which telcos should offer in order to expand their portfolio of cloud services and establish a stronger footing. Operators can sell these services on top of their existing cloud proposition. Cloud security services, unified communication, and wholesale services fall under this category.

In terms of market share, telcos are one of the leading providers of managed security services. They can quickly leverage their existing expertise in network, application, and data security to deliver these services from the cloud. Cloud security is an attractive market, which is set to rise by 200% during the period from 2008 to 2013. Telcos can capitalize on this opportunity by differentiated offerings such as Distributed Denial of Service (DDoS) protection. Operators have an inherent advantage in this area because they can look across their backbones and prevent potential attacks earlier than most other service providers.

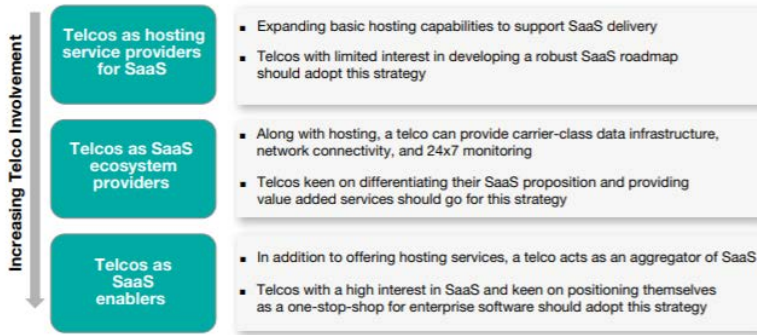
Enterprise customers are interested more than ever in a common platform for all their communications needs including IM26, presence, voice, conferencing, and email. The unified communications market is expected to rise at 55.6% CAGR to US\$4.3 billion between 2008 and 2014, fuelled by cloud computing. Telcos already deliver individual communication

services like messaging, VoIP, and PBX to enterprise customers. They can build on this experience to offer a unified user interface and experience across multiple devices. Reliable network connectivity, which includes fast and secure connections from the cloud data center to the customer premise, is imperative for the success of any cloud business.

Telcos can offer capacity, over their global IP backbone and private MPLS networks, as a service to both cloud service vendors and enterprises. In addition to capacity, large global operators can also whitelabel a complete telco-focused cloud infrastructure solution for regional operators. Telcos should also think beyond traditional offerings and leverage the commercial opportunities presented by more novel services and delivery mechanisms such as cloud billing, PaaS, and the broker approach.

Technical and cost challenges make it difficult for most cloud service providers to run their billing infrastructure in-house. Unlike subscription based billing, pay-per-use billing is complex and failing to get it right can result in revenue leakages. Telcos can leverage their experience in billing metered services to enter the cloud billing arena. Operators along with their billing partners can provide their expertise as a comprehensive cloud billing solution for vendors.

As IaaS and SaaS space becomes mature and increasingly competitive, operators might shift their focus towards PaaS in order to diversify. PaaS is an attractive solution for ISVs and SMEs to improve their productivity and reduce costs by using cloud-delivered toolkits for application development and deployment. Operators can build on their existing experience with Service Delivery Platforms (SDP) to offer PaaS. Telco assets such as voice, location, and presence can be offered to help application developers build applications that can be monetized.



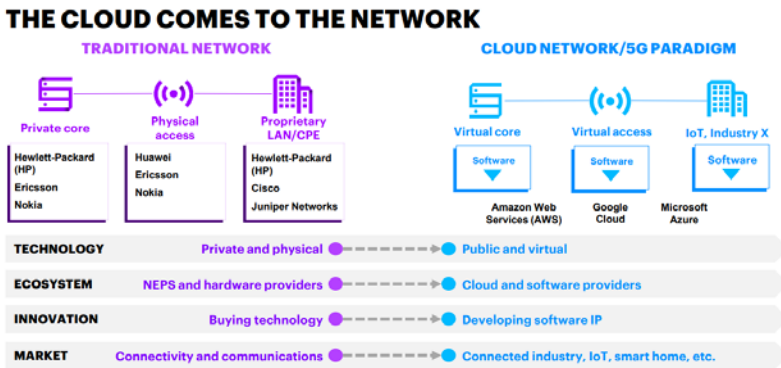
There is a growing demand for “cloud brokers” as intermediaries between end users and cloud providers. From SLAs with multiple vendors to compliance and security, the broker handles all cloud related issues. for a customer. This approach also enables customers to switch cloud vendors without worrying about the operational details. Telco experience in delivering multiple services with stringent SLA requirements, strong enterprise presence, and long lasting relationship with enterprise IT departments gives them an edge in the cloud broker space. Given the revenue potential and high demand of different cloud services, it is imperative that telcos do not delay their entry in this space. By diligently identifying and launching the right services at the right time, operators can maximize their share of wallet while the end customers would reduce IT CAPEX and OPEX.

As seen in previous sections, several telcos have entered into cloud computing and are focusing primarily on IaaS and SaaS. However, there is a significant possibility of these services, especially IaaS, being commoditized in the near future. As the intensity of competition increases and service differentiation dilutes, margins will fall. Therefore, customization and differentiation across their offerings, service delivery, and customer segment targeting, should be the hallmarks of a telco cloud strategy. In the following subsections we will illustrate how telcos can carve their niche in these different areas.

In addition to providing traditional IaaS, operators should focus on offering localized and customized services which have a potential of commanding high margins. This will help them stay relevant in the face of high competition from established players such as Amazon and

Rackspace. Telcos provide enterprise services across various geographies and have a good understanding of local market demand for these services including cloud. They are, therefore, best equipped to address the regional cloud services market needs. For example, in certain geographies cloud - based Virtual Desktop Infrastructure may have high demand, whereas other enterprises might be more interested in disaster recovery.

By quickly identifying and addressing such opportunities, operators can gain an edge over the competition. Offering customized cloud solutions can help telcos price their services at a premium. For instance, replicating the exact software testing environment on the cloud is a challenge for enterprises because many providers do not offer custom OS images and limit the type of configurations. By providing a customized virtual environment for companies to replicate their exact test conditions, operators can not only differentiate their offerings but also charge higher margins.



In the SaaS space, there are three different strategies which telcos can adopt with the level of involvement by operators varying significantly. Telcos should evaluate the level up to which they want to have a SaaS presence and accordingly adopt the right strategy. PaaS is an area which will see limited action from telcos in the near future. Before establishing a PaaS presence, telcos would need to carefully evaluate their technology readiness and experience with platforms such as SDP.

Service Delivery Telcos should endeavor to deliver services in a way that customers can enjoy the cost benefits of public clouds and the security and reliability offered by private clouds. This can be achieved through Virtual

Private Cloud (VPC) deployments. This model delivers services from a public cloud over MPLS-based Virtual Private Networks. VPC, therefore, offers the full security and privacy of a private cloud, but pushes hardware ownership to the service provider. Telcos can leverage their distinct strength in providing reliable private IP service to enable a cost effective and secure VPC solution.

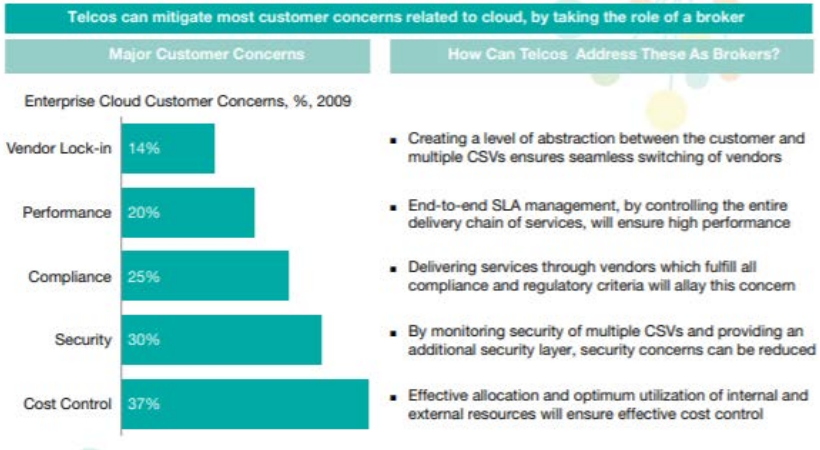
This is another innovative approach to service delivery where telcos are well positioned compared to their competitors because of strong enterprise relationships and experience of delivering multiple services involving stringent SLAs. However, operators should build significant experience in cloud computing before adopting this approach, so that they can successfully tackle the complexities associated with end-to-end solution delivery.

Large enterprise customers have multi-country operations and serious concerns about the security of their applications and data. Also, due to the sheer size and complexity of their operations, deploying cloud services, integrating them with on-premise systems, and continuous maintenance and support becomes a highly complex process. In order to target large enterprises, telcos should try and offer enhanced security and end-to-end cloud solutions across multiple countries.

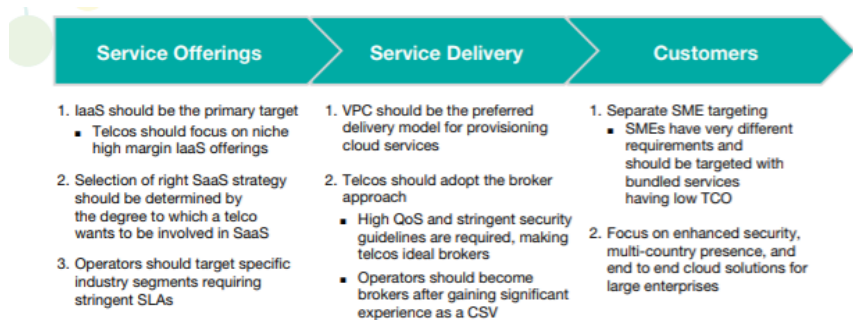
The share of SMEs in the overall cloud services market is expected to rise rapidly in the next few years. SMEs prefer all their ICT needs to be catered for by a single vendor and want solutions that are easy to deploy and support. Total Cost of Ownership (TCO), which also includes maintenance, upgrade and support is another factor which SMEs value more than the actual selling price of a solution. In order to effectively target this segment, telcos should focus on bundling different cloud services such as communication, security, and hosting in a simple package. Moreover, operators should offer standards-based cloud solutions and reduce overheads wherever possible, in order to minimize TCO. In summary, telco focus should be on offering niche IaaS for specific industry segments, provisioned through VPCs.

In conclusion, the revenue potential and high demand of cloud computing presents a real opportunity for telcos to offset the declining revenue from traditional services. Several operators have already entered this area and

others should soon follow suit. The in-place assets of telcos such as data center capabilities, global IP backbone, and experience in delivering managed IT services can not only help them expedite their launch but also establish a leading position.



However, there is significant possibility of cloud services, especially, IaaS being commoditized in the near future. Moreover, the competition is becoming increasingly intense with several players entering this lucrative market. Operators, therefore, need to constantly innovate and focus on the right services delivery models, and industries where they are best positioned, by the virtue of their strengths, to carve their niche and gain an edge over the competition.



7.6 Business Opportunities in Cloud Telecom

Cloud computing represents a major change in how IT resources are delivered and consumed and will influence the telecom industry, its future

services and business offerings. Generating new revenues through offering cloud-based services is less discussed in the literature, followed by a lack of commonly agreed and complete methodologies for this purpose. In this paper we propose a three-step method combining qualitative and quantitative models for the assessment of telco's new business opportunities, in particular, a combined role of cloud broker and carrier.

With low subscriber growth in mature markets, price pressure on voice from competing operators, and traditional services like SMS and voice being challenged by substitutes such as Skype and Facebook, telcos need new ways to drive growth. One of such opportunities is cloud computing. Among the various roles in the cloud ecosystem, two that draw particular interest to telco is the concept of a "cloud carrier" and that of a 'cloud broker'. A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers, being the core business of telco.

While, a cloud broker is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers for two reasons:

- i. it offloads the burden from the customer of having to deal with multiple vendors
- ii. in a similar fashion, offloads the burden of vendors that have to deal with millions of customers. Moreover, most of the telcos already have a billing relationship with many customers that can be built on to extend to the cloud market.

Moreover, the rationale for a telco to step in as cloud broker can be

- i. to stop current subscribers churn
- ii. to acquire new subscribers in the rapidly expanding cloud computing market. Mobile computing with a possibly large international footprint is inherently supported through bundling of cloud services with mobile connectivity as e.g., 3G networks.

To systematically examine the business potential of telco as cloud broker, carrier or a combined broker and carrier solution, we need methodology and tools. The purpose of this paper is to present a tentative understanding

of how such methodology and tools may look like. More precisely we suggest a three step methodology for telco's in relation to their exploitation of cloud:

Step 1: Description. Models that help us provide the necessary understanding of the context where making cloud business is relevant should be evaluated. Here qualitative analysis models are preferably used.

Step 2: Analysis. Tools and models that help us analyze the economic effects of the business prospects. These models are preferably quantitative models and developed based on the input from the qualitative analysis performed in step 1.

Step 3: Validation. After the quantitative analysis model is chosen in step 2, validation of the model is performed using simulation data input. Here, the purpose is to test the developed model and improve the quality for the decision making in business. If the analyzed situation deviates, the model will need to be revised.

Generally, we perceive cloud service provisioning to be a typical example of a value network, which is characterized by value creation through interactions between different roles. The major roles related to cloud computing and their relations are described using a value network perspective - infrastructure provider, platform provider, service provider and aggregator in addition to the customer role. The infrastructure provider supplies the network with computing and storage services necessary to run applications within the cloud, while the platform provider offers an environment that can be used to develop and deploy cloud applications. Moreover, a service provider develops applications that are offered and deployed in the cloud.

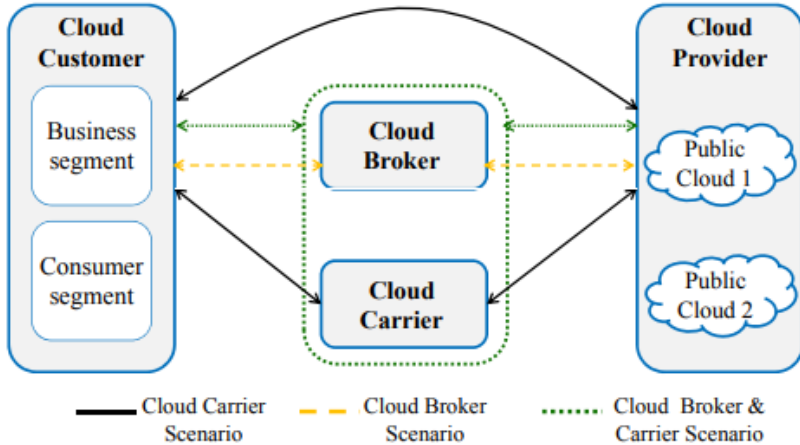
More specifically, we anticipate that the cloud carrier provides the network necessary to connect cloud data centers and cloud customers, possibly offering cloud specific connectivity services. The cloud provider offers cloud services according to the IaaS, PaaS or SaaS delivery models. The deployment model can be public or hybrid. The cloud broker offers cloud services to the cloud customer as an aggregation of the cloud provider's services. The customers can be mass market consumer or small business in the SME/enterprise market segments. Naturally, the customer may buy

services from the cloud provider directly, but usually this will occur in combination with an aggregator's offering.

The combination of the broker and carrier roles is designated to manage relationship between cloud customers and providers, through bundled service and carrier offering through a single point of contact concept. We use Osterwalder's framework to structure the relevant cloud scenario. It has four main building blocks: the service offering, the target customers, infrastructure of partners and resources necessary to develop and deliver the value proposition and finally, the revenue and cost structures associated with the business proposal.

The framework is chosen as being intuitive to understand and serving a good starting point for brain-storming in order to gain a common understanding among stakeholders. Offer here refers to the benefits a company's value proposition to its clients through solving their problems with the company's offering of services or products. A telco's value proposition can preferably be a single point of contact for the cloud customer offering a hassle-free implementation and usage of business applications with no IT staffing and infrastructure, with a pay-asyou-go model, and contracted in a single Service-Level Agreement (SLA) (as compared to two separate SLAs: one SLA from cloud service provider for service quality, and one from network provider for transport). Customer refers to client segments for the products and services, and how to deliver these offerings through distribution channels and keep the customer relationship with the company.

The value proposition could be directed towards current customers reducing churn as well as gaining new customers in domestic or foreign market in two different customer segments – consumers as well as businesses. The former would include youths and adults consuming mobile data traffic on gaming. The latter segment typically includes SoHo/SMEs (Small Office, Home Office/Small and Medium sized Enterprises) as well as larger enterprises and the public sector. Infrastructure could be understood as key processes or activities which create the product or service the company offers, the company's core capabilities and competencies necessary to execute the business model together with partners with complementing capabilities.



