International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Quantum Computing-----Emerging Technology in Indian IT Industry for Sustainable Development

Smt Paramita Chatterjee[1], Smt. Nabanita De[2], Sri Debjit Mitra[3]
[1](Govt. Approved Contractual Whole Time Teacher) Department of Computer Science, Charuchandra College, University of Calcutta
[2] (Govt. Approved Part Time Teacher) Department of Economics, Charuchandra College, University of Calcutta
[3](ICSE School Teacher), (Assistant Teacher), Albany Hall Public School Department of Physics, Contact No: 8420398906,

Abstract: ***The laws of quantum physics permit us to process information using what is known as quantum computing. A quantum computer is different from a digital computer, while quantum computing sounds like a new technology, the fact is that it is a mathematical approach for finding efficient solutions to computational problems. The quantum computer holds the potential to store huge information than before. They need a special environment to function, but optimizes computation time and ability. The key of this computing future lies in the quantum theory applications to machine learning. Commercial production of quantum computers that would process information faster than today's supercomputers is still some time away. The industry first has to solve hardware issues in quantum technology, according to an expert. Quantum theory represents the smallest scales and shapes of matter, describing the behavior of subatomic particles like electrons, protons, neutrons and photons. In silicon chips of classical computers, the unit of data is rendered in one of two states — 0 or 1 pertaining to true/false or yes/no state. However, in quantum theory, data could simultaneously exist in both and holding exponentially more information. The unit, or "bit" in regular computing, becomes "qubit" in quantum theory, which can be either 0/1, or in superposition of both together. This means that the qubit holds greater information storage potential. The use of quantum computing can lead to many fundamental scientific breakthroughs and new technologies with wide ranging societal and commercial applications such as data encryption, new drug discovery and weather prediction. This paper mainly focuses on developing quantum computational capacity which would be India's "top national priority" simply because acquiring such technologies from outside the country will be too difficult and expensive for Indian IT industry. This sector is also a profitable industry and is playing an important role for employment generation and sustainable development of the country.***

Keywords: Quantum physics, qubit, Quantum computer, Sustainable development, Employment Generation

I. INTRODUCTION

A. *In 1982, Nobel laureate Richard Feynman asked: "What kind of computer are we going to use to simulate physics?" and "Can you do it with a new kind of computer - a quantum computer?"*

So the idea for a quantum computer was born, becoming an area of growing scientific interest. The basic unit of information in a quantum computer is known as a quantum bit or "qubit". Currently, there are two categories of quantum computer. The first one is a Universal Quantum Computer, which can perform any kind of computational operation. The second one is the Annealing Machine, which is targeted in solving specific type of optimization problems. Both kinds of machine are made of qubit, which has two distinct features that differentiate from a regular bit: Superposition (In contrast to a regular bit, which can be either 0 or 1, a qubit can exist in both 0 and 1 states at the same time. The qubit may be 0 or 1, or have any ratio between them) and Entanglement (This is a counter-intuitive phenomenon where two or more different qubits can be connected, despite being physically apart) [24]. Through quantum mechanical phenomena, these qubits can perform many computations simultaneously. Theories are being developed for scaling and fault tolerant architectures for implementing better quantum algorithms. Other challenging issues for theoreticians include developing models for measurement and control of qubits particularly to minimize the impact of noise and fabrication non-uniformities on the behavior of qubits. Given this prospect, there are many hyped statements being made about the capabilities of quantum computing to do tasks such as breaking modern encryption methods in seconds and solving intractable problems in minutes. While in theory this is possible, the reality today is that quantum computers have yet to achieve these types of results. As such, it is unlikely classical computing will be replaced any time soon by quantum computing. The more likely future scenario is that quantum computing will augment subroutines of classical algorithms that can be efficiently run on quantum computers. Cost

per unit of quantum computing is also still a factor although this will change as quantum computer improves and easier to access [23]. Enterprises that begin their quantum computing journey now will be best positioned when the emerging technology reaches maturity.

II. LITERATURE REVIEW

Quantum Mechanics (QM) describes the behavior and properties of elementary particles (EP) such as electrons or photons on the atomic and subatomic levels. Formulated in first half of the 20th century mainly by Schrödinger, Bohr, Heisenberg and Dirac, it was only in the late 70's that quantum information processing systems has been proposed. Even later, in the 80's of the last century it was Feynman who proposed the first physical realization of a quantum computer. In parallel to Feynman, Benioff also was one of the first researchers to formulate the principles of quantum computing and Deutsch proposed the first quantum algorithm. The reason that these concepts are becoming of interest to computer engineering community is mainly due to the Moore's law[1]; that is: the number of transistors in a chip doubles every 18 months and the size of the gates is constantly shrinking. Consequently, problems such as heat dissipation and information loss are becoming very important for current and future technologies. Improving the scale of transistors ultimately tends to a technology working on the level of elementary particles (EP) such as a single electron or photon [2]. Geordie Rose, co-founded D-Wave Systems Inc., the 'world's first quantum computing company' [24].In this system developing theoretical approaches go hand-in-hand with experimental advances. The disruptive potential of quantum computing is attracting growing interest and substantial investment from industry and governments globally. This is happening despite the understanding that a universal quantum computer is still years away from being commercially available. Andrew Lockley told, "There's a revolution coming in computing that has the power to disrupt society just as fundamentally as the first information revolution. This new generation of computers isn't just faster or better – they're completely, radically, different." Atos (an international information technology services company), view quantum computing is an emerging technology from 2019 onwards, and its impact will be verging on transformational.

The Commonwealth Bank of Australia (CBA) is one institution which is investing heavily in quantum computing. Dilan Rajasingham (CBA's Executive Manager of Technology Innovation), said: "We're not going to wait for the machine." There are very few groups working in India in the area of quantum computing. It is a highly interdisciplinary area. Computer scientists and mathematicians need to work on algorithms, architectural issues for scalable systems, data storage and data transmission while others will focus on the physical realization of the basic elements of the quantum computers [21]. Mikhail Lukin, (Professor of Harvard, and an alumnus of the Moscow Institute of Physics and Technology (MIPT)), said that scientists are still in the dark on how to build the universal quantum computer that would perform any quantum algorithm far quicker than conventional computers, given the many millions of qubits required for such a device. Moore's law is the observation that the number of transistors in a dense integrated circuit doubles approximately every two years. This proved accurate for several decades, and has been used in the semi conductor industry to guide long term planning and to set targets for research and development Quantum mechanics has led to devices like broadband optical fibers and smartphone displays which work using photons — the smallest indivisible quanta or unit of light. Owing to the enormous potential of quantum computers, companies like Google, Microsoft and IBM have invested massively in quantum computing research.

