Quantum Computing: The Catalyst for a Decentralized Internet

Cian Duffy, 18322506

***Abstract*—This paper seeks to identify the shortcomings of the current attempt at a decentralized internet. It utilizes proofs from various published research papers to propose a decentralized internet using quantum computing. It will identify the real-world applications of this proposed system and explore whether it can be a valid alternative to the status quo.**

***Index Terms*—quantum computing, decentralization**

I. Introduction

In 1989, Tim Berners-Lee proposed a system that would go on to become the worldwide web. On its 25th anniversary, Berners-Lee stated his belief that the system is under threat from government bodies and businesses that intend on polarising the internet [1]. His observation reflects an increasing wariness of the censorship, surveillance, and profiteering of the internet and its users. The recent shift from desktop applications (that run locally on a user's machine) to cloud based applications (that run on remote servers) has created these new risks.

This paper will investigate the costs and benefits of a large-scale shift from the current centralized internet to a fully decentralized one, using various technologies. It will identify the factors that inhibit the growth of these technologies concerning their underlying computational methods. The paper also aims to provide an updated design that implements the dynamic and rapidly developing field of quantum computing. An assessment will be made on the security, scalability, and performance of a decentralized web, and how an implementation of quantum computing can improve these metrics.

II. Decentralization

A. Current Internet Architecture

The centralization of the internet can be explained by its underlying architecture and how it can be controlled. If a person wishes to search for a specific website, they make a request which must be satisfied by a specific server that hosts that website. For the request to reach that specific server, the request is handled by the domain name server (DNS) hierarchy, a server hosting company, and often a third party to a web hosting service. This process repeats every time a person attempts to access a website. However, the recent shift to cloud services which allow large corporations to host data presents a problem: it is now easier than ever for governments and private corporations to exploit and supervise a user's activity through these centralized services.

Figure 1) illustrates that, as of January 2020, Google facilitated 90% of all searches made on the internet worldwide. All of this internet traffic is gathered and processed by Google to improve advertisement targeting. This example is just one demonstration of the ways in which privatized corporations can benefit from the current centralization of the internet.

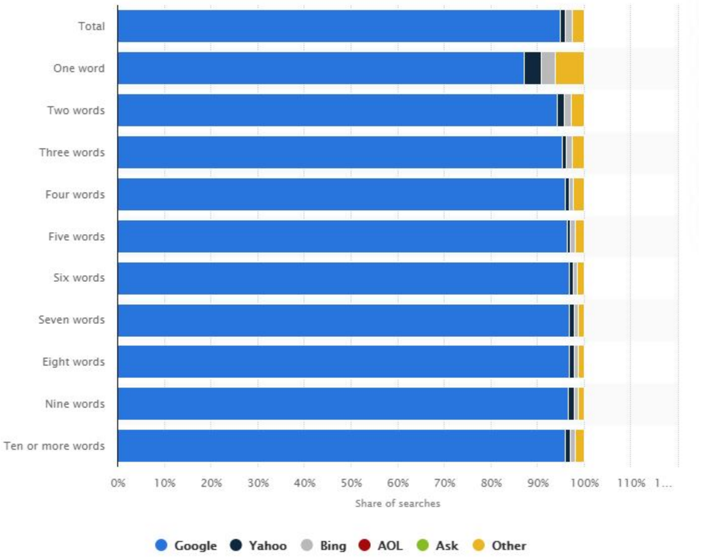

Fig. 1. internet search statistics [2]

B. Blockstack

The initial development of the internet aimed at providing a decentralised service. However, under the system today, big tech companies appear to hold a monopoly on data. It is, therefore, perhaps more apt to describe today's efforts at decentralization as "re-decentralization".

An example of this is Blockstack, a platform for decentralized internet applications using the blockchain name system (BNS) as opposed to the aforementioned DNS. For a fully decentralized web to be a valid alternative to the currently integrated system, it must provide comparable performance while eliminating the privacy concerns identified above.

To understand how Blockstack achieves this goal the underlying protocols and systems it uses has to be analysed. Each user must have the ability to bypass a centralized server when, for example, searching for a website. The user must also have the ability to establish trust on the network independently. This challenge is overcome through the use of blockchain, a peer-to-peer network, and a decentralized storage system [3]. These components identify the three layers of Blockstack's system architecture and will be explored in greater detail below where an examination of the scalability and privacy concerns of the system will be made.