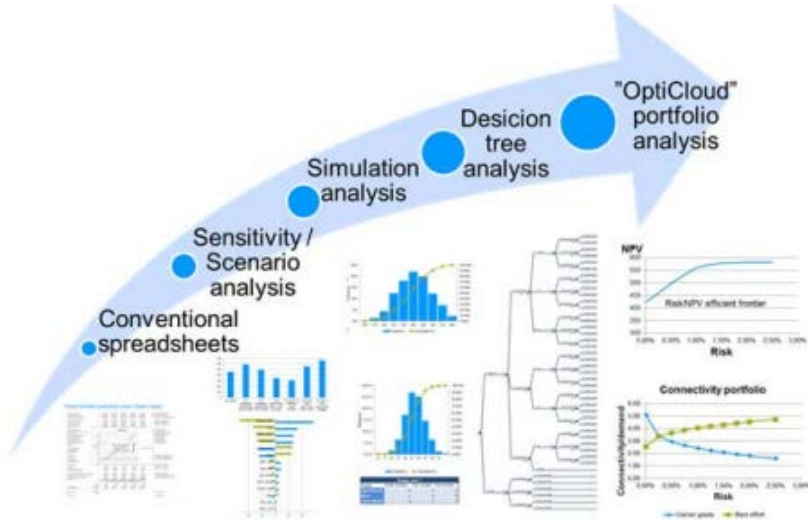
Telcos are already cloud carriers in providing networks for connecting cloud customers to cloud data centers, and this is a key resource for all possible roles. In addition, telcos can take a more active role in offering cloud specific network offerings such as managed networks with QoS (Quality of Service) and security guarantees. Telcos also have data center infrastructure and experience in operating own communication services, as well as for regular hosting services. Furthermore, telcos have billing solutions as well as marketing competence.

The network asset is important for offering an end-to-end service. Strategic partnerships with leading cloud providers are necessary to establish in order to develop and operate competitive cloud based services. Finally, finance refers to cost structure of the business; fixed or variable, operational or investments, together with how the revenues are gained using different pricing models, etc. Major cost categories are related to start-up investments and running personnel cost. The network connectivity needed will be an additional cost component.

The revenue streams for a cloud service provider are pay-as-you-go or subscription based from the bundled services offered to the customers, maybe premium priced as a bundled and integrated solution. Due to product components provided by cloud providers and other partnering vendors, a revenue split with these partners is necessary.

There are different approaches combining different techniques in a systematic manner to account for uncertainty. Below illustrates different

quantitative methods for analysis of cloud computing economics (note that graphs inside the figure are not meant to be clearly readable and are used here for illustration only). The arrow indicates increasing complexity and increased consideration of stochastic variability. To the far left we find a convention business case model, and to the far right we find our portfolio model approach, briefly discussed above and here named OptiCloud.



Quantitative methods are briefly compared below. Conventional spreadsheets are used to estimate net present value (NPV) based on a chosen business strategy basically assuming that all decision (market expansion, service portfolio, etc.) are made at the time of analysis. Sensitivity analysis is typically used to assess sensitivity of the model outputs with respect to changes in the model inputs. The sensitivity is measured as the rate of result change as consequence of the changes in one variable while the values of all other variables are constant.

This is helpful to decide where to put more estimation efforts in order to fine-tune the model. Scenario analysis is an improved sensitivity analysis, since examining the effect of each variable in separation is meaningless in cases when interdependencies between variables exist. The most complete analysis of scenarios would be to assess every possible outcome of each uncertainty factor. Unfortunately, then it becomes too costly and impossible to differentiate between the scenarios. Simulations can handle complex decision problems under uncertainty that have a large number of

input variables. Simulations help to create risk profile of NPV; however, there are no good means to translate it into a clear decision for actions based on the results of simulation.

Decision tree analysis allows accounting for flexibility to make decisions at a certain time in future. The evaluation model corresponds to constructing a decision tree or dynamic programming model that describes the sequence of decisions to be made and the resolution of uncertainties over time . However, decision trees can become too big for graphical representation and comprehension. Quantitative analysis of business models for provision of cloud services involving a single actor are well understood, both organizationally and economically. However, usually companies choose among several service provision channels. Portfolio analysis uses the portfolio theory to balance between return and risk and to select the best portfolio of service provision taking into account the actor's risk attitudes.

Adequate risk management is especially important in a highly volatile and competitive telecommunication environment. Industrial projects in high-tech industries are often characterized by considerable uncertainty that at the same time carry different flexibilities. Moreover, stochastic programming (as a means to implement portfolio analysis) provides the optimization models for adequate treatment of uncertainty in the planning of cloud service delivery. Brokering and carrying of cloud services will demand a specific quality of service. Typically, the portion of demand that is satisfied with lesser quality is considered to be not satisfied and lost. We need to model a decision to select an optimal combination of QoS enhancing measures, i.e., a connectivity of different grades: best effort connectivity or carrier grade (premium) connectivity.

We build a mathematical model to analyze and optimize the connectivity portfolio of a telco offering cloud brokering. The model describes the relation between the profit and the risk of not providing good enough service. Maximizing the expected profit for a reasonable range in the risk values yields a curve commonly known as efficient frontier. The modeling challenge is to find mathematical descriptions for the profit and the risk in terms of tangible variables as user generated service demand, implementation costs and grade of service.

A stochastic approach is necessary to account for the variability in service demand and satisfied demand. At the level reported there the model is completely general with respect to the distribution of the random variables. Of course, in order to further detail the model, and to obtain numerical results, specific distributions must be assumed. In our model, we define profit as a random variable resulting from the difference between revenue and costs, i.e. Profit = revenue – penalty cost - provisioning cost

To make the model more tractable we consider the expected values of these variables, where the expected revenue is proportional to the expected served demand, the expected penalty cost represents the revenue loss for providing the service below user's expectations level, and is thus based on the proportion of expected demand not satisfied, the expected provisioning cost contains a fixed component and a variable component proportional to the capacity of the network, i.e. proportional to the expected satisfied demand.

As previously mentioned, we want to maximize the expected profit for a reasonable range in the risk value. In order to do this, we need to define the notion of risk and how it relates to the profit. We assume that the main risk to cloud brokering comes from possible violation of service level agreements, user's expectations about QoS and resulting potential increase in churn. Such risk can be measured by the share of demand that is not satisfied with required QoS. In other words, we model the risk as proportional to the fraction between unsatisfied demand and average demand.

Based on the models developed, we have implemented computer simulation tools and use modern portfolio theory to balance the trade-off between the profit and the risk of not providing good enough service. To populate the mathematical model and validate it, we need quantitative variables, e.g.: Quality of Service (best effort connectivity vs. carrier grade connectivity), Service bundling (Office 365, etc.); Market size, Expected reduction of churn; Revenue share among partners, risk acceptance by partner; Operating costs (e.g., employees, sales and marketing, connectivity cost depending on its type, penalty costs for broken SLA); Investments in a cloud service platform; Revenues (e.g., revenues from customers and from broker, based on revenue split; revenues from reduced churn from cloud service offerings).

The current version of the model takes into account two connectivity types: best effort connectivity and carrier grade connectivity. However, work is in progress to generalize this to a portfolio of connectivity types. The model produces an efficient frontier allowing cloud broker to tune its connectivity portfolio to requirements of particular user groups by selecting the risk threshold according to their preferences and choosing the optimal connectivity portfolio, i.e. a portion of carrier grade connectivity vs. best effort connectivity. Carrier grade connectivity is here preferred for risk adverse telcos avoiding dissatisfied customers.

Cloud computing represents a major opportunity for telcos with regard to cost savings and revenue generation. This paper addresses telcos' revenue generation opportunities from brokering new cloud services bundled with connectivity to current or new customers. We described a three-step research process to assess telco's new business opportunities. We begin with a qualitative model, gradually building a quantitative model and providing a preliminary validation based on a simplified business case.

This research process and proposed the method mitigates the current lack of completeness for assessment of cloud business opportunities. Further refinement of our three step process implies generalizations such as, specter of cloud products and customers, including users with different quality of service acceptance, risk profile and payment willingness; and use of real case input data in the validation phase as well as to support real business decisions.

Before embarking on a process of transformation, telcos must identify the type of cloud provider they wish to be, as different roles will demand different sets of capabilities. Before embarking on a process of transformation, telcos must identify the type of cloud provider they wish to be, as different roles will demand different sets of capabilities.

A. Repackage existing capabilities— Leverage existing hosting and networking capabilities to develop and deliver cloud infrastructure and storage services. These services will be required for any other functionality that moves up the cloud stack (i.e., PaaS, SaaS, BPaaS). Utilise existing business services and operating functions that can be repurposed and delivered as a cloud service (e.g., billing). Position the new business as a platform enabler—build horizontal and/or vertical cloud enablement

platforms that can protect and monetise the network, infrastructure, product, and data assets by providing an ecosystem to leverage those assets.

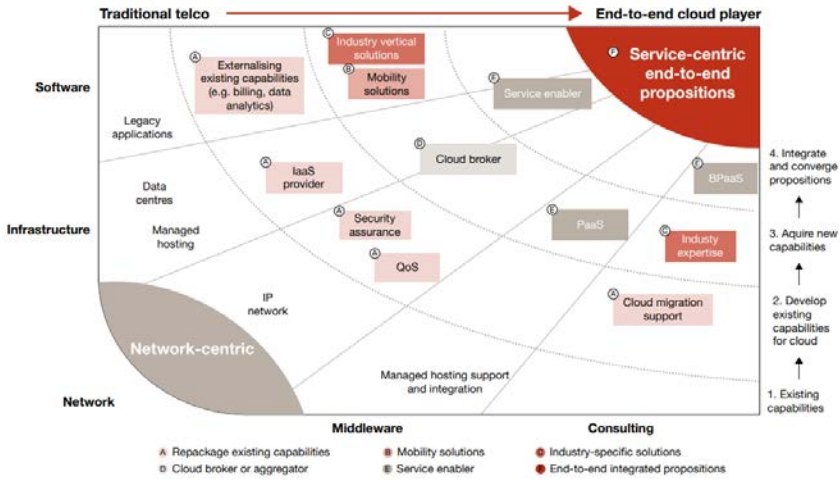
B. Mobility solutions—Work with mobility development teams to create integrated solutions in the cloud with mobile and nonmobile applications.

C. Industry-specific solutions—Work with customers and partners to deliver industry-specific solutions across the value chain (i.e., solutions for highly secure and regulated industries like healthcare and financial services, or solutions for industries with high contentstreaming, etc.). Also team with professional services companies that can provide industryspecific expertise.

D. Cloud broker or aggregator— Aggregate public cloud services and provide some quality of service (QoS) or security assurance (network performance optimisation, data security).

E. Service enabler—Complement core infrastructure, software, and platform capabilities with other assets and processes (e.g., data analytics and network application programming interfaces [APIs]) and provide them to third parties so they can better deliver their own services (application development, content delivery, revenue assurance through operator billing, etc.).

F. End-to-end integrated propositions—Connect some of the services above the network layer (that is, software and business processes) into the network so they are standardised and integrated into the network, and then the operator can change the definition of what the network provides. The operator can push the network boundary upwards.



All of these opportunities should be viewed in terms of the desired customer segment and telcos’ capabilities. A customer shift towards cloud offers telcos the opportunity to transform their business model, building a new fit-for-purpose platform that grows with increasing cloud adoption and gradually replaces the legacy business approach. This transformation opportunity includes the potential to redefine the way telcos offer service to their corporate customers.

Given that telcos have been wrestling with the profitability, complexity, and lack of transparency in their B2B businesses for the last 10 years, continuing on the business-as-usual basis to migrate to cloud is probably not a realistic route to success against the new entrant specialist cloud service providers that don’t have a complex legacy to protect or transform. To access new capabilities and gain the scale required for global cloud services, telcos will need to consider strategic partnerships.

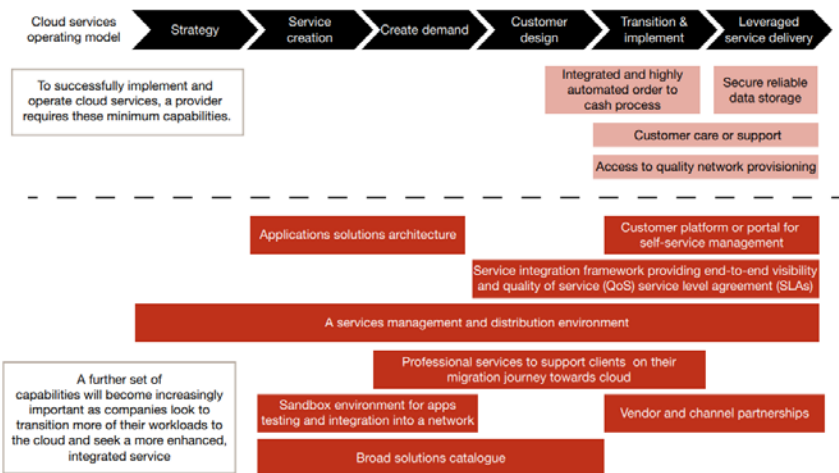
Depending on the type of partnership, new avenues of revenues can be identified and implemented.

- Technology partners—Develop partnerships with key technology solution companies, and integrate their services into the overall telco network and cloud structures.
- Customers as partners—Develop partnerships with customers to gain unique insights into the development of services that can be industry specific and provide the opportunity for shared revenue models.

- Professional services firms as partners—Work with professional services firms, which typically have keen insight into telco operations and services. They can combine that knowledge with their ability to access their firms’ multi-industry expertise and C-level insight, and they can work with the telco to define products and services that can be jointly marketed and sold to directly address specific industry issues.

Based on our experience of best practice companies, to successfully implement and operate cloud services, a telco needs the following minimum capabilities:

- Secure, reliable data storage
- Customer care or support
- Integrated and highly automated order-to-cash process
- Access to quality network provisioning with the ability to guarantee a high level of availability (for example, greater than 98 percent).



A further set of capabilities will become increasingly important as companies look to transition more of their workloads to the cloud and seek a more enhanced, integrated service:

- Customer platform or portal for self-service management
- Applications solutions architecture

- A services management and distribution environment
- Professional services to support clients on their migration journey towards cloud
- Sandbox environment for apps testing and integration into a network (a sandbox environment can be viewed as a PaaS environment)
- Vendor and channel partnerships
- Broad solutions catalogue, including third-party cloud applications
- Service integration framework providing end-to-end visibility and quality of service SLAs
- Telcos are stronger in some of these areas than their tech competitors, and vice versa for some of the other capabilities. Telcos are stronger in the following areas:
 - Network and hosting services— Telcos have the ability to guarantee specific levels of quality through ownership of the network. Smaller carriers may need partnerships to extend the reach of these services.
 - Management services— Larger telcos currently provide comprehensive management services for their hosting and other telco-related WAN services (e.g., managed data services)
 - Existing partnerships—Large carriers have teamed with technology vendors to leverage their capabilities to deliver a cloud self-managed environment.
 - Scale and scope—Telcos are able to act as a single point of contact for a multitude of vendor partner products and services.
 - Distribution channel—Telcos typically have more established IT customer relationships and are able to up-sell and cross-sell more easily.

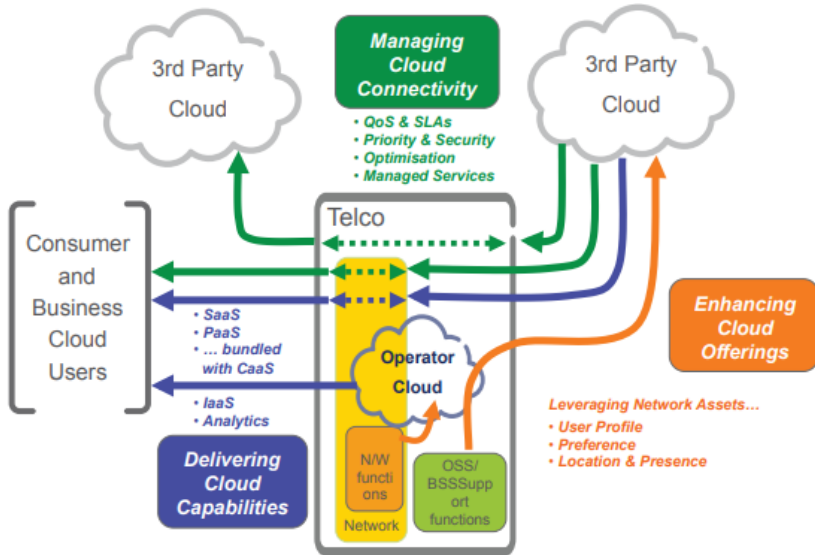
Telcos need to improve in the following areas:

- “Network blinkers”—Telcos tend to analyse all situations from an infrastructure perspective. Instead, they should treat all cloud activities as an enterprise architecture exercise and consider the multiple

dimensions of a client problem. This enables them to deliver more than infrastructure.

