GBBC Open-Source Ideas Series: Cybersecurity

Part II: Implications of Quantum Computing

8 April 2021

Bellevue, Washington, USA

Introduction

Technology continues to improve and advance at previously unthinkable speeds. Daily, we are barraged with new and exciting innovations that promise to forever alter the world around us. No doubt quantum computing will be that kind of technological advancement and then some.

When new technology disrupts our lives, we typically debate the implications of said technology. We are currently at that stage with quantum computing. As we all know, all things are not always favorable for all people; there are pros and cons to everything. This should not deter us, but rather motivate us. Quantum computing has the potential to bring such joy and increased quality of life for so many people that the risks of the technology in the hands of bad actors is all but a nuisance, albeit one we must solve.

So, we do. The greatest minds gather to dream, plan, and build the protections needed so that this new life-altering technology is free to change our world.

Quantum Computing: The Basics

Quantum computing processes and solves problems. Although it sounds easy, the physics behind quantum can leave many people scratching their heads. Quantum theory and mechanics is responsible for much of the technology we now use, including in devices such as LEDs and components in our computers.

Quantum mechanics is a fundamental physics theory that describes the physical properties of existence at the atomic and subatomic particles level. Quantum computers are computers that perform quantum computations using superposition and entanglement to solve problems.

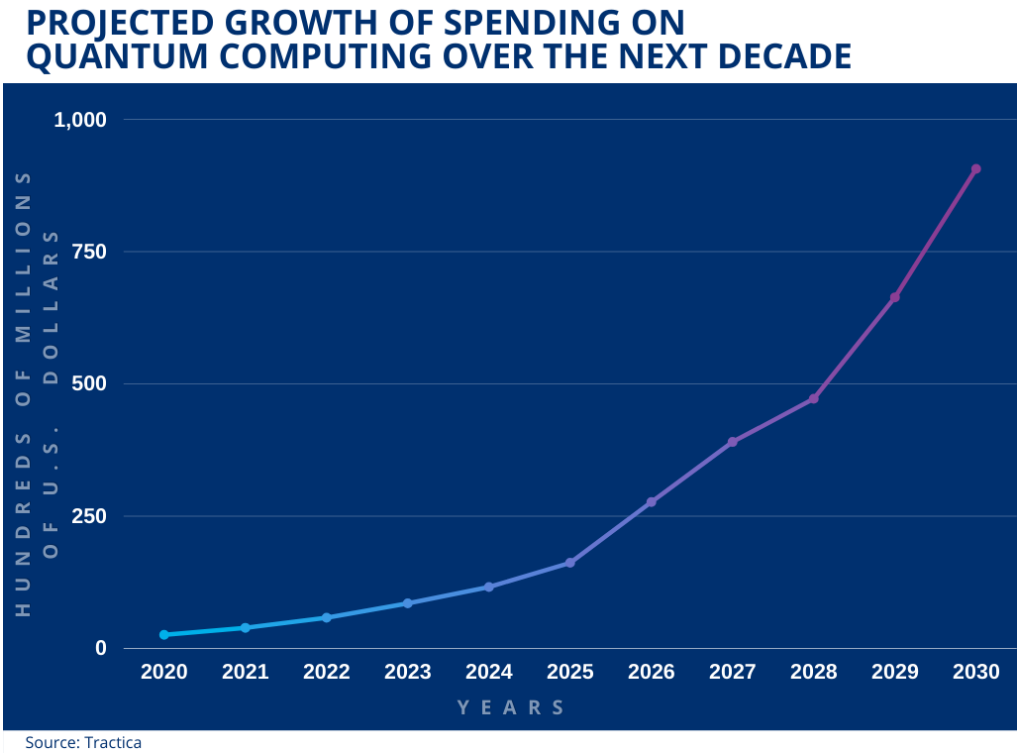
Most people have heard of 1s and 0s, known as bits. Bits are 1s or 0s and any combinations of the two and they represent data for processing by traditional computers. 4 bits will have every combination of 1s and 0s in groups of 4 digits. To crack a password, a traditional computer would try each of these number combinations, discarding the incorrect answers and keeping the correct one.