Now that the motivation behind a decentralized web has been conveyed, an exploration of the technicalities of the system is required. The purpose of this is to justify its scalability and privacy, especially when compared to the current core internet infrastructure.

III. Assessment of Blockstack Design

This section will provide a detailed assessment of the security, scalability, and performance of a decentralized web. By exploring how one of the world's leading decentralized platforms works, on a fundamental level, its effectiveness can be assessed.

A. Security

There is much debate surrounding the use of DNS and its privacy concerns. It is responsible for network location addressing by tying IP addresses to human readable names. For instance, when a person searches for a specific website, DNS converts that name to the IP address of the centralized web server that hosts that website, which can be displayed to the end-user. However, there is an important caveat to this: the information cannot be guaranteed and can be susceptible to network attacks like system spoofing. A network attack occurs when a user's request is redirected to steal private information. A malicious third party user, by the act of system spoofing, can disguise their insecure connection as a secure connection to carry out the network attack [4].

Blockstack is able to overcome this through the implementation of BNS. BNS is an alternative to DNS and is built using blockchain, a system whereby access and transmission security is maintained by multiple parties in a peer-to-peer network. This key feature ensures that the previous security faults are eliminated by each node or peer maintaining their own copy of DNS records. A consensus is driven by algorithms such as proof of work (POW) and proof of stake (POS) where cryptographic keys are used as a means of ensuring appropriate access to data. Now that the entire network has an agreed-upon ledger, known as the blockchain record, website requests are handled locally by retrieving blockchain data which will satisfy the request and can be certified using the secure key check.

B. Scalability

The next question is whether the same scalability of "traditional" cloud/server storage can be achieved by this new decentralized approach. It is clear that peer-to-peer networking requires each user or node to be in total agreement for a robust system. Therefore, the scalability of the system is intrinsically linked to its underlying components and in this case blockchain.

Blockstack's answer to decentralized storage (as opposed to centralized server/cloud storage) comes in the form of Gaia, where a user's saved data generated by apps and services are stored on blockchain-based backends owned by the user. With more users joining the system the computational power necessary to sustain the blockchain grows and is a primary cause of concern regarding this technology.

Take Bitcoin, for example, which has gained much traction in contemporary mainstream media. It is one of the largest cryptocurrencies and is built on the same technology that is being discussed, where the speed of transactions completed is dependent on the number of transactions and interval time of each block. Due to its increase in popularity and use, single transactions can take up to a total of ten minutes (transaction size and block frequency causes variance) [5]. This low throughput of transactions is due to the underlying capabilities of the blockchain and is also apparent in the design specifications for the decentralized storage of data.

Another major concern for this system is whether it will handle the same traffic that major tech companies such as Google and Microsoft receive today. This is identified as one of the potential drawbacks of creating such a secure and distributed system.

C. Performance

The scalability concerns, due to the computational bottleneck described above, are directly linked to the number of transactions or in this case memory accesses that are required. Given that Blockstack is not experiencing the same activity, due to the small community of developers using it, it ensures performance is comparable to that of current centralized systems. The Gaia system (Blockstack's storage system) itself performs well due to the small overheads introduced by the security measures it provides. Encryption for file uploading and decryption for file downloading introduce negligible wait times. It is important to note that this may vary due to different internet service providers.

In summary, this approach to a decentralized internet introduces a new level of privacy and security that strongly competes with the issues faced by today's standards. It gives data ownership back to the user which eliminates the possibility of corporate exploitation, whilst also ensuring the security of that data. By doing this, it is clear to see that a decentralized web is becoming a viable option over the currently integrated service that is offered by major tech companies.

A major obstacle in the successful deployment of this service, however, is caused by scalability concerns. The requirements of the blockchain are simply not met as the total active users begin to rise [6]. When the system gives the power back to the user, in terms of security, it also relies on the user for the computation to do so. As the number of users rises the power needed to run the blockchain simply isn't sufficiently met.