- Inability to leverage existing capabilities—Despite clear synergies between emerging cloud propositions and the services already delivered by telcos, the telcos are failing to capture this opportunity due to: – Capital constraints for R&D – Complex organisations (e.g. separating IT-related initiatives from non-IT initiatives) – The inability to integrate complex services because of different product and marketing organisations – The inability to communicate between internal telco business and client organisations, which leaves potential service opportunities untouched – The inability to see the bigger, longer-term opportunity
- Legacy product constraints—The legacy of the proliferated products is strong and restricts telcos to a set of processes and systems that limit their progression to cloud (particularly true for multinational corporate clients).
- Lack of simplification—Products and services are convoluted and unbundled, which is not appealing to the smaller and midsize B2B customers. Telcos can offer out-of-the-box operational capabilities such as distribution, retail, customer care, and billing (which most other cloud providers targeting the SMB segment cannot offer); however, telcos are currently unable to act as cloud brokers or aggregators to structure service offerings into SMB-friendly products.
- Brokering—Telcos should create an environment where the telco becomes the integration point for customers requiring multiple interfaces, applications and network services through a single point. As stated earlier, the partnerships that telcos develop combined with their infrastructure can position the telco as a hub for the trafficking of services. For many telcos, it will be easier to build a standalone system and process stack for their cloud proposition and migrate their legacy products onto it, rather than reengineering their existing systems and processes. To rapidly gain the capabilities they do not possess, telcos will need to form partnerships and conduct mergers and acquisitions to ensure they can deliver a competitive set of cloud propositions. Telcos will need to use these acquisitions to build a coherent cloud

business. However, it should be noted that integrating these acquisitions into the core is certain to destroy them, so the telcos will need to use these acquisitions as the kernel of a new integrated business model. A selected overview of M&A activity during the last few years shows how the size of the investments is increasing. Telcos are prepared to make even bigger bets as they realise the need to push into the IT space.



Although the notion of delivering computing as a service, where users pay for shared resources based on their usage, has been around for decades, it was not until a couple of years ago that cloud computing in its current form emerged. Since then, it has evolved and progressively changed the way we do business, communicate, and entertain ourselves.

Efficiencies, convenience and pay-per-use business models make cloud computing attractive to consumers and businesses alike. Consumers may not be aware of it but they are increasingly using ICT services that are cloud-based, from email and word processing to online music and social networking. Businesses, on the other hand, have benefited not only from outsourced applications, such as ondemand customer relationship management and collaboration, but also from cloud-based computing platforms and infrastructure, including hosted storage and data centres.

Telecom operators eager to exploit this next wave of opportunity are actively exploring their position in the emerging cloud value chain, some through direct investments while others through partnerships and acquisitions. U.S.-based Verizon, for instance, reported that it has spent well over US\$2 billion in 2011 alone, including a major acquisition, in a bid to capture “a big share” of the global cloud services opportunity, whereas France Telecom’s Orange Business Services has invested €750 million in its global network backbone in 2011 to achieve the requirements for cloudbased service delivery. Telstra, meanwhile, which has partnered with leading software, hardware and IT services companies, declared that cloud offerings will generate 25 to 30 percent of its total revenue within the next five years. The Australian operator plans to make A\$800 million, cloud-related investments during that period. With the global economic outlook remaining volatile, consumers and businesses alike will continue to keep a close watch on expenditures while in continual search of innovative and cost-effective ICT solutions. Whether it is consumer or business, cloud computing is enabling new revenue models and opening up new business opportunities for telecom operators.

Today, many of the cloud services targeted at consumers are offered by OTT players, which exploit ubiquitous connectivity to provide easy-to-adopt, on-demand services. More often than not, these companies are not providers of communications or connectivity services; hence a market for bundling basic connectivity (fixed or mobile) and communications (voice, messaging, data and video) with cloud-based applications is opened – and largely untapped – for telecom operators. Moreover, telecom operators often have an advantage over OTT web service companies when it comes to offering connectivity with hosted infrastructure.

In the consumer market, this can be as simple as online storage services that enable users to store and share their digital assets in the cloud. Leveraging their network capabilities, operators also have an opportunity to offer prioritised or guaranteed services – instead of best-effort – on selected OTT cloud applications, leading to new revenue potential. By combining cloud services with connectivity and communications-as-a-service (CaaS), telecom operators are creating compelling offerings that enable the monetisation of OTT applications to complement their core business.

In the business market, the value telecom operators bring is comparable to that in the consumer space, although the scale, usage and charging schemes will be vastly different. For business users, telecom operators are particularly well-positioned to deliver cloud services because they already own the networks and have trusted customer relationships. Telecom operators can offer business cloud services under a simple pricing structure that includes connectivity and devices, self-service provisioning, on-demand infrastructure hardware, as well as front- and back-office applications.

They can also provide value-added services, including analytics and reporting, predictive capacity planning, and managed services. Operators' ability to offer secure and reliable connectivity with varying degrees of quality-of-service (QoS) required by enterprises also puts them in a uniquely competitive position. QoS can be provided for different cloud service types used by the same user, or it can be allocated among different user types, according to their profiles and network policies. After all, telecom operators are already in the business of providing usage-based services with service reliability at the heart of those services, so extending that core capability to cloud offerings will only be a natural extension.

For telecom operators offering enterprise cloud services, target segments can be based on enterprise size for horizontal applications, such as unified communications (UC) and enterprise resource planning (ERP), or it can be vertical market-based for industry-specific applications such as meter data management for utilities companies. We expect industry-specific cloud services to benefit from the rise of M2M communications, and vice-versa, and there are already cloud offerings purposely built for airlines, healthcare providers and financial institutions.

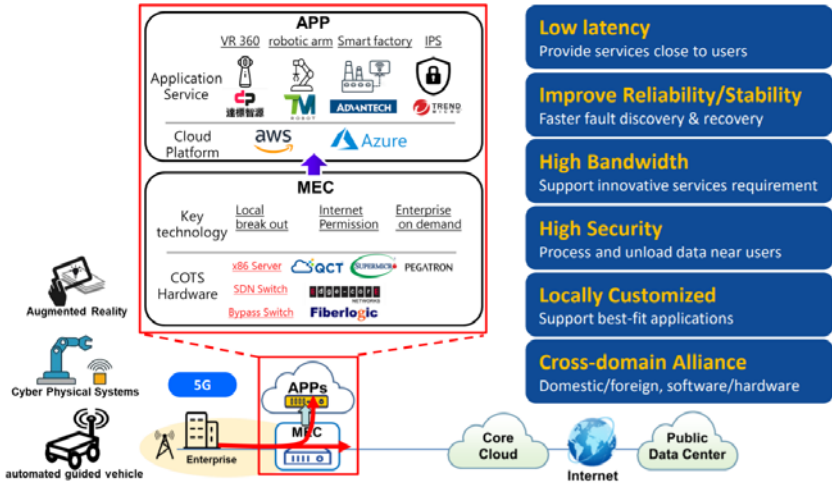
Cloud services, as distributed resources, depend on network performance and would suffer without good connectivity within and between them. Managing cloud connectivity appears to be the most natural value-adding activity for telecom operators given their expertise in connecting and managing networks. Operators are in a unique position to provide managed connectivity between cloud users and third-party providers, offering flexibility in network resources both in real-time and on-demand.

In this role, they are essentially intermediating brokers, enabling users to switch cloud vendors without worrying about network-related details. In addition, operators can offer connectivity services according to pre-determined agreements and choose to employ network-based techniques, including caching, optimization and data acceleration, to enhance the user experience of cloud applications. There are also possibilities for operators to offer device management, on top of end-to-end network management.

As with any service provisioning, telecom operators can partner and resell third-party SaaS and PaaS offerings bundled with their own services, or they can invest in the infrastructure and deliver both third-party and their own offerings on that infrastructure more efficiently. For instance, hosted unified communications, or UCaaS, which include IP telephony, video conferencing, presence, unified messaging and collaboration delivered on any device with service level agreements (SLAs), are some of the offerings that can ideally take advantage of an operator's own cloud infrastructure.

By having in-house data centers, not only can telecom operators offer own and third-party cloud-based applications, but more significantly, they can also provide IaaS in the form of on-demand hardware and computing platforms. Another key advantage of owning infrastructure is that operators can "cloud-burst" onto third-party infrastructure as demand grows.

with telecom operators' move to embrace two-sided business models, they are embarking on a transformation of their internal support systems. This, in turn, is providing them with the capability to expose network assets and interfaces that can be exploited by such features as location and presence, and by OSS/BSS assets such as subscriber profiles.



Telecom service providers can embed these attributes (for example, user preferences and activities and analytics thereof) with third-party cloud offerings, enhancing their value by making them more relevant and meaningful to users.

Of course, they can also embed these attributes with their own cloud offerings. Either way, it provides the linkage between the upstream and downstream components critical in two-sided business models. Furthermore, telecom operators are able to strengthen their relationships with end-users and third-party providers by acting as a service and billing aggregator.

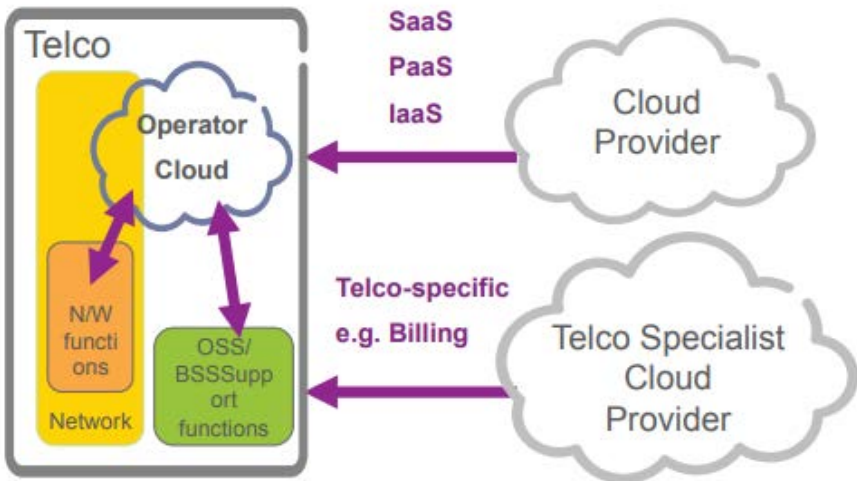
Telecom service providers operate in a complex operational environment, heavily dependent on technologies to run their networks and support the delivery of their services. Just as telecom operators are promoting cloud as a change agent for business, they too can benefit from its adoption. With operators seeking to transform themselves from their legacy environments and mindsets, adoption of cloud services can lead to efficiency gains, operational flexibility, and substantial cost savings¹. Cloud-based services are also highly suitable for product prototyping and trialling ahead of large-scale market launches.

As users of cloud computing, telecom operators can either:

- a. Simply transfer selected business functions and computing requirements to cloud to realise flexibility and faster time-to-market

as well as operational and cost efficiencies just as any large enterprise would. In the case of operators building cloud infrastructure, they can become their own customers by migrating their existing services and support functions onto the shared infrastructure, thus reducing their total cost of ownership.

- b. Simultaneously commercialize those cloud-based applications, becoming both users and providers at the same time. This opportunity exists in traditional telecom functions like OSS/BSS, where a telecom operator outsources its billing and customer care to an OSS/BSS specialist while partnering with the specialist to offer that functionality to other enterprises, such as utilities suppliers or OTT providers. More importantly, it also exists in emerging segments, providing operators with a nimble vehicle to enter a new market, such as M2M. Operators can offer low-cost, per-subscription M2M offerings with user activation, configuration, management and billing done in the form of software through an external M2M cloud enablement provider. This model also works in reverse, with the M2M cloud provider selling directly into end-users while reselling the necessary telecom services. These reciprocal business models are expected to become commonplace as we enter the connected world.



In the future, the operations of telecom service providers are expected, to some degree, to move to a model where network functions and support systems will no longer reside physically within the operators' domain. Rather, geographically spread access networks will be built and parts of the network functionality and service intelligence could be consumed on a pay-per-use or pay-as-yougrow basis from geographically-independent third-party providers.



CHAPTER - 8

Cloud Storage With Blockchain Technology

Everywhere we turn these days “the cloud” is being talked about. While “the Cloud” is just a metaphor, Cloud computing is what people are really talking about. Now is the right time to say the future application stays in cloud. Many of the enterprise applications and customer’s demands are mostly serviced from cloud computing technologies. Cloud service providers like Dell EMC and Amazon are attracted to cloud-based services considered superior to traditional data centers in terms of cost and technical dimensions. However, unlike any other storage technology it has its own drawbacks, security being the most common of them all.

Moving business data to the cloud means that the responsibility of data security becomes shared with the cloud provider. The overlapping of trust boundaries and increased exposure of data can provide malicious cloud consumers with greater opportunities to attack IT resources and steal or damage business data. The answer to this challenge in cloud security can be tackled by the use of a “Distributed cloud model” using blockchain technology. Blockchain is a hot topic and many are looking for new, secure, cost-efficient methods to store their ever growing data libraries.

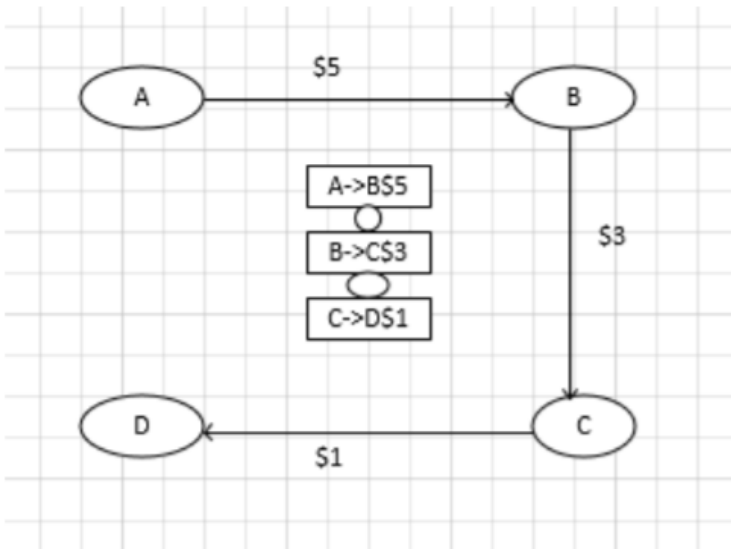
Originally devised for the digital currency, Bitcoin, blockchain eliminates the need for trusted third parties. Additionally, blockchain database isn’t stored in any single location. This creates a transparent, traceable peer to peer system that’s almost impossible to hack.

A traditional cloud storage model consists of a front end platform which could be a client or a mobile device, a back end platform which could be a server or storage and a network, possibly internet or an intranet. Google

Drive is a typical example of traditional cloud storage. When you upload data to the cloud, Google stores it in one of their datacenters. When you want to access the data from a mobile device/laptop, a request is sent to the data center and you can access your data.

Running vast data centers are expensive. The tech in these data centers need to be refreshed on a regular basis. Moreover, there are operational costs because of cooling, maintenance and updates. Safety is another aspect to consider. All cloud service providers have strict safety processes in place but there is always room to penetrate and gain access to confidential data. The recent iCloud hack of celebrities was one such occurrence. And it isn't just human error that puts your privacy in danger. Large companies have the ability to search non-encrypted files. Their privacy terms outline a lot of different scenarios where they can legally access and share your data.

