Sample Student Draft of the Research Project with Comments in Bold

In today’s technology oriented society, computers lie at the heart of nearly every industry. “In today’s society” is just a kiss-of-death phrase for an intro; think of other, jazzier ways to introduce your point] As computing power grows rapidly, the demand for even more power grows with it. People have come to expect more and more things to be done instantly, things that once were impossible, or at the very best things that would have taken days or weeks to complete. This demand has left scientists searching for new ways of increasing the speed of computers, ways that will increase speed not incrementally, but rather exponentially. As power increases, scientists have come to realize that today’s modern silicon computer chips won’t be able to keep up with demand much longer. The so-called next generation of computers has to be based on something else, something which will allow for drastically faster processing capabilities. This generation of computers will be based on quantum theory, which will allow computers to do previously impossible calculations in near real-time. Quantum theory essentially says that very tiny particles, things too small to be seen with the naked eye, obey a different set of laws than ordinary macroscopic items. This law states that a tiny particle (a quantum) can move from one place to another, without ever existing at any point in between. [this still seems so weird to me – how can it not exist as it is moving from point A to point B? Of course, if you could clarify this, you’d probably be up for a Nobel Prize, so I’m not sure you can do more than tell us this!] While nearly everything will be affected by quantum computers, at least everything that uses computers now, and many more aspects of life that were previously not even connected to computers, the field of encryption may benefit the most from this new-found
computing power. [Is there any way of explaining how this movement of quanta (?) makes sense for computing applications? Wait... you do this below]

In a modern computer, information is stored, moved, and manipulated using what are called binary digits or “bits.” These bits are represented either by a 0 or 1, also called an off or on. Information is represented in series of these bits, such that two bits have four possible combinations (00, 01, 10, and 11) and 3 bits would have 8 possible combinations and so on. In a quantum computer, information is represented by quantum bits (qbits). Each of these qbits can represent a 0, 1, but also can represent two other states, states falling somewhere between a 0 and 1 that are difficult to show on paper, but at the same time are highly useful when put into practice. [OK, you do go into this a bit more here] A 2 qbits would represent 16 possible combinations and 3 qbits could comprise 64 different combinations, etc. So with the addition of each bit, the number of theoretical combinations represented by a qbit is exponentially larger than that of the classical two bit binary system. For each additional bit, the difference between a binary system and a quantum system is multiplied. Another huge fundamental difference in classical and quantum computers is the way operations are performed on the bits. While a binary-based computer must perform one operation at a time (or with multiple processors a number of operations equal to the number of processors), a quantum computer can perform an operation on every single qbit at the same time. Supposing 100 operations needed to be performed on 100 bits, a quantum computer would take 100 ticks of an imaginary clock (not actually seconds), whereas a binary computer would take 100x100, or 10,000 ticks of this same clock. Not only that, but the quantum computer with 100 bits could store over $10^{30}$ times as much information as the binary computer.
Building these quantum computers has turned out to be surprisingly easy; however, building quantum computers that are reusable, or that are reliable has proven to be incredibly difficult. Small 3 and 4 qbit computers that are able to perform basic arithmetic are already possible. The problem with these computers has been reading the data without causing the computer to essentially “disappear”. This idea of quantum bits “disappearing” while the computer is in operation is known as decoherence. Decoherence occurs when these tiny quantum particles interact with their environment. In an ordinary classical computer, bits are merely carried as an electrical signal, and electrical signal is highly predictable as it follows the path of least resistance. In a quantum computer, however, bits are hard to control, because they are on the atomic and/or subatomic level, and therefore could spontaneously be absorbed by whatever medium they are flowing through. Computer Business Review (italicize titles) seems to have put this problem best by likening controlling a quantum computer to controlling the waves on the surface of a pond: anything you do to it is going to cause more waves which interact with the original waves. While there are many different solutions proposed to help detect, prevent, and/or correct these errors, none are yet perfect, or even “good enough”. The problem with trying to detect errors in a quantum computer lies in that by viewing an atomic particle, it can, and generally will, alter the state of the particle.