This technology creates special blocks which are signed by quantum keys, rather than traditional digital signatures. The technology has already been tested in one of Russia's largest banks — Gazprombank. Russian-born the Singaporean entrepreneur Serguei Beloussov told "Total information security is guaranteed by quantum communications has a flip side and poses a philosophical dilemma", "Most governments of the world over control their populations through control over information. So, if information becomes completely private, they would lose this control" [22].

III. OBJECTIVE OF THE STUDY

A. Concept of Quantum Computing
B. Quantum Computer-Hardware & Software Advancement
C. Cryptographic Analysis
D. Employment generation and profitability in Indian IT Industry
E. Challenges and inclusion of quantum computing in Indian IT sector
F. Future Prospect of Sustainability

IV. SOURCES OF STUDY

This article is mainly based on secondary data. The Theoretical observation is collected from different published papers, books, journals and website. The conceptual part is taken from different scientitists writings, interviews and e-books, e-journal. On this basis of the study is formed and concluded a definite path for sustainable development in Indian IT Industry.

1) Analysis & Interpretation

V. CONCEPT OF QUANTUM COMPUTING

The basic characteristic of a quantum computer which differentiates it from conventional computer is that it uses qubits in place of bits. A qubit may be a particle like an electron with "spin up representing 1" and "spin down representing 0"and quantum states called superposition that involves spin up and spin down simultaneously. A small number of particles in superposition states can carry an enormous amount of information [4]. In real world, bits are represented by 0 or 1. Only one of the four states can possible at any time in space. But in case of quantum state all four possible outcomes are possible like, if we deal with 0 & 1 then simultaneously we can have four possibility that is 01, 10,00,11[8]. Similarly if we used three bits we can have eight possibility such as (000,010,011,100,101,110,111,001), so for 100 bits say we can have 2^{100} possibility or outcomes.

A. Origin of Quantum Computing

From an experimental point of view, there are three areas in which research needs to be focused:

1) Realizing qubits which are the elementary physical systems of a quantum computer to hold information,

2) Interconnects to pass information from one point to other in the physical platform on which qubits are fabricated and

3) Scaling-up the quantum computing systems. Much of the research effort now is focused on realizing the stable qubits on test beads.

Broadly, the major research groups in various parts of the world are working on:

The concept of the duality was first discovered by de Broglie and he made a hypothesis" that particle like electron, proton etc. has a dual character that is particle like and the other is wave like" according to him if p be the momentum of the particle, λ be the wavelength then according to the hypothesis,

$\lambda = h/p$ where h is the Planck constant. [9] As an example, if one see in case of light, it shows both characteristics, particle like and wave like. Wave like phenomena proves by the phenomena like interference, diffraction etc. and particle like phenomena proved by the phenomena such as photoelectric effect. Now, the physical state of a system represented by state vector by the k et vector ψ signed as$|\psi>$ [10].For a system with two states we can call the two k ets as $|0>$ and $|1>$. Now in case of representation of qubits if bit 0 is denoted by $|0>$and bit 1 denoted by$|1>$, then if we can take linear superposition of this two state denoted as

$$|\psi>=a_0|0>+a_1|1>$$

That's it represented mixed state or represented 1 and 0 simultaneously.

B. Quantum computing Gates

Now the concept of physics utilizes in computer science to make suitable gates for quantum computing as we use gates for the conventional computers. To design the quantum computer we just need reversible which can determine certain input information but in case of our conventional computer information gets irreversibly lost during the gate operation of like AND, ⊼NAND etc. [1] To overcome it we use the reversible gate like the usual NOT gate (N), CONTROL NOT gate (CN or CNOT or XOR), CONTROL CONTROL NOT gate (CCN or CCNOT). These are also called Tofolli gate. In the CN gate A'=A, i.e. the input A gets through unchanged. The filled circle on the first wire represents a control in the following sense: if A=0 then XOR operation on the second wire just lets the signal B get through and therefore B'=B. If A=1, then XOR operation on the second wire acts as a NOT gate and B'=B. In the CCN gate A'=A and B'=B. The XOR operation on the last wire acts as a NOT gate but only if A=B=1.

A	B	A'	B'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Figure 1: CN (Reversible gate or Tofolli gate) (Truth Table) (1

QUANTUM COMPUTING _

C. Difference between Classical Computer and Quantum Computer:

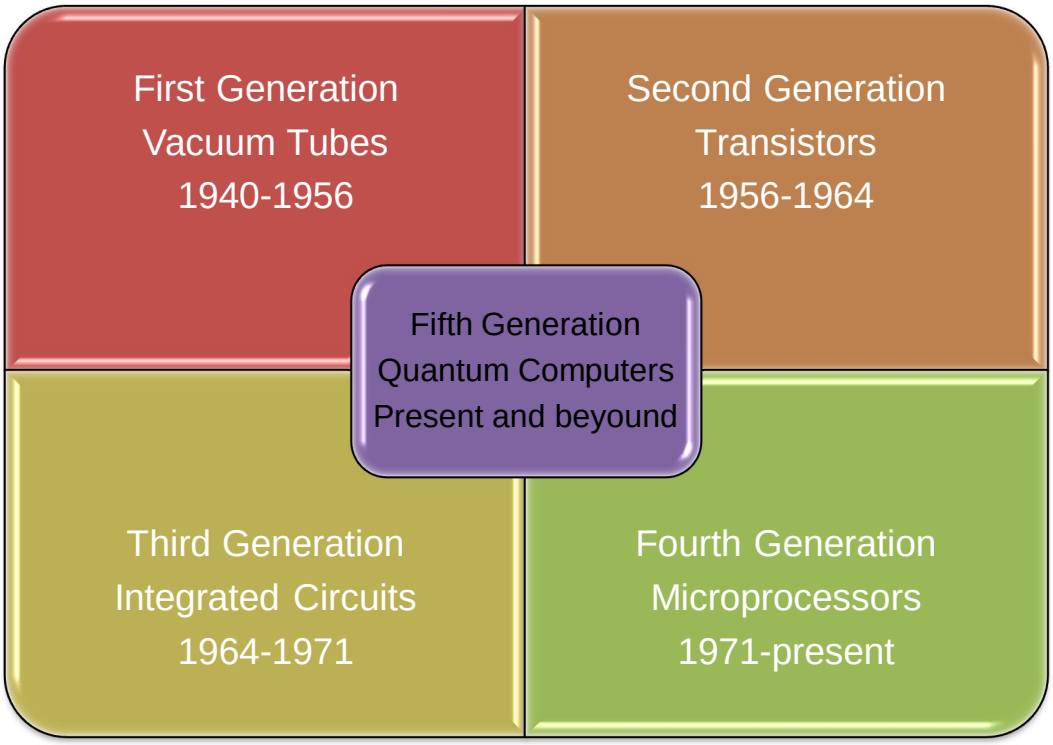


Figure 2: Source :(Accenture) [13]