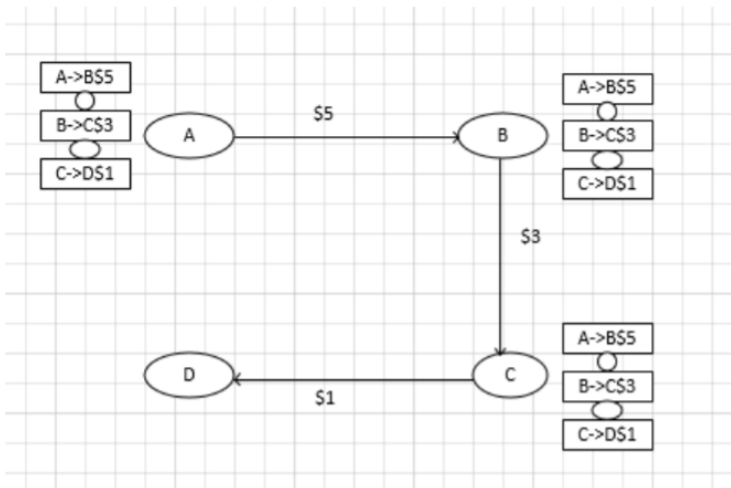
Blockchain technology is not new; rather, it is a combination of proven technologies applied in a new way. It is the combination of the internet, private key cryptography and distributed open ledger protocol. Let use an example to explain Blockchain in simple terms. Suppose there are four entities/nodes A, B, C and D and they want to transfer a certain amount to each other. Let us assume A has \$10 and A transfers \$5 to B and B transfers \$3 to C and C transfers \$1 to D.



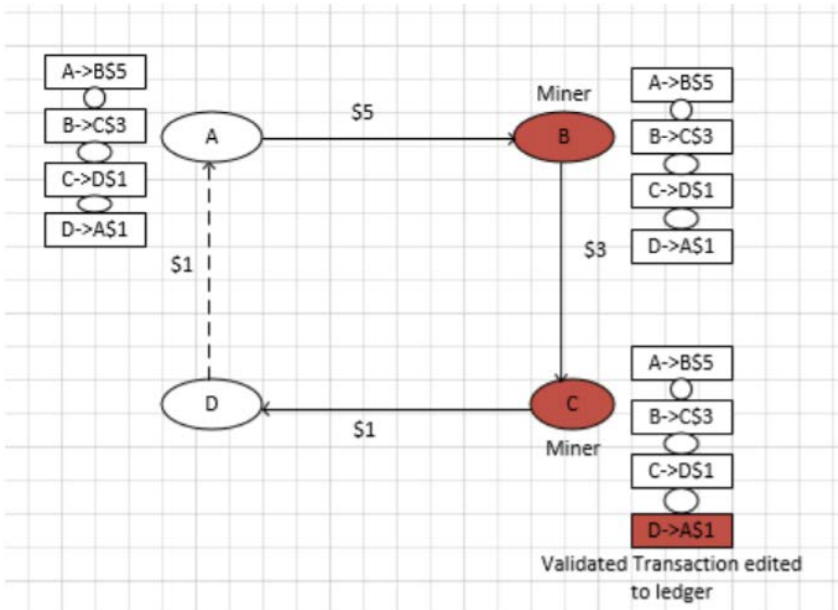
All these transactions are recorded centrally and linked to each other and all the entities are aware of these transactions. The record where all the transactions are stored is called a “ledger” and the protocol described above is an open ledger protocol. All the entities are aware of each transaction and it is verifiable. In case D wants \$15 from A, A cannot transfer this amount since it is only left with \$5 and all the other entities are aware of the same. Blockchain uses a same approach with the only difference being that the data, i.e. transactions, are not centrally recorded but each entity will have a copy of the transactions.

By storing data across its network, the blockchain eliminates the risks that come with data being held centrally. Blockchain security methods include use of public-key cryptography. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to the data. This is where blockchain has its advantage.

Decentralized data is transparent to everyone involved. Every node in a decentralized system has a copy of the blockchain. Transactions are broadcast to the network using software. Mining nodes validate transactions, add them to the block they are building, and then broadcast the completed block to other nodes. This also maintains sync between the different copies of data that various nodes are holding onto.



Suppose D wants to transfer \$1 to A. D encrypts the data with a public key and sends it to A which has the private key to decrypt and access the data. A broadcast message regarding this transaction will be sent to the network. In a blockchain network there will be certain special nodes called “miners” which can validate a transaction. Assuming C and B are the miners they will try to validate the transaction from D to A. In this case validation can be done using two points.



If D has the funds to do this transaction Decrypting the public key Since all the nodes in this network have a copy of the previous transactions, both C and B are aware that D has the funds to carry this transaction. Decrypting the public key however is not simple; a miner repeatedly generates keys and tries to guess the correct key until it finds one. If C finds the key that matches the key for this transaction it validates this transaction and edits it to its own ledger. All the remaining nodes will do the same since this transaction is already validated.

Distributed cloud storage is envisioned where all aspects of cloud storage such as transport, processing, or storage of data are entered into the blockchain. Later, what happens to the data can be verified by anyone who

has the access to the blockchain. Such a system provides complete traceability, accountability, and transparency to the cloud.

Distributed Cloud model enables users to store data in a secure and decentralized manner. This is done by using blockchain features such as ledgers, public/private key encryption, and so forth which we discussed earlier in this paper. These features are putting the user back in control over their data and devices. The decentralized aspect ensures there are no central servers to be compromised

To design a high performance distributed cloud architecture that meets both current and future challenges, the following principles should be taken into consideration:

Resilience: Even if some nodes fail, computation continues on other nodes.

Efficiency: The users receive excellent performance even if the nodes involved are heterogeneous.

Ease of deployment: The nodes can be deployed in any configuration without disrupting the other nodes.

Adaptability: The architecture of the network should be able to adapt to the changing environment and broaden its use to meet the increasing needs and demands of customers.

Performance: Linear performance is always needed in a distributed network. **Security:** Data protection, confidentiality and information security must be adequately addressed.

Distributed Blockchain Cloud Architecture The proposed model consists of the following four steps:

1. **Selection of Resource:** The cloud user must select the resource provider from the service provider pool in the blockchain base distributed cloud.
2. **Provision services:** The selected service provider will provide required services, such as data management, task execution and the provision of servers to that user.

3. Registration of services: After providing the requested services, the service provider registers the transaction in the form of blockchain and shares it with all distributed peer service providers.
4. Payment: The user will pay and reward the service provider and all the peers will copy this transaction/movement in their own blockchain. This is a trusted peer-to-peer network maintaining a distributed ledger that consists of validating nodes/miners that update the ledger and respond to requests. Requests can be invoked through client SDKs or REST API calls. Multiple peers endorse/sign the results, which are then verified and sent to the ordering service. After consensus is reached on the order, results are grouped into cryptographically secured, tamper-proof data blocks and sent to peer nodes to be validated and appended to the ledger.

Members can be added rapidly to the Blockchain network whether they are next door or across the world. Once their instance is provisioned they can join the blockchain by exchanging digital certificates and securely conduct data transactions with their peers. Not all business data exchanged between members is suitable for sharing with all participants. In such an environment we can isolate peers into subnets and create private ledgers. Blockchain members can then conduct private and confidential transactions while coexisting with members on the same blockchain. Peers can only join the chain when approved by other organization on that chain. Client requests are routed to a specified channel and once endorsed, the results are updated in that channel's ledger, which is only accessible to its member peer nodes.

Types of Blockchain networks

1. Consortium blockchains: In a consortium blockchain, the consensus process is controlled by a pre-selected group such as a group of corporation. The right to read the blockchain and submit transactions to it may be public or restricted to participants. Consortium blockchains are considered to be "permissioned blockchains" and are best suited for use in business.
2. Semi-private blockchains: Semi private blockchains are run by a single company that grants access to any user who satisfies pre-

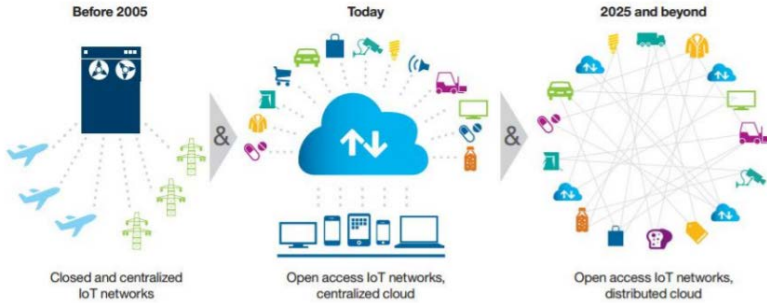
established criteria. Although not truly decentralized, this type of permissioned blockchain is an appealing option for government applications.

3. Private blockchains: Private blockchains are controlled by a single organization that determines who can read it and participate in the consensus process. Since they are 100 percent centralized they are only useful as sandbox environments but not for actual production.
4. Public blockchains: Anyone can read a public blockchain and participate in the consensus process. They are considered to be “permission-less”. Every transaction is public and users can remain anonymous. Bitcoin and Ethereum are prominent examples of public blockchains.

Benefits

1. Full Decentralization and true redundancy: Using blockchain, we can build a cloud storage where data is stored in dozens of discrete nodes intelligently disbursed across the globe.
2. Transparency: Information in blockchains is viewable by all participants and cannot be altered. This reduces risk and fraud and creates trust.
3. Security: The distributed nature of blockchain means it is almost impossible to hack.
4. Fewer Intermediaries: Blockchain is true peer-to-peer network that reduces reliance on third parties like banks, brokers, gateway, etc.
5. Automation: Blockchain is also programmable – which make it possible to automatically trigger actions or events once the conditions are met.
6. Faster Processes: Blockchain can speed up process execution in multi-party scenarios – and allow faster transactions that aren’t limited by office hours.

Distributed Cloud Use Cases



7. Network applications/NFV: The NFV evolution has made it possible to distribute virtual network functions (VNFs) in a more flexible way. The infrastructure for NFV is an important starting point for the distributed cloud evolution. Distributed Cloud infrastructure enables intelligent placement of VNFs, mobile cores and RAN functions.
8. Content delivery Networks: Content delivery solutions have been run as applications on generic computing and storage platforms. This means these platforms must support distribution across regional and hub sites as well as across multiple service providers. A decentralized architecture provides better response time as well as efficiency in transport and peering costs.
9. Data storage with regulatory compliance: Enterprises are increasingly using cloud service providers for scalable storage of various data sets where security and regulatory constraints are major concerns. A decentralized architecture enables compliance with regulations and ensures control of cost and policy with regards to the cloud service providers.
10. Hybrid enterprise cloud: Enterprises that want to use cloud service providers for elasticity and scalability reasons, but also want to control where applications are executed. A cloud platform can be deployed across on-premises and cloud resources such that applications and data can be placed according to policy and performance constraints and intents.

11. IoT and data stream processing: Applications that collect and process data are often composed of several parts that include components for data collection, data throttling, data pruning, anomaly detection and storage. We can improve the improve scalability and performance by placing these components at an optimal location in the network which in turn will lead to better response times and efficient transport and peering costs.

8.1 Integrating Block Chain Security Features In Cloud Computing

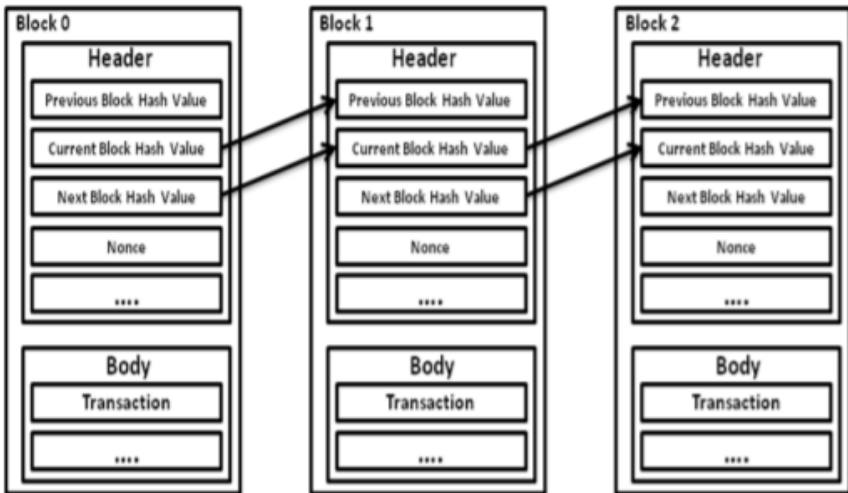
In blockchain all the peers or users needs to maintain a ledger which consists all the transactional data and also update the ledgers in order to ensure integrity whenever there is a new transactions. To verify the reliability of every transaction, encryption technique is used by all the peers present in the blockchain network. Hence the dependency of third party and single point failure is resolved. Broker free is one of the key characteristics of blockchain thereby removing unnecessary fees that is caused by the involvement of third party authority as in cloud and the information of all the transactions are known to each and every peer present in the network.

This makes difficulty for the attacker to hack the data, which in turn reduces the security expenses. Here all the transactions are recorded, verified automatically by huge participation, by using an open source the system can easily been implemented and connected, Hence all the records can be openly accessed by the public which in turn reduces the regulatory or third party costs. The blockchain is organized in such a way that it stores data in a way which is similar to that of distributed database and also structured in such a way that making arbitrary manipulations is very difficult.

Since all the members have a copy of each transactions and verify each block in blockchain, here each block contains a header and body. Each block contains hash value of the previous block along with the header of current block and index keys are used to search a block in the blockchain. The hash values which are stored in the block of each peer are affected because of previous blocks and hence it makes difficult to alter or delete the registered data block by the hacker. Hacking the data block can

only be done if 51% of peers are attacked simultaneously at a time, and this kind of situation is very difficult in reality. Blockchain technology uses public key for verification purpose using a hash function, which is used for both encryption and decryption process in ensure security for the data block. Here ECDSA (Elliptic Curve Digital Signature)

By using public key as users account information, enables peers to know who has sent and how much to other peer. There is no way for accessing data regarding the peers in the network. In bitcoin transaction, hash function is used to check the integrity of each data block which contains transactional details and this is done by verifying the transaction by using hash value for public key encryption. Using root hash value of each transaction, we can check if the weather bitcoin data is altered or not .

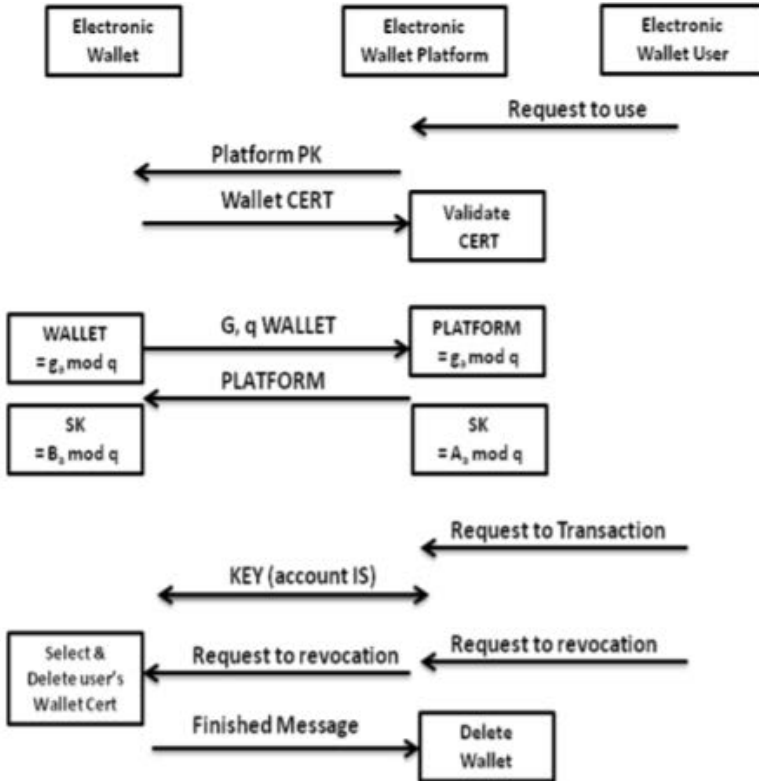


Many researchers is going on to strengthening the security characteristics of blockchain and blockchain focus mainly on providing security for public keys of peers which is used during the transaction i.e. during encryption and decryption process. When an attacker uses “reuse attack” in order to get the personal key which is stored in peer’s device, that can be used for hacking the bitcoin. Once the personal key is obtained, then the attacker can hack the bitcoin if there is leakage in data. Bitcoin is vulnerable, since the malware infection can be done because the trade is done on client’s personal computer or Smartphones. The applications, emails which are less secure must be detected and well trained in order to stop infection of peer’s device, such type of technique can be done in game

environments . The biggest strength of blockchain is that it is very difficult to modify the transaction ledgers, since many peers will share the same ledger. If the attacker modifies 51% of all the peers' ledger, then he can access the data block and this problem can be solved by performing intermediate verification that has to be designed to solve this problem.