For quantum, those bits are not either 1s or 0s but are 1s, 0s, or 1s and 0s all at the same time. When using quantum bits (qubits), the quantum computer reads the combinations simultaneously; the result will be both correct and incorrect answers. Then an algorithm is applied to find just the correct answers. The algorithm will “sweep away” the incorrect answers and leave the correct answer.

The quantum computer will use this technique to work at excessive speeds to take today’s encrypted data and solve it in minutes, exposing our most sensitive data to bad actors. If this technology is such a threat, why, then are companies like IBM, Google, and others investing billions of dollars in quantum computing if it puts our data at risk? Because it changes everything.

Future of the Industry

The potential range of applications for quantum computing is boundless, and will likely influence technology, optimization, modeling, and data analytics, creating unimaginable advancements in encryption, agriculture, and the discovery of new materials. Cancer could be eradicated. Clean energy is possible. Advanced artificial intelligence becomes a very real probability. With quantum poised to impact every industry, businesses will be spending billions on quantum computing, with some analysts expecting "spending on quantum computing to surge from $260 million in 2020 to $9.1 billion by the end of the decade."[i]



Businesses that require large computation power to solve problems are searching for ways to access quantum technology. Quantum-as-a-Service (QaaS) is a new concept for businesses and could grow significantly. This will enable businesses to access quantum computing services remotely. Amazon, Microsoft, and Google all offer a form of QaaS.

A quantum future looks promising but is not yet assured. Issues such as quantum's fragility and its current inability to network processors must be addressed before these use cases can be realized. However, if the last decade's technical advances are any indicator, we should prepare for a quantum environment by allocating resources and protecting our infrastructures from the sudden proliferation of quantum technology.

Effects on the Security of Important Systems

Encryption

In a quantum environment, some encryption algorithms are very easy to break. Shor's algorithm shows that most of what is difficult in a classical computing environment becomes trivial in a quantum computing environment. These include PKI/PKE.

Public Key Infrastructure (PKI) is the "framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates."[ii] Public Key Enablement (PKE) makes sure applications can use the PKI framework. These basic encryption algorithms are used to keep sensitive data and electronic communications secure; this includes those used by most governments and businesses today.

RSA, one of the types of public key cryptography algorithms in PKI/PKE, is used by classical computing to encrypt and decrypt messages and uses a two-key cryptographic algorithm. RSA encryption is most at risk because of the sheer computational ability of a quantum computer. Notably, for some encryption algorithms, "quantum computing might allow those without the key to sidestep entirely the need to do brute-force search by, for example, enabling a key extraction algorithm that can find the decryption key directly without a blind search."[iii]

The systems that protect financial transactions, encrypted communications, and identification all depend on RSA encryption and would be rendered obsolete with quantum computing in the hands of bad actors.

Blockchain

Blockchain technology and cryptocurrencies such as Bitcoin and Ethereum use two key encryptions and are not immune to the dangers of quantum. Blockchain's vulnerability from quantum computing in the hands of bad actors is twofold. The first is related to public key addresses, otherwise known as p2pk. With p2pk, it is possible for even a small quantum computer that can operate Shor's algorithm to deduce the private key from the public key. Once hackers have the private key, they control the transaction. According to Deloitte, "about 25% of the Bitcoins in circulation are vulnerable to a quantum attack. If you have Bitcoins in a vulnerable address and believe that progress in quantum computing is more advanced than publicly known, then you should probably transfer your coins to a new p2pkh address."[iv]

Another vulnerability to the blockchain is quantum's sheer speed. In time, as quantum computers become faster, they will be strong enough to decode and interact with transactions while "in transit", jeopardizing the decentralized system's integrity. For example, a bad actor could decode the private key in the 10 minutes it takes for the transaction to complete to the Bitcoin blockchain. Once they had the private key, they could re-route the transaction to themselves. The implications of this grow each day as blockchain technology is increasingly being used in asset trading, supply chains, identity management, healthcare, and the public sector.

Digital Infrastructure

Even without the threat of quantum computing, supply chains, healthcare, and energy are some of the most targeted infrastructures for hackers. There are several places bad actors could easily access a supply chain, and today's suppliers and vendors are generally not proactive in securing those areas. This leaves the supply chain vulnerable to attacks.