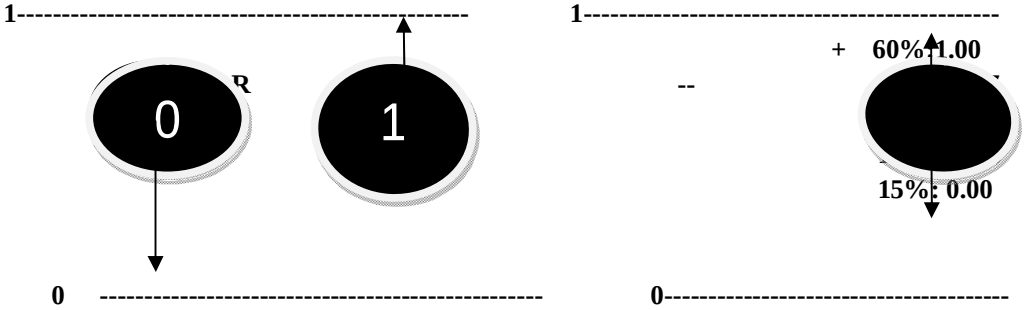
The innovation behind quantum computing is in the way it takes advantage of certain phenomena that occur at the subatomic level.

Table 1: fundamental differences between classical and quantum computing.

1.Information representation:	2.Information processing:
In classical computing, a computer runs on bits that have a value of either 0 or 1. Quantum bits or "qubits" are similar in that for practical purposes we read them as a value of 0 or 1, but they can also hold much more complex information, or even be negative values.	In a classical computer, at the basic level, bits are processed sequentially, which is similar to the way a person would solve a math problem by hand, one step at a time. In quantum computation, qubits are entangled together so changing the state of one qubit influences the state of others regardless of their physical distance. This allows quantum computers to intrinsically converge on the right answer to a problem very quickly.

3.**Qubit Superposition**:

Classical **Quantum**



*__Discrete__ number of possible states: 0 or 1. ***Infinite** (continuous) number of

*__Deterministic__: repeated computations on the possible states. same input will lead to the same output.

* **Probabilistic:** measurements on

Superposed states yield probabilistic answer then reduced to 0 or 1. **[38]**

VI. QUANTUM COMPUTER-HARDWARE AND SOFTWARE ADVANCEMENT

Recent developments have propelled quantum computing from a theoretical concept into a tangible computing option for enterprises—one with the potential to deliver business value by solving difficult subsets of problems in entirely new ways. However, businesses can start innovating now by accessing existing commercial quantum computing capabilities through newly available quantum hardware platforms and software applications. A few leading companies are already using various techniques to make quantum hardware available for purchase and shared use; others are working to offer cloud-based quantum computing platforms and software applications to access quantum computing power. Software APIs with pre-developed algorithms make it easier for enterprises to define problems to test with quantum computers, and build pilot applications that run on existing quantum computing models. On the hardware side, D-Wave is currently the sole manufacturer of commercial adiabatic quantum computers, having released three models since 2010. The company recently announced its next generation quantum computer with 2,000 qubits. There are several other groups, including Google, MIT Lincoln Laboratory and Intelligence Advanced Research Projects Activity (IARPA), working on developing these devices as well. For example, Google recently unveiled a digitized adiabatic quantum computing device that features digital error correction capabilities. By more effectively controlling noise than previous adiabatic quantum computers, this kind of hybrid approach should allow for more rapid scaling in problem sizes [23].

In terms of software, the quantum ecosystem is also growing. Startup companies are emerging to bridge the gap between experimental research and enterprise. Most notably, companies such as 1QBit, QxBranch and QCWare are taking a fresh look at some of the most challenging computational problems today by applying a quantum mindset to the software solution. The technical implementation involves using application programming interfaces (APIs) to provide web-based access to quantum computations.

In the longer term, the emergence of scalable, fault-tolerant, digital quantum computers offers a new direction for progress in high performance computing as conventional technologies reach their fundamental limitations. Quantum speedups have been discovered for a number of areas of interest, including simulations for chemistry, nuclear and particle physics, and materials science, as well as data analysis and machine learning. In addition, quantum speedups have been

discovered for basic primitives of applied mathematics such as linear algebra, integration, optimization, and graph theory. These demonstrate the potential of quantum computers to yield better-scaling methods (in some cases exponentially better) for performing a wide variety of scientific computing tasks. Practical realization of this potential will depend not only on advances in quantum computing hardware but also advances in optimizing languages and compilers to translate these abstract algorithms into concrete sequences of realizable quantum gates, and simulators to test and verify these sequences. The development of such software has recently seen rapid progress, which can be expected to continue given sufficient support [26].