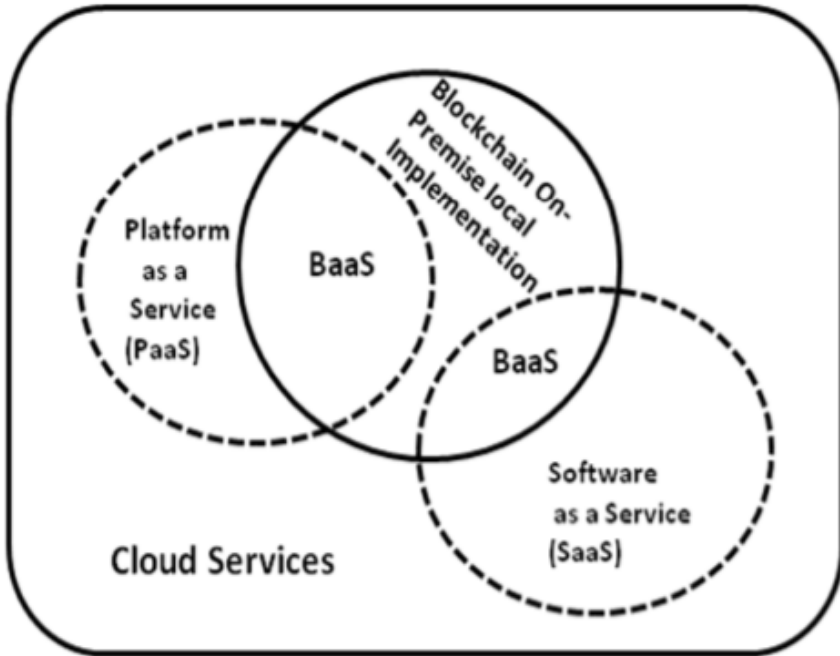
In cloud computing the main focus is on how to provide security for the data during transmission and at rest. To provide strong security service, the combination of blockchain and cloud computing can be helpful. Before the user stores his sensitive information on to the cloud, the anonymity can be checked if blockchain technology is adopted and this is done by installing digital wallet. In this process if the digital wallet is not handled properly, then user's sensitive information can be leaked. In other words the security of blockchain is affected if the sensitive data is leaked in cloud environment, which damages the monetary aspects of blockchain.

To solve this problem, a solution has been proposed which installs and deletes the digital wallet safely. There are few other issues, such as falsifying the transaction ledger or double transaction. Since most of the users use mobile devices, the verification of these devices has to be done. The accuracy and integrity of the timestamp is obtained only when the transaction is guaranteed . The core technology of blockchain must be verified properly, since the vulnerabilities changes from one programming language to another, versions used by peers and also the platform which is used for deployment of digital wallets. The wallet must be implemented securely in order to minimize the verification problems that are occurred during planning, analysis, requirements, quality of service and maintenance



It is a mechanism of hosting all the features of blockchain in cloud computing environment. BaaS allows the peer to create an application, distributed ledger, platform and also security for the data. Thus BaaS helps to deploy blockchain services and core features on to the cloud computing environment, which can be used by developers.

The fundamental technique of BaaS is as same as Software-as-a-Service (SaaS) and the functionality of BaaS can be either PaaS explicitly or SaaS implicitly which may vary based on the type of cloud computing environment been used to access user data, it can be only partial data which does not provide entire information.



All companies that are keen to invest in blockchain technology need to first perform a strategic evaluation to see if it is feasible for their enterprise business model. Thus, it is suggested that companies carry out granular tests on the use-case level to decide which software may be brought on with blockchain technology. A proper strategic technique is needed in order to use blockchain effectively.

For cloud consumers, cloud technology is used as a convenience concept. Cloud subscribers may browse, share and exchange data from everywhere, at any moment, depending on their location. Data functional units continue to face difficulties as they serve a variety of economic sectors in the construction of the next-age digital payments for the effective utilization of network functionality and user interaction. Blockchain technology was developed to cope with economic security. It is a type of shared record service that enables more secure digital purchasing.

The verification procedure is mostly used in the digital ledger process when the consumer makes digital operations. To communicate the most recent activity information block, each component is revised regularly and represented in the computerized funds' transfer information.

The majority of endpoints in blockchain systems are controlled by various organizations. The units are connected based on the database information.

The system's efficiency is harmed as a result of the node consensus concern. The blockchain accepts activity proposals from users to execute the activity under which it was created. Two or even more public blockchains keep a transaction history that will not be changed or destroyed as a consequence of the contract's implementation. The blockchain's preservation is accomplished through this method.

The innovative premise of e-Cash is causing a major transformation of e-commerce. It simply changes the entire systems' paperwork and currency. Another of the greatest e-cash methods is the payment system using credit cards. This technology necessitates a secure space for traders and intermediaries. The E-cash is stored by the financial institution or provider, and the customer must seek it throughout the transaction process. Physical e-cash, unlike digital cash, is stored by the customer in a device including a contactless card or other forms of a chip. Every approach may be categorized as detectable or unverified.

By recognized application, one means that each activity requires final quality assurance, perhaps from a banker. This method is safer since it encrypts and authenticates the E-cash communication using cryptography and electronic signings, accordingly.

Access management:

It is a type of technology that helps to protect the information that is kept. Concerning the knowledge, operations, and analytical processes, the assets are significant. The organization should have various access privileges in an attempt to build a trustworthy setting. For various causes, some circumstances need the exchange of accessibility privileges from one person to the next. A person might, for example, give his or her login rights to some other member. Likewise, an institution's operator who wants to execute a needed calculation on a Cloud Infrastructure delegated the work to some other worker who requires connection to the equivalent system.

Techniques for incorporating blockchain with cloud services include:

Connecting smart contracts with the cloud to simplify corporate connections such as archiving, backup, and commercial information

availability. Incorporating protection ideas into cloud projects, customer, and database administration.

In cryptocurrency systems, the volume of operations is tremendous. In a fluid setting, the fundamental purpose of cloud platforms is flexibility and adaptability.

In the interest of protection: The information is concealed from the client and kept in storage centers. As a result, operational tasks must be allocated with adjusting goals in mind. It indicates that the public cloud gives consumers freedom over where their content is kept and analyzed.

If a component in the system malfunctions, the network is supposed to identify another node. As a result, there is a nodal duplication strategy in computer servers, as well as the usage of various application programs.

Cryptocurrency safety advancements: In a decentralized cloud system with various computing programs, software must be assigned consistently.

Ledger technology has lately become a prominent monetary system that allows for a range of Data Processing Elements to be used in digital payment processes. The major goal of this unified program is to guarantee and improve the communication server and the client's trustworthiness.



CHAPTER - 9

Applications Of Cloud Computing

In cloud computing, software serves as a service (SaaS), platform serves as a service (PaaS), and infrastructure also serves as a service provider (IaaS); which extends cloud computing to a variety of service models and corresponding service providers. Due to the diverse patterns of the cloud computing services, IT companies use it at different levels based on their own advantages resulting to the formation of crowded situation.

IaaS provides customers with rental processing, storage, networking and other basic computing resources that users can deploy and run on any software, including operating systems and applications. Customers do not manage or control the underlying cloud computing infrastructure, but can control the operating system, storage, and deployment of the application. It is possible to select the network components (such as firewall and load balancer). For example, Amazon's AWS and at&t's Syntactic.

PaaS provides customers with the ability to deploy applications created by customers with the development language and tools provided by the vendor to the cloud computing infrastructure. Customers do not need to manage or control the underlying cloud infrastructure, but can control the deployment of applications. Customers may also control the hosting configuration of the application. For example, Google's App Engine platform, Salesforce's force.com platform, Facebook's F8 platform, and Microsoft's Azure platform.

SaaS is the service provider running on the cloud computing infrastructure applications and is able to be in a variety of client devices through the thin client interface access, such as the browser. Customers do not need to manage or control the underlying cloud computing infrastructure, requiring only a limited number of customer-configurable configurations.

For example, Microsoft's Office live, Google's online documentation services and Salesforce's online customer management software.

At present, the technology of IaaS and SaaS is relatively mature and has certain commercial cases abroad, but the overall market potential remains to be maximized. PaaS technology has not matured. The cloud computing vendor platforms are not compatible, using proprietary data formats and API (Application Programming Interface, application programming interface), and it is difficult for users to switch from one platform to another. From the analysis of development in cloud computing industry, it is predicted that China will be the cloud computing service provider for IDC service providers, traditional IT vendors, and internet companies. With the continuous integration of telecommunications and the Internet, cloud computing will have a significant impact on the traditional telecommunications industry. On the one hand, the traditional IDC (Internet Data Center) has been unable to meet the development requirements. To ride this new wave of computing, as a long-term plan, telecom operators has build multi-network integration and cloud computing trends have become obvious.

On the other hand, the trend of internet development is leaning towards high-speed and large amounts of data. Cloud computing lowers cost and improves resource utilization, making the internet into a 'high-speed and large data' era. In addition, the internet terminal has changed from desktop, to laptop, notebook, Tablet PC and smart phones. The aroused problem is the decline of storage capacity and mobile operators have effectively use cloud computing to solve this problem.

Cloud computing is an internet-based computing which shares hardware and software resources and information can

be provided to the computer and other equipments. The whole operation is much like the grid.

Cloud computing will be the next major change since the big change to client-server in the 1980s. Users no longer need to understand the details of the infrastructure, does not require the professional expertise and does not need direct control.

Cloud computing describes an Internet-based new addition in IT services, usage and delivery model that typically involves the use of the Internet to provide dynamically scalable and often virtualized resources. Cloud is actually a metaphor of the Internet. As cloud is previously often used to represent the telecommunications network, it is later also used to represent the internet and the underlying infrastructure. Typical cloud computing providers often provide common network business applications that can be accessed through software such as a browser or other Web services, while software and data are stored on the server. Among the key elements of cloud computing, it also includes a personalized user experience.

Cloud computing can be considered to include the following levels of services: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Cloud computing services typically provide a common online business application that is accessed through a browser, and software and data can be stored in the data center.

There is a certain similarity between cloud computing and nature's cloud and water cycle, which made 'cloud' a fairly appropriate metaphor. According to the American National Institute of Standards and Technology, cloud computing services should have the following characteristics

- Able to access any network device anytime, anywhere.
- Sharing of resource pool by multiple users.
- Flexibility in quick re-deploying.
- Services that can be monitored and measured.
- Quickly deploy resources or get services based on virtualization technology.
- Reduce the processing burden on the user terminal.
- Reduced user reliance on IT expertise.
- Agility enables users to quickly and easily acquire technical resources at low prices.
- Accessibility of the application interface (API) refers to the ability to allow software to interact with the cloud in a way that is consistent

with the 'human-computer interaction'. Cloud computing systems typically use APIs based on Representational State Transfer (REST) network architecture. In the transmission mode of the public cloud, support has been transformed into operating costs, so the cost has dropped significantly. It is clear that the entry into the hurdle is due to the fact that the architecture is typically provided by a third party and does not require a one-time purchase and does not have the pressure of a rare centralized computing task. The principle of general computing based on computational resource packs is implemented internally on a fine grained basis based on user actions and less IT skills.

- Device and local dependencies allow users to access resources through a web browser without having to worry about what devices they are using, or where to access resources (such as PCs, mobile devices, and so on). Often facilities are in a non-local (typically provided by a third party) and are accessed via the Internet, and the user can connect from anywhere.
- A software architecture technology called multi-tenant allows resources and consumption to be shared under a multi-user pool: The centralization of the architecture makes local consumption less (e.g. real estate, electricity, etc.). Peak load capacity increases (users do not need to build the highest possible load level). The original utilization rate of only 10-20% of the system efficiency increased.
- Improved reliability if multiple redundant sites are used, which allows us to design cloud computing to meet business consistency and disaster recovery.
- Extend the resources according to reasonable granularity, close to real-time self-service, without the need for the user to construct the peak load.
- Performance is monitored, and consistency and loosely coupled architectures are built through web services as a system interface. Because the data is centralized, security is improved and resources concerning to security is increased. However, loss of specific sensitive data will continue to be of concern and there is lack

of concern towards the core storage. Compared with the traditional system, the security requirements are higher. Part of the reason is that the provider can focus on the security solution that the user can not provide. However, when the 'data is distributed over a wider range and to a larger number of devices' and the 'multi-terminal system used by unrelated multiple users', the complexity of security is greatly increased. It is not possible for a user to obtain a security audit log. Part of the development of the private cloud is derived from the customer's control of the equipment and to avoid loss of safety information. Maintenance of cloud computing applications is very simple because it is clear that users no longer need to install on the device. Once the changes have reached the user, the maintenance will be easier to support and improve.

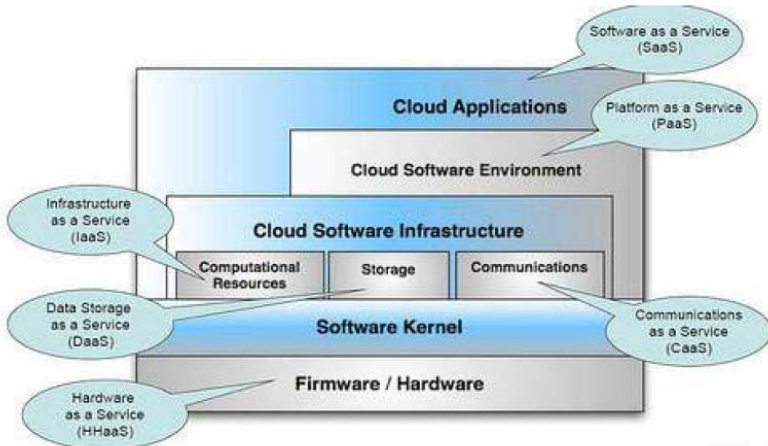
Cloud computing can be considered to include the following levels of services: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

Infrastructure-as-a-Service (IaaS):

Infrastructure-as-a-Service (IaaS) is a service. Consumers can access services from a complete computer infrastructure over the Internet.

Platform as a Service

Platform-as-a-Service (PaaS) refers to the software development platform as a service to SaaS model submitted to the user. Therefore, PaaS is also an application of the SaaS model. However, the emergence of PaaS can accelerate the development of SaaS, especially to speed up the development of SaaS application speed.



Software as a Service:

Software-as-a-Service (SaaS) is a way to provide software through the Internet. Users do not need to buy software, but to rent Web-based software from the provider to manage business activities.

Cloud computing is so fast to develop, and there is a continuous heat because of its clear business model.

Firstly, cloud computing reduces the absolute cost, allowing users to share resources and reduce waste, thus maximizing resource utilization.

Secondly, through cloud computing, companies can have the flexibility to acquire the corresponding services and get more agile service.

Thirdly, cloud computing has changed the structure of IT industry. When communications are conducted inside into the cloud, it has a great impact to the IT department, and provides a higher service capacity to the operators.

In foreign countries, in addition to providing ISP network services to the public, Orange, O2 and other large telecommunications companies also serve as a 'cloud computing' service providers. These companies provide IDC equipment rental and SAAS product application services to different industries. Through their innovative products to improve services and provide a strong boost to the rapid development and growth of public clouds. Therefore, in the future, the domestic telecom enterprises will become one of the main beneficiaries of the cloud computing industry,

receiving large revenues from various types of paid services, achieving profit growth, building their own brand of cloud service system through the analysis of user needs from different domestic industry and cloud computing service provider research and development.

International telecom operators	Local telecom operators
Focus on IaaS solutions and communications collaboration SaaS solutions; an addition to the existing business, and gradually expand into a strategic business, but has not yet formed a large-scale business and customer base	Mainly focus in the promotion of cloud computing technology applications within the country, such as the business counters and call center desktop cloud; external planning to the cloud based on the direction of the development of IDC is currently a small pilot, yet to have large-scale commercial

In the field of telecommunications applications, cloud computing should be 'even more powerful'. Traditional telecommunications industry re-established; operators who obtain the 3G license have the ability to develop integrated information services. Foreign large-scale telecom operators have already started the cloud computing construction work, and have achieved initial success.

Focus on IaaS solutions and communications collaboration SaaS solutions; an addition to the existing business, and gradually expand into a strategic business, but has not yet formed a large-scale business and customer base Mainly focus in the promotion of cloud computing technology applications within the country, such as the business counters and call center desktop cloud; external planning to the cloud based on the direction of the development of IDC is currently a small pilot, yet to have large-scale commercial.