Quantum's effect on digital infrastructure then becomes a double-edged sword. Although quantum would be highly beneficial, the security implications of the technology in the wrong hands could be catastrophic to any system. With businesses and governments unable to guarantee data integrity and security, quantum could compromise vast amounts of data.

As discussed earlier, Shor's algorithm in quantum computers will treat most of today's encryption standards like candy. These quantum computers can change financial transactions and government communications. Nations are in a quantum race to not only be the first to achieve a technological breakthrough but also to protect their infrastructures from bad actors, including one another. The first countries to have access to quantum computing devices could realize enormous financial, military, and societal benefits.

How can these systems prepare for quantum computing?

Encryption

While the public at large may be unaware of the looming threat of quantum computing to the security of our infrastructures, governments are allocating significant resources to research and development programs to advance quantum computing initiatives.

Jarred by the inevitable risks posed by quantum computers, businesses, and governments, including the US National Institute of Standards and Technology (NIST), are moving to secure our infrastructures.

For the last three years NIST has been "examining new approaches to encryption and data protection that could defeat an assault from a quantum computer" and recently "winnowed the 69 submissions it initially received down to a final group of 15. NIST has now begun the third round of public review. This 'selection round' will help the agency decide on the small subset of these algorithms that will form the core of the first post-quantum cryptography standard."[v]

Congress has passed initiatives such as the National Quantum Initiative Act to "establish the goals and priorities for a 10-year plan to accelerate the development of quantum information science and technology applications."[vi] In addition to NIST's post-quantum cryptography challenge, they also have draft approval of a new quantum-resistant signature scheme called eXtended Merkle Signature Scheme (XMSS).

Blockchain

As it stands, the Bitcoin blockchain is resistant to quantum attacks with a few caveats. In the Bitcoin blockchain, it currently takes about 10 minutes for transactions to be mined. Bad actors hoping to circumvent and redirect a transaction will remain unsuccessful as long as redirecting takes longer than 10 minutes. Currently, it is estimated that it would take 8 hours for quantum computers to break the underlying hashing and encryption.

Newer p2pkh addresses that contain only a hash of the keys instead of the entire address as seen with p2pk addresses make it impossible to derive the private key from the public key because the full public key is not exposed. However, as soon as someone makes a transfer, the address is revealed, and that private key can be derived from the public key. Any subsequent usage of that public address exposes the user to the same quantum attacks as p2pk addresses. Therefore, as long as people do not reuse the public address to make any additional transfers, the address remains safe.

Some have speculated that even if people take steps to protect their keys, "quantum computers might eventually become so fast that they will undermine the Bitcoin transaction process. In this case the security of the Bitcoin blockchain will be fundamentally broken. The only solution in this case is to transition to a new type of cryptography called 'post-quantum cryptography', which is considered to be inherently resistant to quantum attacks."[vii] Blockchain developers are acutely aware of the threat to established networks like Bitcoin and Ethereum. Many are experimenting with quantum-resistant protocols. However, these protocols are not immediately available and may not be implemented in time to protect the network.

Digital Infrastructure

With the imminent threat of quantum computing, governments and businesses need to implement quantum protections now. Experts have recommended that, given "the possibility of large-scale quantum computers in the next two decades, and the legal requirements to protect some forms of classified data for at least two decades, government agencies should begin using quantum-safe encryption for security-critical data."[viii]

The challenge lies in the fact that computers and IoT devices are not built to defend against a quantum attack. These devices require interoperable solutions to protect them against bad actors at scale. Many companies are focused on post-quantum algorithms that are used in parallel with traditional algorithms. When new quantum-safe cryptographic algorithms are available, the hybrid approach will use a combination of post-quantum signature and hashing techniques.

With Honeywell announcing the world's fastest quantum computer,[ix] it seems time is not on our side. Digital Fortress includes a suite of tools that, when used together, are not quantum-resistant but quantum-safe.

Digital Fortress

As mentioned earlier, most sensitive data is encrypted with public-key encryption. Quantum computing finds asymmetric algorithms easy to break. For that reason, symmetric algorithms are being investigated, though to use symmetric algorithms, keyspace must at least double. With Digital Fortress's polymorphic technologies, it is possible to multiply the keyspace by a factor in the thousands. This compression technique makes the keyspace many times larger with very little incremental effort.