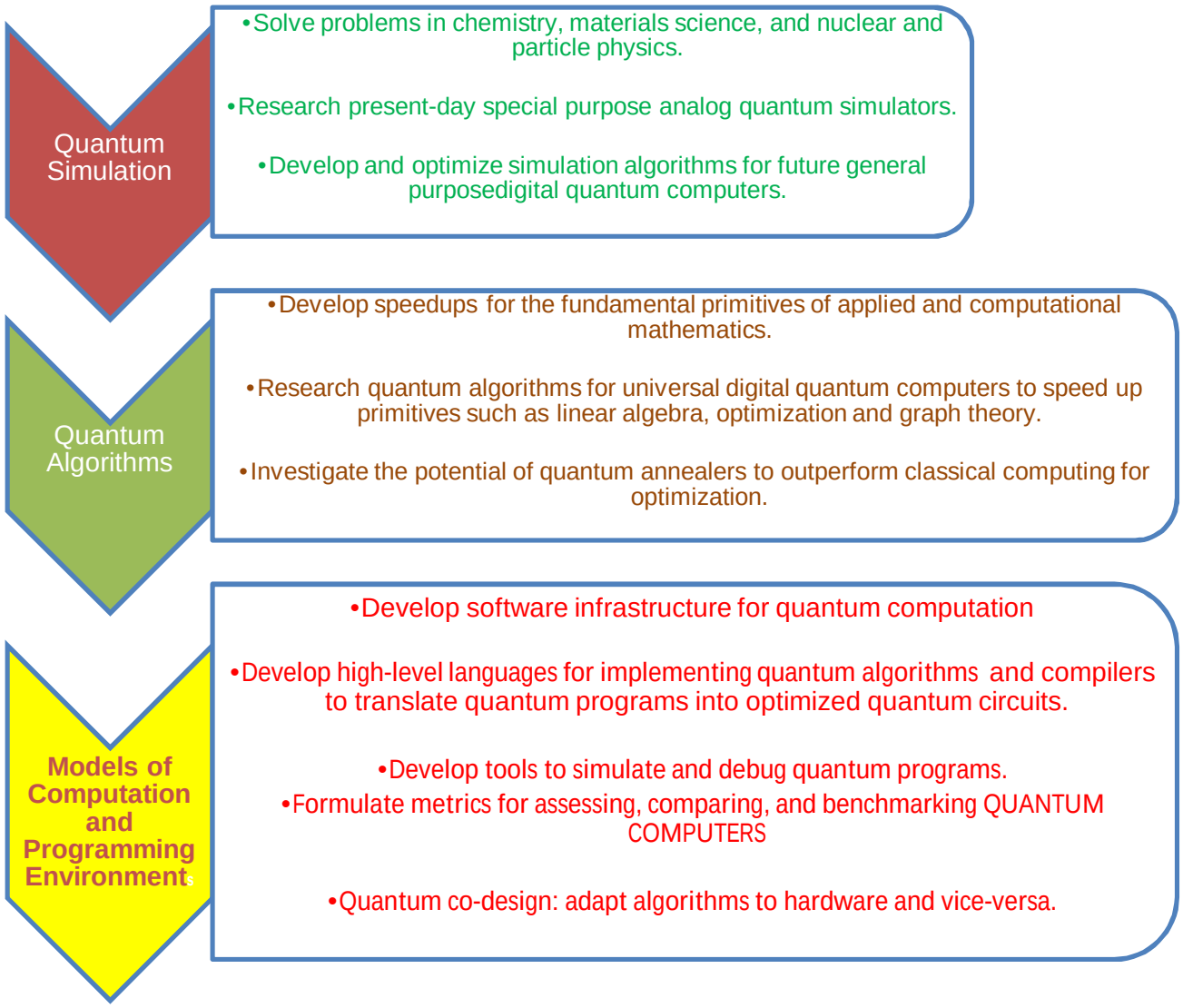


Figure 3: Summary of quantum computing research opportunities

A. Open Source Activity

Open Source Software (OSS) is computer software that is free to download and use, includes the source code, and can be modified or redistributed under an 'open source license', of which there are various kinds. The range of OSS is vast in scope and has been created by individuals, companies or collaborative groups of varying sizes, who may also have global distribution. The main economic benefit of using OSS is cost saving. Quantum computing OSS is also available with 49 currently accessible projects dating from 1999 to July 2016. The majority of these are from universities, with companies including Google, Microsoft and Toronto based Artiste-qb also contributing. OSS for quantum computing encompasses tools for mathematical computation applications: including Matlab and Mathematica; as well as quantum algorithms and quantum simulators in a variety of computer languages . Microsoft 'Liqui|>' by Microsoft and 'QuTip' are two examples of OSS toolkits for quantum computing. These help make programming easier and more accessible using high-level languages (F# for Liqui|> and Python for QuTip). However, using these tools requires familiarity with quantum physics.OSS has an important role in teaching and training the current and next generation of quantum scientists, engineers and entrepreneurs. OSS can also lead innovation, not only to improve quantum algorithms, but facilitate the creation of more complex quantum-based applications, as the knowledge, language and tools become more sophisticated and spread to a wider audience. Just as OSS is enabling businesses to do new things in the digital age, what can OSS for quantum computing achieve in the quantum era? Only time will tell.

Table 2: Open source resources (1999 to July 2016) with corporate activity [24]

Release	Name	Language	Origin (University, Individual or Company)
2006	Qubiter	C++	Artiste-qb, Canada
2009	PyQu	Python	Google, USA
2013	Q++	C++	Cybernet Systems Corp
2014	QuanSuite	Java	Artiste-qb, Canada
2014	Quantum Computing Playground	qScript	Google, USA
2016	Liqui|>	F#	Microsoft Research, USA
2016	Quantum Fog	Python	Artiste-qb, Canada
2016	Qubiter	Python	Artiste-qb, Canada

B. Patent Activity

Patents are one indicator of innovation and looking at the patent landscape for quantum computing gives a valuable insight into activity in this area.

Table 3: A summary of the world-wide patents for quantum computation between 1985 and 2013 [24]

Number of patent families:	839
Number of patent applications :	1,995
Peak publication year:	2005
Top applicant :	D-Wave Systems
Patent assignees :	860
Priority countries:	23
Top Country :	USA

Source "Quantum Technologies: A patent review for Engineering and Physical Sciences Research Council

The USA tops followed by the European Union, Canada, Japan and the UK.

D-Wave Systems (Canada) clearly leading the field, followed by Hewlett Packard, the Japan Science & Tech Agency and Toshiba.

VII. QUANTUM COMPUTING AND CRYPTOGRAPHY

Computer security and protecting valuable data & information has been played an important role in the world of Information & Communication technology. With the development of the Internet, companies had to ensure that customer data as well as their internal private data was protected from outside intrusions; the secure socket layer (SSL) protocol was the first step toward allowing for the secure transmission of information from client to server and vice versa (In Information Technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities. [33]). Data encryption became a requirement for day-to-day operations of any organization connected to the Internet and thus the world of big-business cryptography exploded (cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it [32]). Encryption is at the heart of modern society,so every electronic interaction requires safeguarding information, from securing an email password to protecting missile launch codes. Internet searches, financial transactions, and even democratic elections rely on encryption for security and

confidentiality. Encryption of data for many IT systems today relies on *public-key* cryptography. The importance of encryption cannot be understated and potential threats to it must be taken seriously.

Quantum computing is one such threat. The processing power alone of quantum computers is an incredible achievement, reaching speeds eight orders of magnitude faster than classic computers and thousands of times faster than modern supercomputers. While there is a endless list of positive and innovative applications for quantum computing, there is a concern that its sheer power could be used for more a malicious intent. Many existing security mechanisms and encryption methods are thought to be secure because a brute-force attack is time prohibitive. However, with quantum computers and their computational speediness on the horizon, it is time to rethink what it means to be time prohibitive, and to develop new encryption algorithms that are resistant to the capabilities of quantum computing [29].Quantum cryptography [28] has been at the forefront of purposes for developing quantum computers since the early 1980s. Due to the way the qubits behave when observed, it opened up the possibility of creating a new form of quantum communication between two parties. Where before, transmission of messages relied on the receiver having an encryption key to decode an encoded message, researchers were able to utilize photons to send a message and detect whether the message had been viewed along the way. While this method does not prevent an eavesdropper from reading the message, it created a way for both the sender and receiver to know if the message had been intercepted.