Analysis of disadvantages of telecom operators to develop cloud computing

- a. With resources such as Internet access, IDC (Internet Data Center), mobile communication networks and WiFi hotspots, these resources are the most basic resource for cloud computing development, on which telecom operators can create more attractive ICTs (Information Communication Technology) service portfolio.

- b. Take full advantage of its global backbone network for cloud computing to provide safe and reliable network access services, which ensure end-to-end SLA (Service-Level Agreement).
- c. Has the experience of providing large-scale communication services to tens of millions of users. The billing mode is also paid by usage. These experiences can be directly reused to cloud computing services to ensure the reliability and performance of cloud computing services.
- d. The traditional IDC (Internet Data Center) business has been developed for decades, has accumulated a large enterprise customer base and has won their trust. These customers prefer the telecom operators to provide cloud computing services.

Analysis of disadvantages of telecom operators to develop cloud computing

- a. Cloud computing technology and professionals are less compared to internet companies such as Google and Amazon, and IT companies such as IBM and Microsoft. New research and development is lacking.
- b. Rather than being a core business, cloud computing acts as sub-business to traditional telecommunication business, leading to poor resources.
- c. Operating style is biased towards robustness and conservatism, less competitive in the rapid development of cloud computing field.
- d. The complexity of having a complex IT infrastructure including different vendors, different types of servers, storage and networking equipment, has increased the difficulty of building a cloud computing platform on this infrastructure.

For traditional telecommunications companies, its business scope is limited to telephone communications related business, and with the development of the Internet and the rapid progress of smart phones, people are no longer confined to home with a network cable to connect to the Internet. More people prefer to use the smart phone or 3G-enabled Tablet PC to surf the Internet. Due to the change to portability and trends of wireless and high-speed usage, the traditional business has long been unable to meet the needs of the users. Broaden of business scope is

necessary. Through cloud computing, businesses can be expanding to mobile internet, entertainment, shopping, payment, office and so on. Specifically:

1. Increased infrastructure coverage and upgrading of equipment to accommodate more high-speed users.
2. To develop own integrated information service system. Without it, business and operational capacity will greatly reduce.
3. Develop user resources. Users are the most important element in cloud computing. Through a long period of development, telecom operators have accumulated and cultivated a large user group. Their needs and user experiences cannot be ignored. When combined with cloud computing, this user group will be even larger. It is an important matter to develop and establish the telecom operator within this large user base.
4. To strengthen the ability to integrate the Internet. For Internet and IT companies, the ability of operators to integrate the Internet is too weak. Technology and talent must be introduced. The application of cloud computing can only be achievable with the ability to integrate the internet.

<p>Verizon</p>	<ul style="list-style-type: none"> • sees cloud computing as part of IT's evolution to Everything as a Service • sees cloud computing as natural evolution of its Managed Hosting business • Emphasize that cloud computing is the service's 'delivery engine' • Targeting itself as a major global provider of managed security services 	<ul style="list-style-type: none"> • 2008 - launched the first cloud computing service Synaptic Hosting • May 2009 - launched Synaptic Storage as a Service • November 2009 – launched Synaptic Compute as a Service. Payment according to usage, no fixed and minimum usage payment • 2011 – invested \$ 1 billion to provide cloud-based solutions for enterprise users based on global networks
<p>BT</p>	<ul style="list-style-type: none"> • sees cloud computing as a key driver of enterprise product strategy • Cloud computing is divided into three areas: IaaS, SaaS, CaaS (Communication as a Service) • View CaaS as a cloud service built around real-time communications (such as voice, video, web conferencing, instant messaging, etc.) • Think of the network as a key factor in delivering enterprise-class cloud computing services • Provide enterprise-class cloud computing services for end-to-end performance and availability 	<ul style="list-style-type: none"> • 2009 agreement with Microsoft to launch Microsoft's online business for business customers, providing cloud computing and collaborative communications services to customers • Provision of managed IP PBX and Unified Communications services in Europe and the United States using the Cisco HUCS multi-tenant platform
<p>Orange</p>	<ul style="list-style-type: none"> • Positions itself as an IT operator as an extension of the network operator • Packaging network services and cloud computing services as end-to-end hosted services, providing a single computing resource provisioning portal, a single help desk, and a single end-to-end SLA • Divide the cloud into four components: IaaS, SaaS, Collaboration as a Service, Security as a Service • Plan to integrate voice, video 	<ul style="list-style-type: none"> • Launch of SaaS solution in 2008 IT Plan, for the SME market, is based on a monthly fee of 3 per user per month, and the solution provides Office productivity applications, mail applications and business applications (SAP, Sage, etc.) • In 2009, IaaS solutions were launched for flexible computing, upgraded in 2010, plus self-service portal and customer management capabilities, which are paid for usage

<p>T-Systems</p>	<p>and end-to-end availability as the core competencies of cloud computing, building yourself as a trusted cloud computing service provider</p> <ul style="list-style-type: none"> • Standardize the various components of the cloud computing data center (server, storage, network equipment and software), automate the operation and management of the cloud computing data center, optimize the cost structure of the cloud computing data center, and gradually enrich the functions of the cloud computing platform • Collaborate with industry leaders to create industry cloud solutions and actively participate in industry cloud standards • Reduce IT costs and dynamic IT resource management through cloud computing • Build energy-efficient green data centers through cloud computing technology • Build a vendor-independent cloud computing solution 	<ul style="list-style-type: none"> • Started operations in 2004 IaaS cloud computing platform AppCom, providing virtual servers, storage, shared firewalls and virtual local area networks, etc. • Hosting databases, middleware, SAP, and other standard applications for enterprise clients on their own AppCom cloud computing platform • Launch managed workbench service, based on cloud computing data center for mission-based workers, knowledge workers and mobile workers to provide managed workstations • Introduces unified communications services based on cloud computing, including services such as voice and video conferencing, instant messaging • Cloud computing consulting services, including cloud-ready assessment, migration of traditional IT models to cloud computing models and system integration, optimization of cloud computing models • More than a dozen cloud computing data centers in Europe, North America, South
------------------	---	---

In biology, ecosystem is a great concept, and it is same in the case of internet and telecommunications. A scattered operation is unable to form a good climate for the cloud to develop. More and more enterprises especially Internet companies have begun to notice the concept of the migration of ecosystems. Platform construction is a long-term planning and investment, and once the platform is built, it will have its own vitality in which the development of this platform will have more innovation and development. Telecom operators can cooperate with Internet business to complement each other. It is very important to create an ecosystem for today's multi-network integration in which it will provide enterprises and the overall industry considerable development and vitality.




Today, cloud computing development has just begun. Although there are risks for telecom operators to develop cloud computing, but by seizing the right opportunity and maximizing its use, great benefit will come. Firstly, it is recommended to accumulate experience and the introduction of talent and technology; Secondly, it is recommended to develop the more mature IaaS and SaaS technology to quickly involve in cloud computing field and gain experience. As for the yet to mature PaaS technology, strong development capability is needed and is associated to greater risks. Once again, it is recommended to invest in infrastructure construction and expand the physical area of service. Absorb application developers to provide a platform for the integration of information service. Finally, establish information cloud computing and telecommunications internet, and the ecosystem of the mobile integrated multi-network.



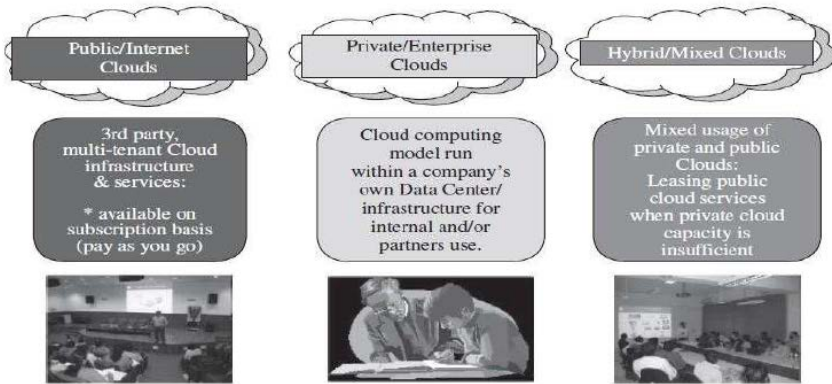
CHAPTER – 10

Data Security In Cloud SaaS (Software As A Service)

Traditional desktop applications such as word processing and spreadsheet can now be accessed as a service in the Web. This model of delivering applications, known as Software as a Service (SaaS), alleviates the burden of software maintenance for customers and simplifies development and testing for providers. Salesforce.com, which relies on the SaaS model, offers business productivity applications (CRM) that reside completely on their servers, allowing customers to customize and access applications on demand. Although cloud computing has emerged mainly from the appearance of public computing utilities, other deployment models, with variations in physical location and distribution, have been adopted. In this sense, regardless of its service class, a cloud can be classified as public, private, community, or hybrid based on model of Deployment.

Service Class	Main Access & Management Tool	Service content
 SaaS	Web Browser	Cloud Applications Social networks, Office suites, CRM, Video processing
 PaaS	Cloud Development Environment	Cloud Platform Programming languages, Frameworks, Mashups editors, Structured data
 IaaS	Virtual Infrastructure Manager	Cloud Infrastructure Compute Servers, Data Storage, Firewall, Load Balancer

Public cloud as a “cloud made available in a pay-as-you-go manner to the general public”. Private cloud as “internal data center of a business or other organization, not made available to the general public.” In most cases, establishing a private cloud means restructuring an existing infrastructure by adding virtualization and cloud-like interfaces. This allows users to interact with the local data center while experiencing the same advantages of public clouds, most notably self-service interface, privileged access to virtual servers, and per-usage metering and billing. A community cloud is “shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).” A hybrid cloud takes shape when a private cloud is supplemented with computing capacity from public clouds. The approach of temporarily renting capacity to handle spikes in load is known as “cloud-bursting”.



10.1 Data Security in Cloud Computing:

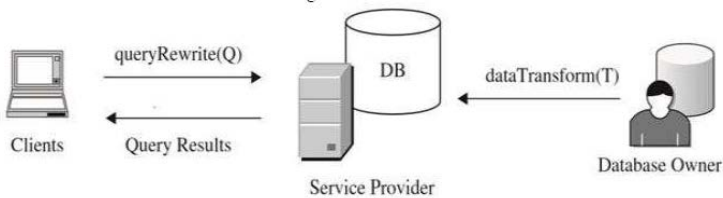
1. Data Security defines as Information in a cloud environment has much more dynamism and fluidity than information that is static on a desktop or in a network folder
2. Nature of cloud computing dictates that data are fluid objects, accessible from a multitude of nodes and geographic locations and, as such, must have a data security methodology that takes this into account while ensuring that this fluidity is not compromised.

3. The idea of content-centric or information-centric protection, being an inherent part of a data object is a development out of the idea of the “de-perimeterization” of the enterprise.
4. This idea was put forward by a group of Chief Information Officers (CIOs) who formed an organization called the Jericho Forum.

Unique issues of the cloud data storage platform from a few different perspectives

1. Database Outsourcing and Query Integrity Assurance

I. Storing data into and fetching data from devices and machines behind a cloud are essentially a novel form of database outsourcing



2. Data Integrity in Untrustworthy Storage

- I. The fear of losing data or data corruption
- II. Relieve the users’ fear by providing technologies that enable users to check the integrity of their data.

3. Web-Application-Based Security

- I. Once the dataset is stored remotely, a Web browser is one of the convenient approaches that end users can use to access their data on remote services.
- II. Web security plays a more important role for cloud computing

Multimedia Data Security:

1. With the development of high speed network technologies and large bandwidth connections, more and more multimedia data are being stored and shared in cyber space.
2. The security requirements for video, audio, pictures, or images are different from other applications

Digital Identity:

1. Digital identity holds the key to flexible data security within a cloud Environment.
2. A digital identity represents who we are and how we interact with others on-line.
3. Access, identity, and risk are three variables that can become inherently connected when applied to the security of data, because access and risk are directly proportional. As access increases, so then risk to the security of the data increases.
4. Access controlled by identifying the actor attempting the access is the most logical manner of performing this operation.
5. Ultimately, digital identity holds the key to securing data, if that digital identity can be programmatically linked to security policies controlling the post-access usage of data.

Identity, Reputation, and Trust:

1. Reputation is a real-world commodity; that is a basic requirement of human-to-human Relationships.
2. Our basic societal communication structure is built upon the idea of reputation and trust.
3. Reputation and its counter value, trust, is easily transferable to a digital realm:
4. EBay, for example, having partly built a successful business model on the strength of a ratings system, builds up the reputation of its buyers and sellers through successful (or unsuccessful) transactions.
5. These types of reputation systems can be extremely useful when used with a digital identity.
6. They can be used to associate varying levels of trust with that identity, which in turn can be used to define the level (granular variations) of security policy applied to data resources that the individual wishes to access.

User-Centric Identity:

1. Digital identities are a mechanism for identifying an individual, particularly within a cloud environment and identity ownership being placed upon the individual is known as user- centric identity.
2. It allows users to consent and control how their identity (and the individual identifiers making up the identity, the claims) is used.
3. This reversal of ownership away from centrally managed identity platforms (enterprise- centric) has many advantages.
4. This includes the potential to improve the privacy aspects of a digital identity, by giving an individual the ability to apply permission policies based on their identity and to control which aspects of that identity are divulged
5. An identity may be controllable by the end user, to the extent that the user can then decide what information is given to the party relying on the identity

Information Card:

1. Information cards permit a user to present to a Web site or other service (relying party) one or more claims, in the form of a software token, which may be used to uniquely identify that user.
2. They can be used in place of user name/ passwords, digital certificates, and other identification systems, when user identity needs to be established to control access to a Web site or other resource, or to permit digital signing.
3. Information cards are part of an identity meta-system consisting of:
 - A. Identity providers (IdP), who provision and manage information cards with specific claims, to users.
 - B. Users who own and utilize the cards to gain access to Web sites and other resources that support information cards.
4. An identity selector/service, which is a piece of software on the user's desktop or in the cloud that allows a user to select and manage their cards.

5. Relying parties. These are the applications, services & so on, that can use an information card to authenticate a person and to then authorize an action such as logging onto a Web site, accessing a document, signing content, and so on.
6. Each information card is associated with a set of claims which can be used to identify the user. These claims include identifiers such as name, email address post code.

Using Information Cards to Protect Data:

1. Information cards are built around a set of open standards devised by a consortium that includes Microsoft, IBM, Novell, and so on.
2. The original remit of the cards was to create a type of single sign on system for the Internet, to help users to move away from the need to remember multiple passwords.
3. However, the information card system can be used in many more ways.
4. Because an information card is a type of digital identity, it can be used in the same way that other digital identities can be used.
5. For example, an information card can be used to digitally sign data and content and to control access to data and content. One of the more sophisticated uses of an information card is the advantage given to the cards by way of the claims system.

Cloud Computing and Data Security Risk:

1. Cloud computing is a development that is meant to allow more open accessibility easier and improved data sharing.
2. Data are uploaded into a cloud and stored in a data center, for access by users from that data center; or in a more fully cloud-based model, the data themselves are created in the cloud and stored and accessed from the cloud (again via a data center).
3. The most obvious risk in this scenario is that associated with the storage of that data .A user uploading or creating cloud-based data include those data that are stored and maintained by a third-party cloud provider such as Google, Amazon, Microsoft, and so on.

This action has several risks associated with it:

- i. Firstly, it is necessary to protect the data during upload into the data center to ensure that the data do not get hijacked on the way into the database.
- ii. Secondly, it is necessary to store the data in the data center to ensure that they are encrypted at all times.
- iii. Thirdly, and perhaps less obvious, the access to those data need to be controlled; this control should also be applied to the hosting company, including the administrators of the data center.
- iv. In addition, an area often forgotten in the application of security to a data resource is the protection of that resource during its use.

Data security risks are compounded by the open nature of cloud computing.

1. Access control becomes a much more fundamental issue in cloud-based systems because of the accessibility of the data.
2. Information-centric access control (as opposed to access control lists) can help to balance improved accessibility with risk, by associating access rules with different data objects within an open and accessible platform, without losing the inherent usability of that platform
3. A further area of risk associated not only with cloud computing, but also with traditional network computing, is the use of content after access.
4. The risk is potentially higher in a cloud network, for the simple reason that the information is outside of your corporate walls.