IV. Quantum Computing

The deployment of a decentralized web has faced some challenges specific to the blockchain capabilities that have been identified above. Current efforts are being made to overcome the scalability problem by using methods such as increasing block sizes and processing transactions in parallel, but these solutions also have consequences.

The obstacle to deploying the blockchain system to business environments and the general public lies in the limited storage and computational resources of each node or user. A possible solution to this may be found in the field of quantum computing.

The aim here is to show that through the use of quantum computing, the scalability and efficiency of blockchain can be improved.

A. Blockchain

To reiterate, blockchain refers to a network of nodes, where each node has a shared ledger with a history of transactions. Each block in the chain contains the most recent transactions and each node has access to this ensuring constant agreement. The execution of this "proof of work" method requires computational power, and in the case of Bitcoin, anyone with sufficient computer components can lend their computational power to the system for rewards. This involves creating a block header or otherwise known as a digital fingerprint, generated by a hash function linking each block. This is a type of encoding process which takes information, such as several transactions, in the form of 1s and 0s and generates an alphanumeric hash code. It encodes all transactions in linked blocks with this cryptographic hash function so that the hash of each block is dependent on the hash of all previous blocks. If this digital history of transactions is changed by one malicious node or user, then the hash will not be consistent, and the system will know not to trust it.

B. Quantum Bits

The fundamentals of all computation, within classical computers, originates from the representation of information through bits: 1s and 0s as just stated. 1 represents true and 0 represents false. Computers can send information through a network in the form of bits and modern cryptography provides a secure way of scrambling those bits. This occurs through the one-way hash function that was previously discussed in relation to the "proof of work" algorithm.

Naturally, the proof of work algorithm requires mass amounts of computational work that cannot be scaled because of the limitations of modern computers and how they execute the work. Quantum computers however, are not restricted by the same logic of 1s and 0s and differ in several of ways.

1) They use quantum bits where each quantum bit, or qubit, can represent a superposition of 1 and 0 as seen in Figure 2). So, if one qubit can be in a superposition of 2 states, then 2 qubits can be in a superposition of 4 states and 3 qubits a superposition of 8 states, and so on. This logarithmic increase of states shows that data can be represented more efficiently, and therefore, computation using these qubits takes less time.
2) Quantum computers benefit from the phenomena of quantum mechanics known as entanglement. If two qubits are said to be entangled, then the measurement of one can provide information on what will happen during the measurement of the second.

There is of course much more detail as to how quantum computers process these qubits. Simply understanding that quantum computing lends itself to quantum mechanics to achieve extreme computational power is sufficient for the current context [7]. With this fact, an investigation can be made into how a fully quantum blockchain at an abstract level can begin to remove the limitations that were identified above, and therefore, improve the validity of a fully decentralized and now quantum internet.

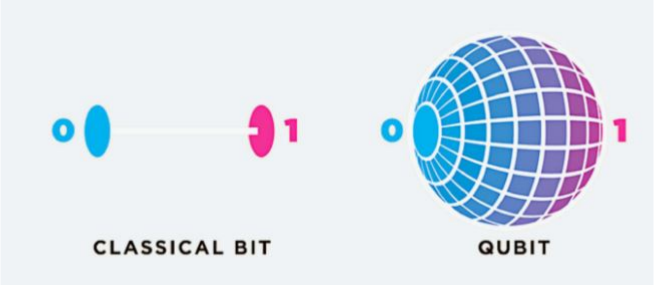

Fig. 2. Bit vs qubit [8]

C. Quantum Blockchain

It is important to note that the study of quantum computing is still very much in its infancy especially when compared to modern day classical computers. However, they do exist, and IBM even offers an online platform where users can develop software and run it using their quantum systems [9]. The full-scale implementation of such devices requires more development in the field, but proposals and research can still be made using what is currently known about their architecture and capabilities.

One such proposal describes the possible implementation of a quantum system to replace the data structure in the classical blockchain system. The proposed system recreates the chain through the entanglement of qubits and is "experimentally realizable" [10]. Essentially, the system encodes a blockchain using the entangled qubits to then be integrated into a fully quantum network. One of the main advantages of this is that entangled qubits cannot be copied and any attempt to do so will be detected due to its quantum state. This is known as the "No Clone Theorem".