A cryptographic application of a quantum system was one of the earliest ideas involved with quantum computation and can be accredited to Stephen Wiesner in the 1960s. Wiesner developed a theory that was meant to prevent counterfeiting of money using the laws of physics as a basis for protection. His method relied on information that is encoded in quantum states thereby being able to prevent any outside party from accessing said information without disturbing the state. This property of quantum information has given birth to a new method of information exchange and other companies are investing in it to develop new products giving users the utmost security of knowing if their critical data has been intercepted or viewed by an unintended audience outside the exchange. In 2002 and 2003, a Swiss company called id Quantique and an American company called MagiQ Technologies, both developed commercial communication products leveraging this technology for message transmission and receipt (Bacon & Leung, 2007). These two companies are noted as marketing the very first quantum key distribution systems. This could be the preferred method for secure communication of the future instead of relying on a receiver held private key utilized in systems based on the famous RSA crypto architecture for example. Larger organizations are also starting to invest in quantum technologies, such as Hewlett-Packard, Microsoft, IBM, Lucent, Toshiba and NEC; each have active research programs exploring how quantum cryptography can be leveraged into their future business models (Bacon & Leung, 2007).

VIII. INDIAN IT INDUSTRY

he Indian software industry started in 1970 with the entry of TCS into the domain of outsourced application migration work. The software industry has gained a brand identity as a knowledge economy due to its IT and ITES sector. The IT-ITES industry has two major components, IT services and business outsourcing (BPO). The industry has increased its contribution to India's GDP from 1.2% in FY 1998 to 7.5% in FY 2012[11].T he contribution of the IT sector to India's GDP stood at 7.7 per cent in 2016.The IT hardware industry can play a big role in providing products and solutions to aid the India growth story. It has the potential to leapfrog India to next generation of technology adoption and holds immense transformational potential for various industry verticals. The Indian IT sector is broadly categorized into IT services and software, Information technology enabled services (ITeS) and IT hardware products segment. The Indian desktop PC market can be divided into two segments, unbranded assembled PCs and branded PCs. In the branded PC market, multinational as well as Indian brands are present. Assembled PCs account form the largest chunk of total PC sales. This is because these are substantially cheaper than the branded products and the consumer of hardware and peripherals is extremely price sensitive. Servers can be further divided into high, medium and low end servers. In the case of printers, the market can be segmented on the basis of type of printer i.e. laser, inkjet and dot matrix [12]. As per the 'BMI India IT report, 2012' the share of hardware in total IT spending is expected remain above 50% during the 2012-2016 forecast period. PC forecasts will grow at a CAGR of 22% between 2012 and 2016. Overall, the hardware market is predicted to grow from an estimated US$9.3bn in 2012 to US$16.0bn in 2016, with PC sales including accessories projected to rise from an estimated US$7.6bn to US$13.0bn over the same period. In 2011, annual PC sales were estimated at 11.8mn units and are expected to increase to more than 30mn by 2016. While these three verticals lead the market in the current scenario, sectors such as Communications and Media, Financial Services and Healthcare are expected to ride the next wave of growth witnessing growth rates of 12 percent, 11.6 percent and 11.4 percent respectively This growing market, which is currently sized at USD 13 billion, has been led by BFSI, Manufacturing and Government, which have the maximum share in hardware spend in India .Factors such as infrastructure requirement in public sector, capital-intensive nature of manufacturing firms and increasing need or modernization of banks has

been driving the spending of these three verticals. While these three verticals lead the market in the current scenario, sectors such as Communications and Media, Financial Services and Healthcare are expected to ride the next wave of growth witnessing growth rates of 12 percent, 11.6 percent and 11.4 percent respectively [12].

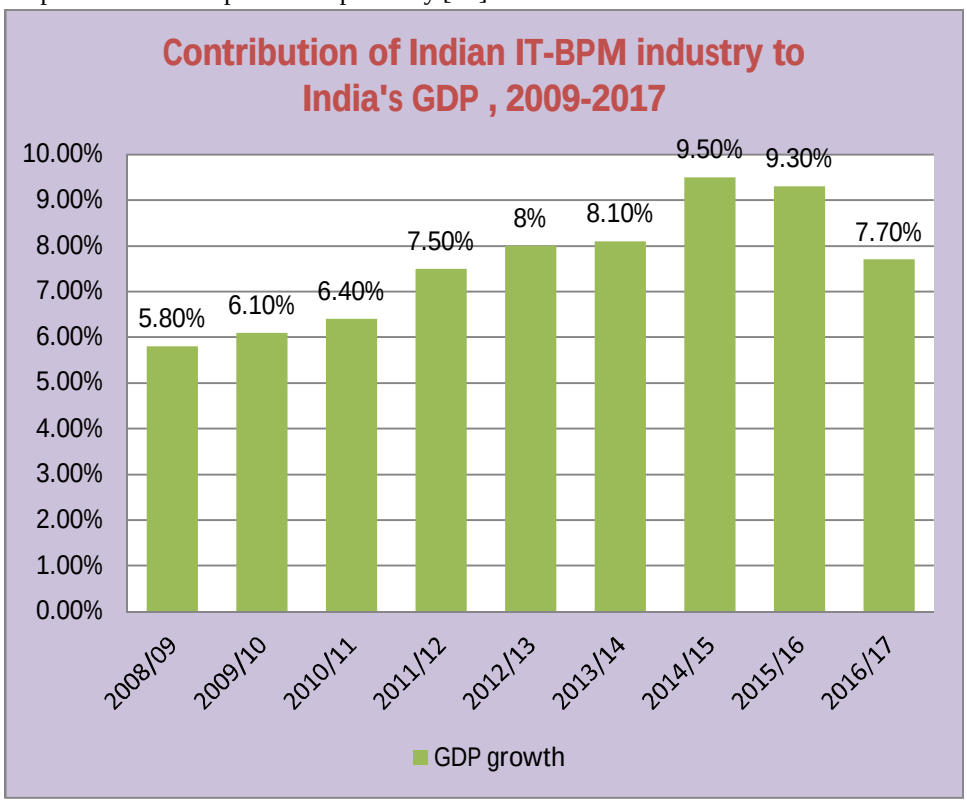


Figure 5: Source: website of Indian IT industry.