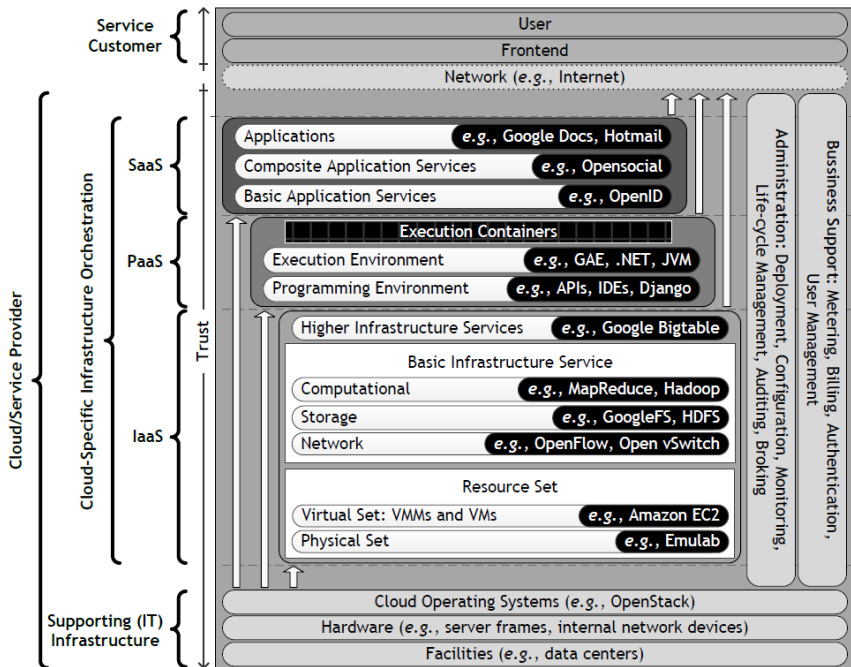
Data-centric mashups:

1. Cloud Computing perform business processes around data creation and dissemination by their very nature, can be used to hijack data, leaking sensitive information and/or affecting integrity of that data.
2. Cloud computing, more than any other form of digital communication technology, has created a need to ensure that protection is applied at the inception of the information, in a content centric manner, ensuring

that a security policy becomes an integral part of that data throughout its life cycle.

Encryption

1. It is a vital component of the protection policy, but further controls over the access of that data and on the use of the data must be met.
2. In the case of mashups, the controlling of access to data resources, can help to alleviate the security concerns by ensuring that mashup access is authenticated.
3. Linking security policies, as applied to the use of content, to the access control method offer a way of continuing protection of data, post access and throughout the life cycle; this type of data security philosophy must be incorporated into the use of cloud computing to alleviate security risks.



Physical security is established on-site throughout data center. Other security measures would be unnecessary if this prerequisite was not fulfilled. Data centers must be well secured (e.g., using a security center for managing video cameras and personnel entrances) in order to prevent

break-ins and other physical violations. Access to the massive computation servers, storage servers, and network equipments should be physically restricted, allowing only exclusive personnel with security clearance to perform managing operations. In fact, private identity cards assigned to each employee are many times used as means to open door locks and access certain areas of the facilities. Providers might also lay further security options to customers, though with a higher price associated. For instance, racks might be surrounded by cages with padlocks, to which the opening keys are kept with the customers. In addition, a weighting chamber might be installed before entering IT rooms so as to check the exit weight of the persons, who entered. This approach is useful to find out if any equipment was stolen inside.

The internal networks of cloud computing environments can be composed of service-driven networks, Storage Area Networks (SANs), and computational and storage-related hardware. Hence, as any other enterprise network, perimeter security must be deployed to analyze network traffic and safeguard data in transit. Network security approaches include firewalls and IPSes to prevent security incidents; IDSes to alert malicious intrusion attempts and honeypots to create distractions for attackers and therein learn their movements. Typically, a Security Operations Center (SOC) is established within the facility, monitoring and analyzing network health to detect pattern anomalies.

A Computer Security Incident Response Team (CSIRT) placed within the SOC collaborates with other CSIRTs around the globe to share intelligence and aid in security incidents if necessary. Security Information and Event Management (SIEM) solutions are mandatory in order to obtain a high-level perspective of the network security status. SIEM solutions correlate real-time events triggered by perimeter defenses and security agents setup in each node within the network to learn what is normal and abnormal behavior. Hewlett-Packard (HP) ArcSight is an example of a SIEM that performs event correlation. Security experts configure them in order to serve their alert requirements and purposes. Several SIEM platforms available in the market were compared by Author.

Various cloud IDS solutions are available nowadays. Author recommended IDS and IPS positioning in clouds to achieve the desired security in next generation networks, with particular attention to the trade-

off between security and performance, as discussed by Author in their state-of-the-art survey on IDS and IPS solutions.

Author conceptualized a four layered model that subsumes modern data centers. The bottom layer is composed of the physical infrastructure, which aggregates server farms to form clusters. Then, a virtual infrastructure layer is built upon it. This layer enables to run co-resident VMs that can be setup to serve virtual data centers. A single virtual data center can be rented to a single customer, giving the customer full control over the management of VMs. The third layer is called a virtual infrastructure coordination layer, whose purpose is to tie up virtual data centers and cross-geographic location deployment. This layer mounts scattered virtual data centers, which can then be configured to build distributed virtual data centers.

The last layer is for the service provider, which can be another entity involved in the cloud computing business or the very cloud provider. At the top of the model, applications run in a SaaS manner. Security matters should be regarded transversely to the whole model. According to GigaOM, a media company, the datacenter infrastructure now extends beyond the four walls of the data center. A new realm of data centers is emerging.

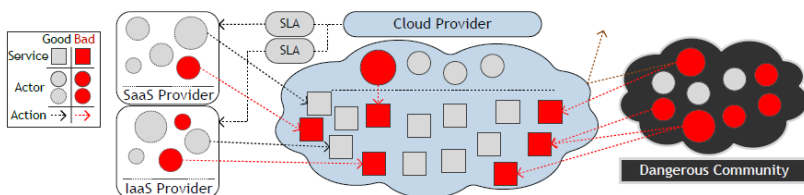
Nowadays, data centers are not just the machines, but are the data centers plus the network connecting them, further complicating the security requirements of clouds, and consequently of interclouds. For example, Google Spanner database, recently made public, syncs data across five data centers. Netflix, one of the biggest broadband traffic drivers, and Facebook, also operate this way. Author identified flooding attacks, hardware interruption, theft or modification, infrastructure misuse, and natural disasters as main issues to data center facilities. Note that the term flooding is related with the availability property when Denial of Service (DoS) states are achieved, therefore being part of a security requirement.

The cloud security model depicts the actors in the cloud business and operation. It is composed of the cloud infrastructure and the entities that manage and ultimately use it. Cloud providers own data centers, having all the responsibilities regarding the management of the resources they contain. On the other hand, cloud customers and end users rent services

from the cloud provider. An optional service provider can be included in the security model to represent the cases where cloud resources are rented to intermediate providers. This optional service provider is used in the model to enable the specification of what it is being rented. Additionally, SLAs are closed with providers so as to describe how services are executed and the terms of service. Typical SLAs include data exchange rates, mean time to repair, jitter and other service properties related with security as well . While bandwidth, storage or processing power are measurable parameters, security-related are non-quantitative properties, thus comprising an obstacle.

The cloud security model described so far is schematized , where it is possible to discriminate possible attack vectors. Dashed circles represent users that have closed SLAs with a service provider. In the model,two service providers are illustrated: one SaaS provider and one IaaS provider. Each provider is now able to sell services to end users. Also depicted, one supposedly normal user can turn and act maliciously without apparent suspicion, being more stealthier than others. In addition, a malicious employee with privileged access and knowledge of the cloud resources can do considerable damage. Finally, across the Internet, a potential dangerous community can scan for vulnerabilities and exploit them afterwards.

Other ways to get inside the cloud network include getting access to login credentials of honest customers. Each actor, good or bad, can have more or less knowledge of the cloud and can produce more or less impact, and be more bolder,hence the different circles and sizes used for actors.A noteworthy aspect is that, while cloud customers are responsible for application-level security, providers are delegated with physical and logical security responsibilities. Responsibility over problems on intermediate layers of the cloud stack are shared between the two entities. Cloud customers may, nonetheless, outsource their security responsibilities to third-parties who sell security related services.



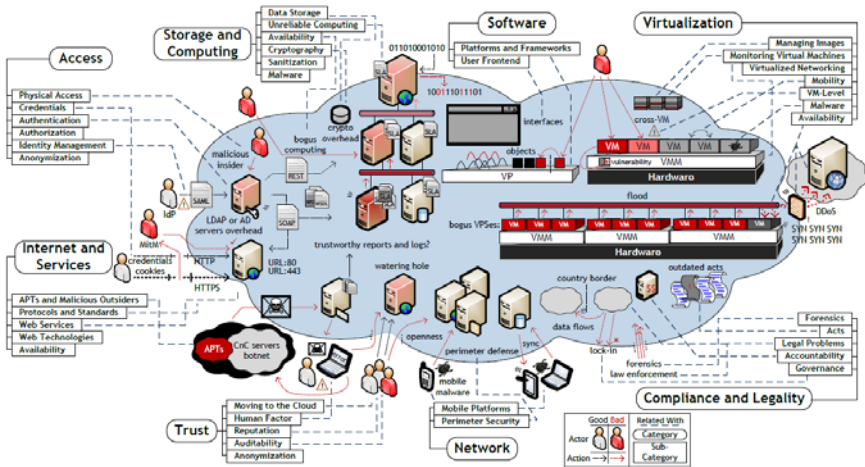
Cloud security covers numerous subjects. In order to understand them, the underlying concepts that might identify the source of vulnerabilities and threats must be introduced. This subsection analyzes those concepts, starting with an explanation on virtualization elements and then on multi-tenancy. Cloud software is also discussed, followed by the discussion of the concept of data outsourcing. Then, data storage security and standardization are reviewed, and the section ends with a discussion on trust.

Before presenting the taxonomy for cloud security issues, a brief introduction to the concept of security issue is given, so as to better elucidate when the various security terms are invoked throughout this article. A security issue is a general term to address something like an event or action, a software or hardware misconfiguration, or an application loophole—that is not as it supposedly should be in the context of security. The security community traditionally uses the terms vulnerability, threat, attack and risk to further specify what the issue is, therefore being important to understand their differences. So, vulnerability, or gap, is a flaw or weakness of a system, which can be compromised by a threat. The risk is the likelihood of a threat agent taking advantage of a vulnerability, in the form of an attack, and corresponding business impact.

Author clearly distinguished the difference between cloud-specific issues and general issues. Their study, which is based on sound definitions of risk factors and cloud computing, states that cloud-specific issues must be intrinsic or prevalent in a core technology; have their root cause in the essential characteristics proposed by the NIST; are caused when tried-and-tested security controls are difficult or impossible to implement; or are prevalent in established state-of-the-art cloud offerings. Author categorized cloud computing threats into multi-tenancy issues, account control, malicious insiders, management console security, and data control. Author discussed issues of four categories. The first category is cloud infrastructure, platform and hosted code. The second category is data, while the third is access. Finally, the fourth category is named compliance.

Author did not explicitly provide a taxonomy for cloud security issues, but those authors divide their work into six categories: authentication and authorization, virtualization, availability, accountability, storage, and

computation. Former studies, however, lack the higher level perspective of the security factors that affect cloud environments because they were also more focused. The taxonomy proposed in this article revolves around eight main categories: software, storage and computing, virtualization, Internet and services, network, access, trust, and compliance and legality. An illustration of the taxonomy allows the extraction of a mental picture of the security state in cloud environments and the identification of possible factors causing the cloud security fuzz.



Additionally, issues ranging from the Internet to the cloud enabled enterprise network, to the very front door of clouds are also included. This drill down allows to better understand the attack vectors existent for cloud systems. Finally, two more areas of security issues are included, which are more subjective than others because trust, compliance and legal problems may not be directly related with the technology deployed in the majority of the cases. Each category is divided into some sub-categories that further address specific issues. This structure other sub-categories to be added in the future, if necessary. Some issues are related with some of those sub-categories so as to better understand what the discussions in the next section are referring to. Note that the categories and sub-categories were chosen while not having in mind where they fall within the cloud service delivery models, but which security issues are included in each one. The categories were chosen so as to minimize overlap (in terms of having issues falling into more than

one category), while covering all impossible security issues that may affect clouds. Additionally, the order of the categories is not the same as here in presented.

The problem of outsourcing storage and computing responsibilities to a third-party is that customers do not know what happens within the cloud. Because customers do not have their data locally, a plethora of barriers arise. Author said that storage security has always been an important aspect of the Quality of Service (QoS). Hence, proper techniques and mechanisms are required to efficiently and reliably check data status in two scenarios: before and after being computed, and while being persistently stored. However, Author acknowledged that the main issue of such checking is to verify how frequently, efficiently and securely a storage server, or a group of servers, is faithfully storing customers outsourced data, which is always under the threat of being tampered with by insiders or outsiders. The discussion included below tackles security issues related with data storage, unreliable computing, availability, cryptography, sanitization, and malware

10.2 Cloud Security With Data Storage:

Data storage services, like Dropbox and Google Drive, opt to offer persistent hard storage plans for data. As it is discussed in, there is a cloud war going on between cloud providers. Prices are flattening due to the wide solutions available across several providers there is a competitive landscape out there. In the midst, some even offer bold solutions, such as free space on the cloud without nothing in return. Nevertheless, data is sent, viewed or edited remotely. These three fundamental actions drive where such storage providers are heading. A realm of online collaboration is required to achieve that objective. In fact, Box is a step forth to achieve that objective. However, such a model implies for document owners to delegate, to some extent, authorization permissions to other tenants, creating an even more dynamic environment.

However, the loss of control issue yielded by clouds makes it harder to check for data integrity and in such an environment. Customers are physically separated from their data, and consequently the cloud storage or computing servers, which customer have no control over them whatsoever. Moreover, the data is somewhere within the server pool, at an

unknown location. Because the virtualization layer abstracts resources above, this prevents pin-pointing the exact physical location (e.g., storage partition, network port, and switches involved) of the data at a certain moment in time. As a consequence, this unique issue makes it even harder to contain an incident, because isolating or tracking a compromised source implies finding it at forehand.

As discussed data centers are highly available by ensuring electrical source redundancy and efficient cooling. On top of that, clouds are elastic, meaning that resources are allocated and reused as fit proper. A third step in availability is data redundancy. This means that data is backed up to some other server, which is usually in another data center of the cloud provider. In case of a complete failure of one of the data centers, the data on other data center is still available. However, big players like Google and Amazon have data centers spread over different countries around the world.

This is a multi-location feature that can bring compliance and legal problems,as data travels across borders.Author pointed out that data integrity is preserved in a standalone database systemwhere Atomicity, Consistency, Isolation and Durability (ACID) properties are ensured and transactions between data sources must be handled correctly in a fail safe manner. Auditing is an adequate solution for checking the data state. But, it would not be fair to let one of the entities engaged in the storage agreement to conduct the auditing tasks,because neither of them could be assured to provide unbiased and honest auditing results . Additionally, customers may not have the time, willingness, resources, or feasibility to carry those duties. In such case,they may delegate such responsibility to an optional trusted third-party auditor.

10.3 Cloud Security In Unreliable Computing:

Author stated that many service applications fit within a pattern of behavior. Such service applications have the goal of implementing the frontend for SaaS applications, which arrive via web service or HyperText Markup Language (HTML) requests. That pattern is composed of a sessions state manager, other services that may be called upon, and cached reference data. As explained in the work, a service call tree is obtained when an application calls another service which, in turn, requests another

service, and so on and so forth. Therein, to meet a system-wide SLA, services down the tree are under enormous pressure to meet tight SLAs. Traditional SaaS applications have 300 millisecond response time for 99.9% of the total number of requests with a rate of 500 requests per second.

A top-down approach reveals ever-tighter SLAs constraints in the call stack, to which the bottom level is the most stringent. Therefore, any delay in one service node can have a snowball effect to services below. Such delay can be perpetrated by malicious agents, downtimes or slowdowns, which can result in dishonest computing. Moreover, data can be accidentally lost through administrator errors in backups, restores or even migrations. For instance, MapReduce, a computing framework for processing large datasets in distributing systems, may output dishonest, inaccurate computational results because of misconfigured or malicious servers. Finding out which machines are compromised is nonetheless a difficult task. Moreover, MapReduce does not have an integrated security model because it was designed to run in a single data center.