Using these long symmetric algorithms, even with compression applied, can generate patterns in the data. Anytime you see patterns emerge, those patterns can quickly be exploited. A symmetric key generated by the polymorphic random number generator never cycles, thereby eliminating patterns in long strings of numbers. The result is a key that cannot be derived, as the numbers are an ever-evolving set of random information. The data itself is broken into tiny shards and distributed across a network encrypted with data camouflage.

Data Camouflage is a process that takes a message and puts a string of random numbers next to the data. An application in the file randomly flips the bits of data. Someone may be able to know what percentage of bits have been flipped but when and where the bits flipped is completely random. The result is a damaged file intertwined with an intact file and an inability to distinguish between the two.

Earlier it was mentioned that quantum algorithms will "sweep away" the wrong answers and leave the correct answers. When using the technique of data camouflage, damaged files are inserted into pixels containing intact files. The quantum computer gets distracted trying to figure out why this file is damaged, gets "bogged down" and unsure of what to do, and thus "sweeps away" the entire file.

Blockchain provides the perfect avenue for implementing polymorphic technologies as seen in the Digital Fortress. Blockchain naturally has small fragments of data in each block and is perfect for a shard. When polymorphic encryption is applied to blocks, the result is much better encryption, quickly, without bogging down systems.

Digital Fortress is a sector agnostic system that combines interoperability between systems and quantum-safe cybersecurity. Dragonchain's patented interoperability system, Interchain, connects disparate systems that otherwise would still struggle with connectivity. Organizations can finally overcome the roadblocks to interoperability and the barriers to quantum protection. Interchain is interoperable with any traditional system through RESTful APIs. This allows any supply chain, accounting system, IT system, health records database, or any application to capitalize on quantum-safe encryption right now.

The Digital Fortress includes Dragonchain's hybrid blockchain platform to support selective transparency, where only the proof is decentralized to Dragon Net, Bitcoin, and Ethereum for verification. Sensitive data remains at the business level, protected by quantum-safe polymorphic

encryption integrated at the core of the architecture. The system offers secure GDPR/HIPAA/CCPA capable compliance to protect personally identifiable information (PII).

Breaching a system secured by the Digital Fortress would require one to compromise Bitcoin *and* Ethereum *and* all Interchained networks *and* all five levels of Dragon Net's decentralized consensus protocol *and* the business' private blockchain node *and* quantum-safe encryption. The Digital Fortress protects sensitive information from quantum attacks and simultaneously decentralizes the proof of the data integrity and origin.

Final Thoughts

The foundation of cybersecurity is broken. Our security infrastructure was built on the assumption that there would never be enough computing power to break modern algorithms. We now know that to be misguided. Solutions for securing our infrastructures on a global scale will take many forms. Establishing and incentivizing a set of ethical principles, while admirable, will neglect to capture all systems and devices leaving windows open for bad actors. Organizations must commit to building on strong, secure foundations. Data must remain secure whether it is at rest or in motion. Every computer and IoT device must remain quantum-safe at all times.

Government and enterprise leaders will need education on the risks associated with quantum computing when in the hands of bad actors. These leaders will be the first to analyze and implement the counter measures needed. With the conclusion of NIST's post-quantum cryptography challenge, global standards for organizations may offer a path to quantum resistance. These standards may ensure international interoperability *if* all organizations adhere to the guidelines.

By reducing the obstacles of implementing quantum-safe technology, our systems can be protected today for what lies ahead.

---

[i] https://www.cnet.com/news/amazon-ibm-and-microsoft-race-to-bring-global-access-to-quantum-computing/

[ii] https://csrc.nist.gov/glossary/term/PKI#:~:text=Definition(s)%3A,destruction%20of%20public%20key%20certificates

[iii] https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985

[iv] https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

[v] https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

[vi] https://www.congress.gov/bill/115th-congress/house-bill/6227

[vii] https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

[viii] https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985

[ix] https://www.honeywell.com/us/en/news/2020/06/the-worlds-highest-performing-quantum-computer-is-here