A. *IT for Masses (Manpower developmental Scheme):* IT for Masses" is a Plan Scheme of DeitY. It was introduced in the 10th 5Y plan, continued in the 11th 5Y Plan, retained in the 12th 5Y Plan. The Working Group on Information Technology Sector for 12th 5Y (2012-17) has considered and recommended continuance of the scheme in 12th Plan under 'e-inclusion' as thrust area. To achieve greater equity and inclusivity, there is a need to concentrate efforts in selected geographical areas, comprising of:

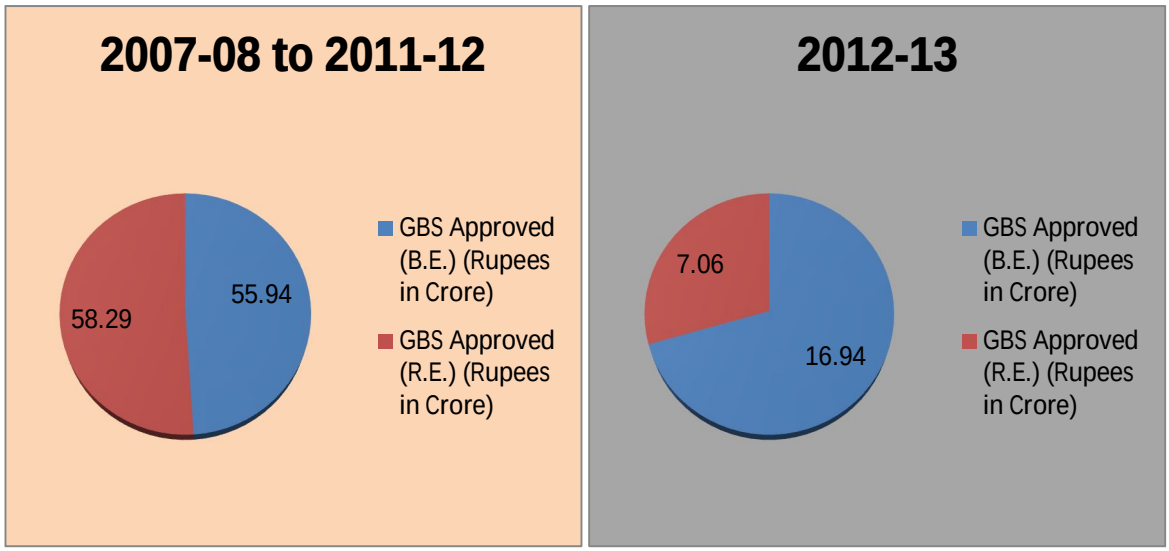


Figure 6 & 7: 12th Plan (2012-17) Allocation & Expenditure [N4] & from 2013-14 onwards, IT for Masses Programme will be merged with Manpower Development Scheme of the Department

Table 4: Achievements (11th And 12th plan)

Year	Number of on-going projects	Number of projects completed	Number of beneficiaries – Completed projects
2007-08 to 2011-12	22 (Spill over to 12th Plan	38	2,95,468
2012-13	20	43	3,05,912

Source: Report of the Working Group on IT Sector for Twelfth Five Year Plan (2012-17)[20]

B. India's IT Market Size growing; TCS the Market Leader [15]

1) India's technology and BPM sector (including hardware) is likely to generate revenues of USD160 billion during FY16 compared to USD146.5 billion in FY15, implying a growth rate of 9.2 per cent.

2) The contribution of the IT sector to India's GDP rose to approximately 9.5 per cent in FY15 from 1.2 per cent in FY98.

3) TCS is the market leader, accounting for about 10.4 per cent of India's total IT & ITeS sector revenue in FY16.

4) The top five IT firms contribute over 25 per cent to the total industry revenue, indicating the market is fairly competitive.

Table 5: Leading IT players by revenue (FY16)

Company Name	Revenue (USD billion)
TCs	16.6
Infosys	9.5
Wipro	7.8
HCL Tech	4.7
Tech Mahindra	4.04

Source: TCS website and Annual Report, TechSci Research [15]

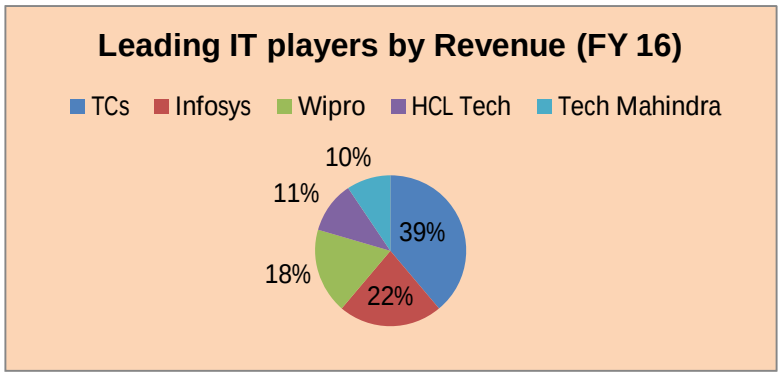


Figure 8: Compounded from Table 5

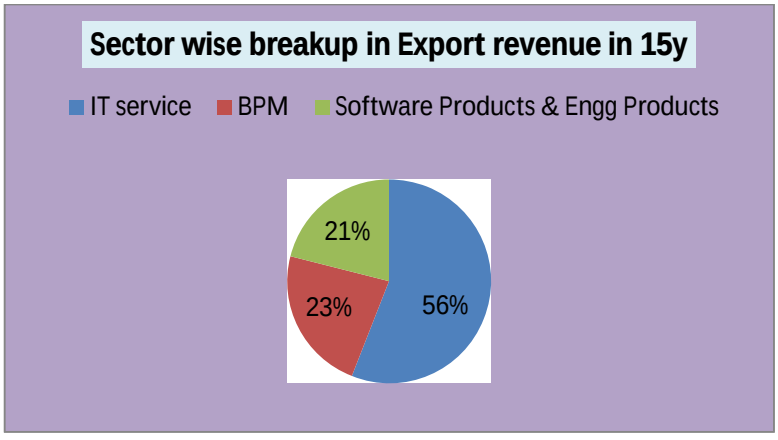


Figure 9: Source: Nasscom, Make in India, Techsci research [9]