10.4 Cloud Security in Availability:

Cloud services need to be up and running around the clock to meet the high availability goal. IaaS physical and virtual resources, like databases and processing servers, need to be available in order to support data fetch operations and execute computational tasks of programs, respectively. To this end, architectural changes are made at the application and infrastructural levels to add high availability and scalability. Author said that a multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on many servers. This approach enables DoS attacks resiliency by building software and hardware failure measures in all tiers. Notwithstanding, it is easy for a malicious actor just to rent several services from the same cloud provider and manage them at will.

Then, it is possible to have servers processing highly-demanding intensive tasks so as to occupy available resources, including memory and processing power and time. Although SLAs are agreed to depict the quantity and speed of memory and CPUs, nothing is deterrent to have them occupied at all times in a bogus manner, with fake tasks for instance. At a

certain point, resources might be denied to other customers. Nevertheless, such issue is partially allayed by the elasticity feature of cloud environments. Another issue in terms of availability is related with hardware availability . A single minor glitch can lead to partial or complete blackouts of the systems. So far, then cloud outages of major cloud providers have been reported in various studies. Those cloud outages, programming bugs, protocol blowups, and network glitches. Thus, outage events should be negotiated upfront in SLAs to discriminate disaster recovery and backup plans. Outages ranged from several minutes to several hours paralyzing businesses in general and happened mostly in 2008 and 2009 on Amazon S3, GAE, Gmail and Microsoft Azure

10.5 Cloud Security in Cryptography:

Cryptographic mechanisms are many times the most straightforward security measures applied. Nevertheless, they require careful implementation because cryptography does not guarantee complete security. Cryptographic mechanisms rely on the assumption that it is computationally unfeasible to calculate some values, given the result of an operation. Examples are the prime factorization of large numbers and the intractability of the discrete logarithm, both providing the security for the Rivest, Shamir, Adleman (RSA) standard. However, faulty implementations or bad password choices make malicious actors resort to brute force attacks first—a technique that goes through the universe of all possible combinations for a given cryptosystem.

The MEGA service encrypts every file at the user end before being uploaded to the cloud. Files are encrypted and checked for integrity by chunks using Advanced Encryption Standard (AES) and Message Authentication Codes (MACs), respectively. A symmetric key of 128 bits is used for these operations. Author mentioned insecure or obsolete cryptography and poor key management as potential issues. Author added faulty algorithms. Hence, programmers should have these cryptographic concerns in mind when developing SaaS applications and mechanisms for securely storing data and computing programs.

Nowadays, brute-force attacks represent a growing threat, mostly because they are easier to carry out. Two preponderant factors contribute to this issue: evolving technology and password cracking methods. Nowadays,

computers pack greater processing power distributed across various platforms, including multi-core CPUs and Graphics Processing Units (GPUs) with high clock rates. This enables to quickly search—in terms of time complexity—several huge combinatory key spaces of lower- and upper-case letters, digits and symbols. For instance, it was recently shown that a custom-built 25 AMD Radeon GPU-based cluster with the OpenCL framework can tore through 348 billion password hashes per second .

Windows XP passwords can be cracked from just a few minutes up to a few hours, depending on whether Local Area Network Manager (LM) or NT LM (NTLM) security is used. In addition to capable hardware, crackers also rely on advanced techniques that were tuned up over the time, allowing an efficient search of the keyspace universe in terms of algorithm complexity. Massive database password breaches (containing millions of plaintext, hashed, or encrypted passwords) throughout the years have given a structured perspective on user habits when it comes to password choosing, and provided the elements to assemble big rainbow tables and dictionary lists in the order of hundreds of millions .

For example, it is common to see passwords with first capital letters or a name followed by a year, or to exchange particular letters for similar numbers (e.g., “cracker” would become “cr4ck3r”). The recently hacked LivingSocial company exposed salted and hashed passwords of fifty million customers due to a cyberattack . A vastness of cracking applications is publicly available, including oclHashcat, Extreme GPU Bruteforcer, John the Ripper, Ophcrack, GRTCrack, and CloudCracker.

10.6 Cloud Security in Sanitization:

Sanitization is the process of cleaning or removing certain pieces of data from a resource after it becomes available for other parties. For example, deleting data has been a concern in distributed systems for a while now, to which monitoring, marking and tracking mechanisms have been employed for data discovery. Data sanitization is an important task in order to properly dispose of data and physical resources that are sent to the garbage. For instance, Google has destruction policies to physically wreck hard drives. However, deficient implementation of data destruction policies at the end of a lifecycle, may result in data loss and data disclosure , because hard disks might be discarded without being completely wiped or might

not be wrecked at all because other tenants might still be using them . Hence, one can say media sanitization is hard or impossible due to resource pooling and elasticity in cloud environments.

Since pooling and elasticity entail that resources allocated to one user will be reallocated to a different user at a later time, it might be possible for subsequent tenants to read data previously written. In fact, the media recently reported a case related with sanitization. Basically, cloud recycling, as it was termed, consists in reusing a cloud instance previously used by another customer. What was strange in the case was that of the instance being exposed to massive amounts of network traffic right after being lit up. It should have been zero. After the new customer investigated, it was found that an Internet Protocol (IP) address was maybe cached and that it belonged to an ad company that perhaps did not realized that IP was still part of their live infrastructure. The instance was nonetheless returned by the new customer. This case describes an innocent oversight that could render all cloud safeguards irrelevant if a bad actor happened to gain access to that instance. Pearson said there is a higher risk to customers when reusing hardware resources than dedicated hardware.

10.7 Cloud Security in Malware:

According to FireEye in their Advanced Threat Report, it is stated that malware events occur once every three minutes at a single organization, in average. Moreover, 50% of malware downloads additional malicious executables within the first 60 seconds of infection (usually called droppers), Websense says in the 2013 Threat Report. Droppers can also disable local security, prevent updates and perform an inventory of the victim. Malicious code with an adequate payload can be afterwards downloaded from bulletproof repositories and may further communicate with Command and-Control (CnC) infrastructures in order to become part of a botnet. Chen et al. said that botnets in clouds are easier to shutdown than traditional ones [48]. Although malware has been around for long, these indicators show off which kind of threat current companies (including cloud providers) must deal with—and the data is worrisome. One specific issue related with cloud-based storage providers, such as Media Fire or Sugar Sync, is inherent with the functionality of syncing data across several devices. If malware finds its way into a folder

synchronized with such a cloud, then it can spread across the devices that are also configured with that specific account.

Additionally, even if endpoint protection like anti-virus agents are installed, and if the agent match esa signature for the malware, which only has about 30% to 50% chances of doing so , and if it successfully deletes it from the hard disk, which sometimes is not able to, but if it does, then the cloud can just sync the malware back onto the device. Typically, if the first time succeeded, the agent will detect it the following times, and, for the enterprise SOC team, that is good news. Surely and outlier will be visible in the monitoring systems as one node is detected with 500 to 1000 or more alerts of the same malware. These type of applications typically create temporary hidden folders to sync data, which is the probable location for the malware to be detected in this case. A noteworthy issue from this discussion is the current signature-based anti-virus effectiveness, which is nowadays very low due to the static nature of the signature databases that have to cope with an increasing growth of dynamic malware.



CHAPTER - 11

Integrating Cloud Computing & Block Chain in Engineering Application

With the current growing interest in the blockchain and CoT, many new integrated BCoT platforms and systems have been proposed in the literature studies to provide security solutions and applications. The study proposed a cloud centric IoT framework enabled by smart contracts and blockchain for secure data provenance. Blockchain incorporates in cloud computing to build a comprehensive security network where IoT metadata (e.g., cryptographic hash) is stored in blockchain while actual data is kept in cloud storage, which makes it highly scalable for dense IoT deployments.

Another work in introduced a blockchain cloud network for access control with four main components:IoT devices, a data owner, a blockchain network and a cloud computing platform. Similarly, a hierarchical access control structure for BCoT was investigated. The blockchain network topology involves distributed side blockchains deployed at fog nodes and a multi-blockchain operated in the cloud, which would speed up access verification offer flexible storage for scalable IoT networks. In addition, to protect BCoT in security-critical applications, a forensic investigation framework is proposed using decentralized blockchain.

Following by the advantages of BCoT conjunction, provided secure identity management solutions which allow cloud service providers to autonomously control and authenticate user identity in BCoT. Blockchain is combined with virtual clouds to support identity verification in a fashion there is no prior requirements on trust between cloud users and cloud providers. On the other side, data management is also critical in

interconnected CoT where IoT data is enormous and thus requires careful management for data privacy objectives.

Motivated by this, presented a blockchain based data protection mechanism which can prevent effectively inappropriate IoT data movement due to malicious tampering during Virtual Machine (VM) migration on cloud computing. Also, a Mchain construction method is applied to integrity evaluation on VM measurements data.

In this architecture, a two-layer blockchain network, which includes a data validation layer and a PoW task layer, is integrated with IaaS cloud to enhance system integrity. Moreover, the work in also considered an integrated blockchain-CoT architecture where the focus was on solving the mining issue by offloading mining tasks to cloud nodes from IoT devices. Then, a joint problem of user access association and cloud resource allocation is formulated that is then solved by deep reinforcement learning (DRL).

In the same direction, the author also considered the offloading issue in BCoT networks, in order to optimize the economic cost of IoT devices. The study paid attention to the cloud service quality in the BCoT systems. In this case, the blockchain plays an important role in providing trust and reliability for high-quality cloud service provisions. The combination of cloud computing with blockchain was also considered. Here, the computing resources of remote cloud are allocated at the network edge to provide low-latency and real-time computing services for IoT devices. Meanwhile, the resource management in BCoT systems was studied where the blockchain is able to preserve data privacy during the resource trading between cloud providers and IoT users.

In general, most of the above BCoT platforms are based on a single cloud and may be enough for some applications. However, with complex IoT systems which require huge network resources to serve numerous IoT users, inter-cloud BCoT integration would be more efficient and convenient .As a result, BCoT architectures have been extended to multi cloud models for complex collaborative scenarios.

As an example, a BCoT framework was proposed in a joint cloud collaboration environment where multiple clouds are interconnected securely by a peer-to-peer ledge network. Further, the single cloud can

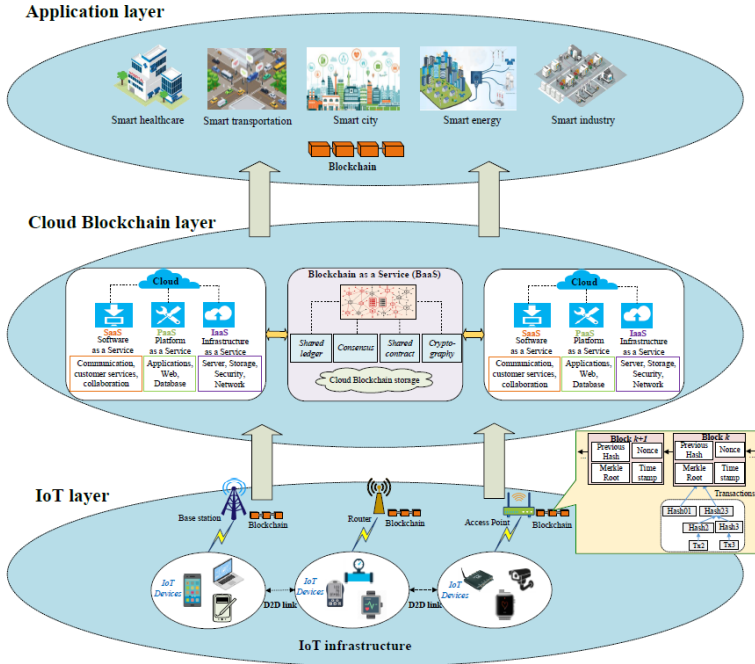
offer instant services for IoT users via blockchain which also mitigates risks of malicious attacks. Moreover, proposed a cloud federation model which enable distributed resource provisions using an individual cloud under the management of blockchain network. Besides, a BCoT model with micro-clouds was introduced by using blockchain-enabled distributed ledgers.

Motivated by extensive literature review, we propose a conceptual BCoT architecture, including three main layers: IoT layer, cloud blockchain layer and application layer.

Details of each layer and the general concept will be presented as the following.

1) IoT Layer:

IoT devices are responsible for harvesting data from local environments and transmitting wirelessly it to near by gateways such as base station, router or wireless access point. An IoT device holds a blockchain account (like a wallet in Bitcoin) which allows it to join the blockchain network to perform transactions (e.g., offloading data) and interactions with cloud services. Specially, each resource-limited IoT device (e.g., a wearable sensor) may act as a lightweight node that can participate in the validation process of a transaction through its representative gateway. It is feasible in blockchain based sensor network scenarios. where small sensors are connected with blockchain via its gateway (e.g., a smartphone or a fog node).



All interactions of sensors with blockchain such as creating transactions, offloading data or even mining tasks, are performed by the gateway . Meanwhile, for IoT devices with relatively large resources such as computers or powerful smartphones, they have enough capacities to serve other lightweight IoT sensors and maintain the full blockchain. IoT devices can also interact each other through IoT gateways to achieve corporative communication(e.g., device to device (D2D) communication in collaborative networks). Such a hybrid communication concept offers highly flexible services for IoT users in a secure and efficient manner.

2) Cloud Blockchain Layer:

This plays as a middleware between the IoT network and industrial applications in the BCoT architecture. For a generic architecture, we pay attention to a blockchain platform with multiple clouds, but it also reflects comprehensively technical aspects of a single-cloud BCoT architecture.

This model exhibits two merits:

1. ensuring highly secure network management via blockchain
2. providing on-demand and reliable computing services for large-scale IoT applications. The integrated cloud blockchain layer consists of blockchain services and cloud computing services.

Blockchain services:

The main purpose of blockchain in the proposed architecture is to provide secure network management. The blockchain network is deployed and hosted on a cloud platform as Blockchain as a Service (BaaS). In particular, BaaS can offer a number of blockchain-enabled services to support IoT applications.

Shared ledger:

It represents the database that is shared and distributed among BCoT members (e.g., IoT users, cloud nodes and blockchain entities). The shared ledger records transactions, such as information exchange or data sharing among IoT devices and cloud. It enables industrial networks where cloud users can control and verify their own transactions when communicating with blockchain cloud.

Consensus:

Consensus provides verification services on user transactions by using consensus mechanisms such as PoW, PoS run by a network of miners. This service is highly necessary for BCoT in improving blockchain consistency and ensuring high security for the system. Interestingly, IoT users can use their virtual cloud machines to join the consensus process in order to receive rewards as a result of their efforts (e.g., cryptocurrency in Bitcoin).

Shared contract:

BCoT also offer smart contract services to applications. With its self-executing and independent features, smart contracts are highly beneficial to build business logic and trust in the BCoT system. Furthermore, smart contracts provide security services on user access authentication or data sharing verification once the IoT peer nodes perform transactions, which also supports to maintain security over the cloud blockchain.

Cryptography:

This is responsible for providing public key cryptography to secure all information and storage of data among IoT and cloud entities. Digital signatures ensure any data being recorded in blockchain is true and untampered with, and this improves immutability and security for user transactions. In addition to such services, BaaS also offers cloud blockchain storage. The decentralized cloud storage based on blockchain can be built on the cloud platform. Blockchain-based storage manages IoT data through its hash values and implements verification periodically to detect any data modification potentials.

For example, Interplanetary File System (IPFS) is a blockchain-based storage system which is now available on cloud, allowing to store securely among storage nodes. This has also been proven to effectively solve data storage issues brought by centralized cloud models in terms of data leakage and storage management.

Cloud computing services:

In the BCoT architecture, cloud computing uses its full services to support applications, including Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Data aggregated by IoT gateways will be received by cloud servers and kept in the cloud blockchain storage. The cloud server also offers intelligent services on offloaded IoT data using available tools such as data mining or machine learning. IoT data can be stored off-chain in cloud database or on-chain in blockchain. On the other hand, multiple clouds can be incorporated to implement functionalities such as data sharing or collaborative system management. In this context, as a middle layer, blockchain layer plays an important role in handling and controlling cloud interactions to facilitate cloud service delivery to IoT users and avoid conflicts among clouds.

3) Application Layer:

Many industrial applications can gain benefits from the BCoT integration in different areas where IoT scenarios are involved, like smart healthcare, smart transportation, smart city, smart energy, and smart industry. BCoT not only provides useful services to industrial applications, such as

network management and QoS improvement but also guarantees security and privacy properties for applied domains.

For example, in smart healthcare, BCoT can support data processing services thanks to computation ability of cloud, which can assist healthcare providers in analyzing intelligently patient information for better medical care. In the meantime, network security of healthcare is ensured with blockchain which offers traceability and verification services during the medical data exchange and data processing.