This forms the basis for Quantum Key Distribution or QKD. Although QKD does not transmit data it can be utilized with any encryption method to encode a message. According to the no clone theorem, it is provably secure. This renders the scalability problems of the system invalid as the computational power necessary to sustain it can be rectified by the efficiency of quantum computing.

V. Assessment of New Design

It is clear that quantum computing can lend itself to the current efforts of web decentralization. An updated assessment using the same categories as before can therefore be provided. An evaluation of a decentralized web through the use of quantum computing will be made.

A. Security

Blockstack's implementation of the blockchain domain name system showed a solution to the privacy concerns of traditional DNS, so this security must not be impeded by the use of quantum computing.

Let's say a person wanted to search through a list of 1 trillion items and every item took 1 microsecond to check. It would take a classical computer approximately one week to check each item, whereas a quantum computer could perform this task in one second.

There was initially some fear that a quantum computer could therefore break the security algorithms that make blockchain such a secure system, since the algorithms rely on the computational limitations of today. This technology has not only caused this problem but has also answered it. The new method of private data sharing that employs quantum computing (QKD) is "unbreakable" by both classical and quantum computers ensuring the same security offered by the standard blockchain [11].

B. Scalability

The scalability of the new proposed system has its associated strengths and weaknesses. One of the main strengths is the theoretical scalability of the system. Given that a proposal can be made for a more efficient quantum blockchain that is founded on provable quantum physics, then the initial scaling problem is no longer an issue.

In reality, quantum computing is potentially decades off being readily available to the majority of users that wish to participate in a decentralized internet. This of course, would be a major obstacle as the success of this system is reliant on the underlying technology of its users. The benefit of security has been established, although the scalability, in practice at least, remains yet to be fully explored.

C. Performance

Lastly, the performance of this system has proven troublesome to measure as it is purely a theoretical one. However, its subsystems are currently being realised with small-scale programmable quantum computers, and an educated projection of how the overall system will perform is possible. For example, the efficiency and performance of quantum key distribution can and has been assessed with extremely promising results [12].

The experimental results confirm the effectiveness of the technology concerning stable and efficient transmissions of data. Even though the system itself has not been implemented and tested, its subsystems have shown positive results which suggests a remarkable performance of the overall system.

VI. real-world Applications

There are two main topics of discussion relating to the real-world applications of the provided system. The first identifies the current concerns of the centralized web and how Blockstack can address them. The second explores the viability of quantum computing as it is a fundamental feature in this proposed system. In particular, whether the cost of integrating these new experimental systems into the already established environment are worth the benefits they will bring.

A. Government Censorship

One of the major examples that evokes the growing demand for a decentralized internet is the government censorship in China seen over the past two decades. This refers to the filtering of online information coming in and out of the country. Often referred to as the Great Chinese Firewall, this IP and DNS filtering means that internet users within the region can struggle to access online material from websites ranging from YouTube to Wikipedia [13]. The government bodies who uphold these censorship policies claim that it helps to maintain a stable society with a unified ideology.

In 2019, those same government bodies decided to ban any material associated with the cartoon character Winnie The Pooh, after images of this character were used online to mock the Chinese President Xi Jinping. This censorship is one of the leading motivations behind the Chinese citizens attempting to bypass this firewall.

A recent study found that citizens who successfully bypassed the firewall were 10 times more likely to express political views online as opposed to those who did not [14]. This indicates a negative response to government censorship. It stifles political debate and can be seen in many other countries today. Given that these censorship systems are founded upon DNS and IP, a decentralized web through the Blockstack platform provides a simple solution to increase the free flow of information not just pertaining to political discussion.

Growing unrest can be seen surrounding the centralization of information and data. Therefore, the real-world applications of a decentralized web are becoming more and more prominent.

B. Network Implementation

As previously discussed, the study of quantum computing is very much in its early stages of development. Nevertheless, real-world applications currently exist which will help to identify the future requirements of this technology. This proposal for quantum computing, in the context of decentralization, has helped to correct the weaknesses that arise with a scaled blockchain. One of the factors blocking the deployment of this technology is its availability. However, it can integrated using the currently available systems.