While viable solutions that will allow for commercialization of quantum computers are nowhere in the foreseeable future, several working prototypes have been demonstrated in the past three years. The first quantum computer, which was merely 3 bits in size, was developed at Los Alamos National Laboratory in 1999. In 2000, IBM developed a small quantum computer with five atoms, which serve as both the memory
and processor. Even though this tiny computer is capable of only the most basic computations (and is only useful for a fraction of a second), it was a step in the right direction. Just earlier this year a Japanese team of researchers was able to build one of the fundamental pieces of logic necessary (a small gate which performs operations on the bits) for a fully functional computer. This team of researchers had already demonstrated the other fundamental element in 1999, although they have yet to put the two together which would be essential for a functional machine. Another major problem with this team’s breakthrough is that this machine was only functional for a few hundred picoseconds, or a few hundred trillionths of a second. One operation takes approximately 15 picoseconds to perform, and therefore this “computer” is only useful for a few operations before it completely collapses and is rendered useless. Until the problem of decoherence is solved, all of these advancements will be helpful, but at the same time they will not lead to a functional computer. In order for quantum computers to become useful in the marketplace, they must be infinitely reusable, or at least to the extent that a modern microprocessor lasts for many years before it fails to work properly. Even without a “useful” lifespan, any developments in quantum computing are seen as huge advances because basic theorems can be tested, analyzed and if the need arises, modified, so that quantum computers can be fully utilized as soon as they are stable.

By testing quantum computers, even though they only work for a fraction of a second at this time, researchers are able to prove (or disprove) the basic principles that will allow programmers of the future to write for a quantum computer. Everything must be entirely redesigned to function on a quantum computer. The very simplest moving of data or addition and subtraction will have entirely different underlying processes which
make them functional on a quantum computer. Today’s binary computers are highly simplified in relation to a quantum computer, and therefore writing a program for a quantum computer cannot be written in the same way as modern programs are.

Earlier this year the first company entirely devoted to building a quantum computer was formed. D-Wave Systems is a recent startup based in Vancouver, Canada, and funded primarily by Draper Fisher Jurvetson, a highly successful venture firm in Silicon Valley. While the CEO of D-Wave believes their quantum computers could be more powerful than any current supercomputer in a matter of just 5 years, others are far more skeptical. Although no breakthroughs have come from this company yet, Tim Blair of IBM concedes that they too are making progress just like everyone else. Aside from this new company, the majority of progress in quantum computing has come from IBM (which works in conjunction with Stanford), MIT, and NEC Corporation (which works in cooperation with Japan’s Institute of Physical and Chemical Research). Until this point, IBM and NEC have been the source of almost all of the major breakthroughs in quantum computing. D-Wave, which promises to make huge steps in a short amount of time, unfortunately has not accomplished anything major up to this point, and doesn’t even have anything listed under “News” on their website. Although nothing yet has been developed by this company, it’s not to say nothing will, and regardless, funding from one major investment firm could lead to funding from others. If enough companies are provided with ample funding, research should progress more quickly than if only three or four companies are working on this task.

Although the full potential of quantum computers may in fact never be realized, even what would normally be considered a partial success will yield enormous results.
The first place quantum computers will be used is in everyday searching. Be it searching the entire internet, a large company database, or just searching through a long text file for a particular word, quantum computers will have the ability to make this near instantaneous, regardless of the size of what is being searched. As the internet continues to grow, searching the entire internet takes more and more processing power. Google, the largest search engine in the world, runs on thousands of computers, and uses a highly efficient search algorithm in order to return results in a timely manner. Something this large or even many times this large, could easily be replaced in the future by one quantum computer. Although Google is indeed a unique case, almost any commerce type website has a large database, and since these businesses cannot usually afford thousands of computers, search results are not returned as expeditiously as many would like.

This is an excellent draft, Tommy – informative, interesting, well-written… but it needs a punchier introduction, and it needs outside voices – it needs quotation, speculation, from scientists working in the field. Who are the big guns in quantum research? Anyone come up repeatedly in articles or interviews? You have a great frame here, so you just need to take it to the next level with quotes.