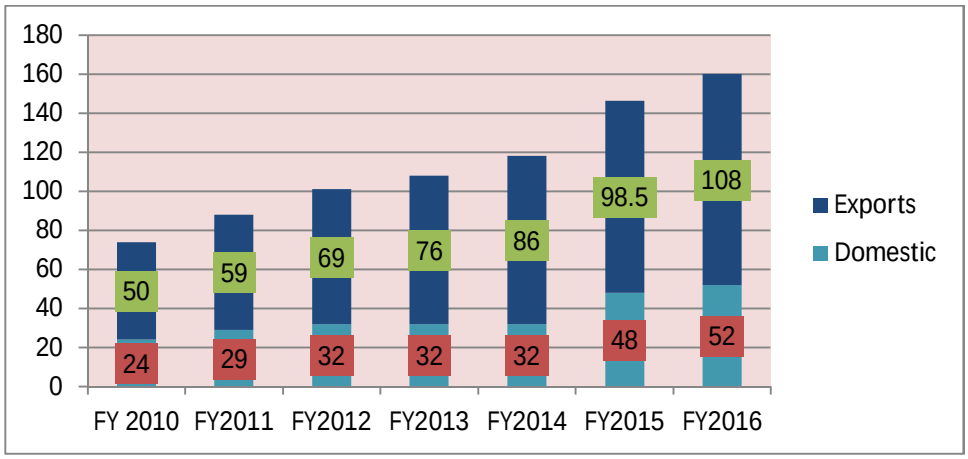


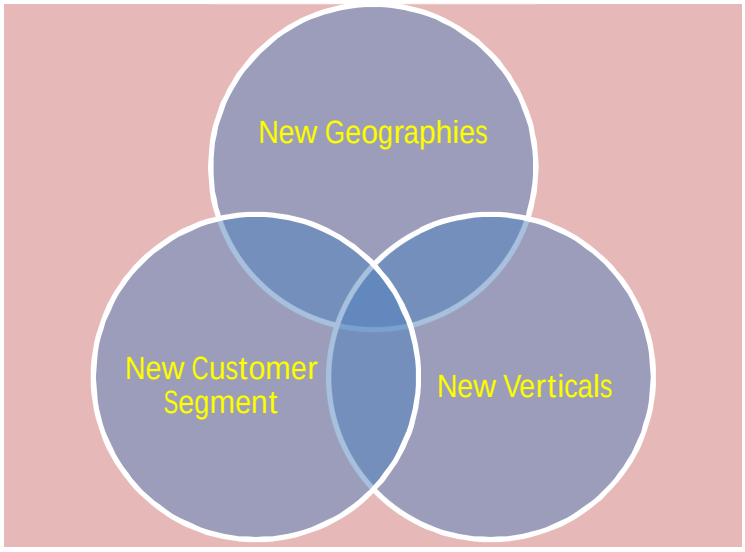
Figure 10: Source: NASCOMM, TechSci Research , Note: E - Estimates

IX. OPPORTUNITIES OF APPLICATION OF QUANTUM COMPUTING IN INDIAN IT INDUSTRY- CHALLENGES

A major barrier to developing quantum computing is availability of test bed computing systems that can be used to explore algorithms and computational approaches. The development of two to three testbeds, which would support ASCR (Advanced Scientific Computing Research), BES, and HEP-based algorithm development activities. These testbeds will not look like conventional computers – they would likely comprise approximately a six-nine qubits and likely would be based on optical or circuit-based approaches, requiring modest technical support to use [16].

In collaboration with 1QBit, Accenture Labs has mapped many possible use cases for quantum computing with a focus on finding those that are the most promising in various industries. The goal is to identify and validate the problems where a quantum algorithm will outpace existing computing methods and improve results. Enterprises that begin business experiments with quantum technology now will be better prepared for major industry changes that could come through the introduction of quantum computing.

On the hardware side, D-Wave is currently the sole manufacturer of commercial adiabatic quantum computers, having released three models since 2010. The company recently announced its next-generation quantum computer with 2,000 qubits .There are several other groups, including Google, MIT Lincoln Laboratory and Intelligence Advanced Research Projects Activity (IARPA), working on developing these devices as well. In terms of software, the quantum ecosystem is also growing. Startup companies are emerging to bridge the gap between experimental research and enterprise. Most notably, companies such as 1QBit, QxBranch and QCWare are taking a fresh look at some of the most challenging computational problems today by applying a quantum mindset to the software solution [13]



[15]

Figure 11: Newer Geographies and Verticals Provide Huge Opportunities

Table 6: Quantum Computing Applications by Industry

Industry	Sample Opportunity Areas For Quantum Computing
1. Financial Services	Risk optimization & fraud detection.
2. Health Care	Protein Folding & drug discovery
3. Manufacturing	Supply Chain & purchasing
4.Resources	Asset degradation modelling and utility system distribution optimization.
5. Media & Technology	Advertisement Scheduling & ad revenue maximization.

A. Impacts of Quantum Computing

1) National and economic security

a) Quantum computers could break all present-day public key encryption systems−

b) Quantum encryption not susceptible to computational attack •

2) Physical Sciences

a) Quantum simulations: materials design, pharmaceutical design, chemical processes, etc. – any problem that involves quantum mechanics−Broad non-computing impacts in new sensor and detector technologies:

b) Diamond NV (nitrogen-vacancy) centers are leading to previously unimaginable magnetic imaging systems

c) Chip-scale atomic clocks – precision timekeeping

d) Exquisitely sensitive magnetometers, accelerometers, gravimeters

e) Fundamentally new detectors and sensors in physical sciences, based on superposition, entanglement, and squeezing.[42]

Source: US department of Energy

X. POLICY RECOMMENDATION:

A. Short-Term Plan

1) Begin learning about quantum computing and the tools available to harness it.

2) Identify areas of the business where today's quantum computers can make a difference.

3) Test initial use cases.

4) .Create a timeline for how these use cases will scale with quantum computing advancements.

B. Long-Term Plan

1) Create a quantum computing roadmap for the business and reevaluate throughout the year.

2) Appoint an employee(s) to monitor trends and report in monthly.

3) Build quantum-ready applications on top of a hardware agnostic interface, to allow for seamless switching between different types of quantum computers as they evolve[23]

4) *Technology switching costs:* Quantum computing threatens modern cryptographic tools and renders them ineffective. It does not negate all of the cryptography tools at society's disposal, just the tremendously popular ones. The gains that are promised by mature quantum computing are exciting with a great potential for capitalization, however, the unintended costs to our existing communications infrastructure will be extremely expensive, starting on the very day that quantum computers graduate from the lab to commercially available.It can take years for a standards body to significantly alter a well-established and popular standard. This is because it is usually much simpler to create a new standard than it is to retrofit an old one with sweeping new features. Nevertheless, without technology standards, the market will still find a solution to its problems, often resulting in a number of expensive proprietary methods vying for market dominance until an oligopoly of winners emerge who will sacrifice interoperability for market share and price premiums. In most cases, the elements that interface with the components and systems are the only ones that require standardization. The internal workings of a system can often remain not standardized, and be treated as an economic differentiator by its respective manufacturer. Most commercial communication and security products are built on top of standards based cryptography and protocols because designing and building a secure

system is tricky in the sense that a security system appears to be working, until sometime after it has been successfully exploited.