For this new paradigm of computing to be a viable option, today's network infrastructure must be altered to share and process quantum data. It has been shown that networking between quantum nodes can be designed using fibre-optic hardware similar to that of existing telecommunication equipment [15]. Not only does this reduce the cost of creating a new telecommunications network, which is dedicated to quantum networking, but it expands the real-world applications of this emerging technology.

C. Summary

The demand for a decentralized internet exists in today's world and has been shown to be quantifiable through various research papers and articles. The scalability concerns which impede the full-scale deployment, and therefore the real-world application, can be answered by the field of quantum computing. This furthers the interest and demand for this new innovative technology.

VII. Conclusion

This paper has sought to provide an assessment of the Blockstack system to measure the security, scalability, and performance metrics of a decentralized web. Within this assessment, it identified the weaknesses of this implementation due to scalability concerns. It proposed a new modified system where the underlying computation limitations were rectified through the use of quantum computing. By integrating the power of quantum computing into the blockchain system, a possible and practical design has been provided where a fully decentralized and quantum internet can be developed upon. The practicality of this system, although theoretical, is founded upon established research of its underlying technologies. Demand for such a system has also been identified and thereby furthers the real-world applications. As a result, this paper provides a possible design for the implementation of a decentralized and quantum internet.

References

[1] Berners-Lee, T. (2014, August 23). Tim Berners-Lee on the Web at 25: the past, present and future. WIRED UK; WIRED UK. https://www.wired.co.uk/article/tim-berners-lee

[2] Global online search query search platform share 2020 Statista. (2020). Statista; Statista. https://www.statista.com/statistics/413229/search-query-size-search-engine-share/

[3] Ali, M., Shea, R., Nelson, J., & Freedman, M. (2017). Blockstack: A New Decentralized internet. https://docs.huihoo.com/blockstack/Blockstack-A-New-Decentralized-internet.pdf

[4] Liu, Y., Zhang, Y., Zhu, S., & Chi, C. (2019). A Comparative Study of Blockchain-Based DNS Design. Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications. https://doi.org/10.1145/3376044.3376057

[5] avg-confirmation-time. Blockchain.com. https://www.blockchain.com/charts/avg-confirmation-time

[6] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A Survey on the Scalability of Blockchain Systems. IEEE Network, 33(5), 166–173. https://doi.org/10.1109/mnet.001.1800290

[7] Singh, J., & Singh, M. (2016). Evolution in Quantum Computing. 2016 International Conference System Modelling & Advancement in Research Trends (SMART). https://doi.org/10.1109/sysmart.2016.7894533

[8] K, A. (2021, April 12). An Introduction to Quantum Computing - Alex K - Medium. Medium; Medium. https://thealexk.medium.com/an-introduction-to-quantum-computing-e74450da46c6

[9] IBM Quantum. (2021). IBM Quantum. https://quantum-computing.ibm.com/

[10] Rajan, D., & Visser, M. (2019). Quantum Blockchain Using Entanglement in Time. Quantum Reports, 1(1), 3–11. https://doi.org/10.3390/quantum1010002

[11] Cui, W., Dou, T., & Yan, S. (2020). Threats and Opportunities: Blockchain meets Quantum Computation. 2020 39th Chinese Control Conference (CCC). https://doi.org/10.23919/ccc50068.2020.9189608

[12] Zhao, B., Zha, X., Chen, Z., Shi, R., Wang, D., Peng, T., & Yan, L. (2020). Performance Analysis of Quantum Key Distribution Technology for Power Business. Applied Sciences, 10(8), 2906. https://doi.org/10.3390/app10082906

[13] Leskin, P. (2019, October 10). Here are all the major US tech companies blocked behind China's "Great Firewall." Business Insider; Business Insider. https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5?r=US&IR=T#flickr-16

[14] Zhang, C. (2020). Who bypasses the Great Firewall in China? First Monday. https://doi.org/10.5210/fm.v25i4.10256

[15] Treiber, A., Poppe, A., Hentsche, M., Lorunser, T., Hubel, H., & Zeilinger, A. (2009). Reliable hands-off entanglement-based QKD system for fiber networks. CLEO/Europe - EQEC 2009 - European Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference. https://doi.org/10.1109/cleoe-eqec.2009.5194792