5) *Avoiding technology switching costs*: Technology switching costs occur anytime a change is made in a basic technological system such as a data center, core network, wireless sub-system, etc. These costs can often be avoided by reasonable planning before the switch from one technology to another must be made. For many categories of secure information, there may be no need to introduce quantum-safe techniques into systems for some time. For other such categories, action may be required within a relatively short time period [30].

XI. CONCLUSION

Quantum computing is an exciting new technology. Quantum imaging has high potential for use in industry and in defence and security, where there is a need to see through turbid media, or in the presence of noise or background light [44].It has the potential to perform computation at an unprecedented rate which will have exceptional benefits for society. Quantum computing poses serious risks to widely-used encryption methods, most notably RSA (Rivest Shamir-Adleman) and ECC (Elliptic Curve Cryptography) . Rather than slow the pace of innovation and stifle growth, the reaction to these concerns should be to migrate our encryption standards to post-quantum cryptography. The goal should be to stop the use of theoretically unsecure encryption methods, such as RSA, and instead use methods that are proven computationally hard to solve [29].

The economic impact of quantum computing can be considered from both research and commercial perspectives. Research in quantum computing by universities and companies is generating revenue for suppliers on a local, national and global basis, through the purchase of specialist equipment and components. One such supplier is M-Squared Lasers, a Scottish company founded in 2005, who provide lasers for the scientific, medical and defence sectors. Quantum computing is a growth area for the company [24].

REFERENCES

[1] Jozef Gruska, “Quantum Computing
[2] “Quantum Computing Basics and Concepts”, Chapter
[3] Benenti Gluliano , Casati Giulio, Strini Giuliano, “Principles of Quantum Computation and Information”, Vol 1:Basic Concept
[4] Aaronson Scott , “The Limits of Quantum”, Information Technolog
[5] Sanghvi Niramay , Varadan Varun ,Shah Avi, November 2014 , “The Concept and Future of Quantum Computing”, International Journal of Computer Application , Vol 106-No-
[6] Brandl I. Matthias , Nov 15, 2017, “A Quantum Von Neumann Architecture for Large-Scale Quantum Computing”
[7] Omer Bernhard , 20th Jan , 2000, “Quantum Programming in QCL”
[8] https:// www.allaboutcircuits.com /technical-articles/fundamental-of-quantum-computing/
[9] Dr. Chattopadhyay D., Dr. Rakshit P.C. ,” quantum mechanics statistical mechanics and solid state physics”
[10] Zettili Nouredine , Wiley, “ Quantum Mechanics- Concepts and Applications” Second Edition
[11] An overview of Indian Software Industry” Chapter 4
[12] Overview of Indian IT Industry” Chapter
[13] “ Think Beyond Ones and Zeros , Quantum Computing Now”, Accenture Lab
[14] Ms. Pritish , Dr. Saxena Taruna , October 2015,”An Analysis of the Indian Telecom Industry”, IOSR Journal of Business and Management, Vol 17, Issue 10, Ver.I
[15] “ IT & ITES” ,January 2017 , IBEF, www.ibef.org
[16] “IT-BPM Industry in India : Sustaining Growth and Investing for the Future” 22 June 2017, NASSCO
[17] “Indian IT/ITES Industry, Evolving Business Models for Sustained Growth” CII
[18] Report of the Working Group on Information Technology Sector, Twelfth Five Year Plan (2012-17) Govt. of India, Ministry of Communication & Information Technology , Department of Information Technology
[19] Twelfth Five Year Plan (2012-17) Faster, More Inclusive and Sustainable Growth, Volume
[20] meity.gov.in/content/IT-Masses-O
[21] https:// mamidala.wordpress.com/2014/06/25/quantum-computing-in-India-an-opportunity-that-should-not-be-missed
[22] http:// indianexpress.com/article/technology/science/quantum-computing-as-the-future-here-why-it-is-still-waiting-for-the-hardware-4776855
[23] “Innovating with Quantum Computing , Enterprise experimentation provides view into future of computing” Accenture
[24] Srivastava Rupesh , Choi Iris , Cook Tim , December 2016 , “ The Commercial Prospects for Quantum Computing “, NQUIT User Engagement Tea
[25] Montanaro Ashley , 25 february 2013, “ Quantum Computing Applications”, University of Bristol
[26] Report , June 2015 , “ Quantum Technology : From Research to Application”, Leopoldina , Acatech , Unio
[27] Swaim L.Travis , “Quantum Computing and Cryptography Today : Preparaing for a Breakdown”, University of Maryland University Colleg
[28] “Quantum Computing : The Risk to Existing Encryption Methods”, Computer Systems Security , Tufts Universit
[29] ETSI White Paper No. 8, June 2015, “Quantum Safe Cryptography and Security , An Introduction, Benefits , Enablers and Challenges”, ISBN No.979-10-92620-03-0
[30] Barreno A.Marco , July 21, 2002, “The Future of Cryptography Under Quantum Computers , Dartmouth College Computer Science Technical Report
[31] chsoftwarequality.techtarget.com

[32] searchnetworking.techtarget.co
[33] Chandrasekhar C.P., " ICT in a Developing Country Context : An Indian Case Study", Jawaharlal Nehru Universit
[34] Jussawalla Meheroo ,Taylor Richard, Pai Sunyeen , November 2001, "Lessons of Investment in Technology Parks and Thrie Role in Bridging the Digital Divide", The World Development Federation
[35] Kirkman S.Geoffrey , Cornelius K.Peter, Sachs D. Jaffrey , Schwab Klaus , 2002,"The Global Information Technology Report 2001-2002 , Readiness for the Networked World", Oxford University Press, World Economic Foru
[36] Kumar Nagesh , K.J. Joseph, April 2005, "Export of Software and Business Process Outsourcing from Developing Countries: Lessons from the Indian Experience", Asia-Pacific Trade and Investment Review, Vol.1, No.
[37] Vulk Cornelis , Moller Matthias , 19th June 2017, " On the impact of quantum computing technology on future developments in high-performance scientific computing " Ethics and Information Technology
[38] Rahaman Mijanur , Md. Islam Masudul , 2016, " an Overview on Quantum Computing as a service (QCaS) : Probability or Possibility", I.J.Mathematical Sciences and Computing, 1, 16-22, MECS
[39] https:// www.ibef.org/industry/information/technology/India.aspx
[40] www.statista.com/statistic/320776/Contribution-of--Indian-IT-Industry-to-India's-GDP
[41] Binkley Steve , April 5 ,2016,"Quantum Computing(and Quantum Information Science)", ASCSC Quantum
[42] Innovating with quantum Computing", Accentur
[43] Lewis .M.A, Kramer M, Tranaguin M , 31st March,2016, "Quantum Technologies Implications for European Policy", European Commission