International Journal of Enterprise Information Systems
Volume 17 • Issue 4

From Far East to Baltic Sea:
Impact of Quantum Computers on Supply Chain Users of Blockchain

Fakhreddin F. Rad, Södertörn University, Sweden

ABSTRACT

This study conceptually investigates the impact of quantum computers on blockchains within the supply chain context. Powerful quantum computers enable attackers to break into blockchains by rapid inverse calculations of mathematical problems that are the core of one of the main blockchain security foundations, known as asymmetric cryptography. They are also able to violate the integrity of public blockchains like bitcoin through mining acceleration. Hence, quantum computers can engender threats to the supply chain users of blockchain. On the other hand, there are ongoing efforts to create a quantum-resistant solution. One approach for such a solution is to utilize quantum tools themselves. Moreover, sufficiently powerful quantum computers are still being developed, and it is still unclear whether a quantum solution will arrive first or vice versa. The contrasting duality of quantum computers and lack of a clear picture over the timing of the arrival of a solution and threats give rise to the uncertainty that might hinder the attractiveness of blockchains for supply chains.

KEYWORDS

Asymmetric Cryptography, Authentication, Efficiency, Hash Function, Immutability, One-Way Function, Principle-Agent Theory, Smart Contract, Transaction Cost Theory, Transparency, Uncertainty

INTRODUCTION

Blockchain growth in various areas is evident throughout the world. While the US and China are the leaders, Europe also strives to maximize its blockchain potential (Anderberg et al., 2019; Firdaus et al., 2019; Liu, 2020). In a survey among European businesses, half of the respondents perceived that blockchain would impact their current operating models (O'Dea, 2020). Well-established firms in the EU, such as Danish Maersk, German BASF, and Bosch are already involved with blockchain technology (Hackius & Petersen, 2017; Kouhizadeh et al., 2020). In addition, blockchain investment examples can be found in other European countries' large firms, such as Russian Gazprom (Khatri, 2019). The United Kingdom, Germany, France, and Estonia have the highest number of blockchain startups in the EU (Anderberg et al., 2019). The worldwide amount of financial resources directed to blockchain solutions demonstrate continuous growth, from 1.5 billion U.S dollars in 2018 to the estimation of 15.9 billion by 2023 (Liu, 2020). The PwC's survey of 600 executives in 2018 revealed

DOI: 10.4018/IJEIS.2021100105

that 84% of the companies have already had a certain degree of involvement with blockchains (Davies & Likens, 2018).

The advent of industry 4.0 (also known as digitalization) has unfolded revolutionary promises to the business landscape. In this regard, blockchain is one of the underlying technologies of industry 4.0 that can play an important role in its success (Ghobakhloo, 2018; Schwab & Davis, 2018). Notwithstanding the significant investment across the world, blockchain technology is still evolving. Blockchain has not reached its maturity, as various aspects such as benefits and challenges are yet to be fully elaborated (Manners-Bell & Lyon, 2019; Van Hoek et al., 2019).

In this regard, quantum computers are one of the main matters that can engender a crucial impact on blockchains (Fernández-Caramès & Fraga-Lamas, 2020; Gheorghiu et al., 2017) and can have serious consequences for relevant investments. Quantum computers are referred to as machines that use quantum mechanics to execute computations that are, in many cases, performed faster than classical computers (DiVincenzo, 2000).

One of the blockchain use areas that can be significantly impacted by quantum computers is the supply chain. Blockchain offers important opportunities to supply chains such as transparency, immutability, and authenticability (Manners-Bell & Lyon, 2019; Van Hoek et al., 2019). There are various cases of blockchain utilization in supply chains. For example, Grass Roots uses blockchain with supply farms to create transparency on transferred content (Van Hoek et al., 2019). Maersk uses blockchain to replace hardcopies with digital content and to achieve transparency that enables shared views and collaboration among supply chain partners (Kouhizadeh et al., 2020).

However, the emergence of powerful quantum computers can affect all blockchain opportunities and investments. Quantum computers are a double-edged sword that can be part of the blockchain's security solution as well as the problem (Campbell, 2019; Gheorghiu et al., 2017). Such features require further investigations into the details of the subject to enhance pertinent understanding, improve certainty, and guide further actions. While the impact of quantum computers on a blockchain is previously discussed (e.g., Fernández-Caramès & Fraga-Lamas, 2020; Gheorghiu et al., 2017; Kiktenko et al., 2018), there is a dearth of research in the corresponding domain. In the supply chain context, such scarcity is even further escalated.

Due to the scarcity of relevant research and the importance of the subject, this study aimed to conceptually investigate the impact of quantum computers on blockchain security and to identify the consequent effect on supply chains. Hence, the following research question is developed: *How do quantum computers impact blockchain-based supply chains?*

In the following section, the methodology of this paper is elaborated. Then, blockchain and its applicability for supply chains are discussed. Thereafter, the core of blockchain security is unfolded. In section five, the impact of quantum computers on blockchain security is revealed. Respectively, sections six and seven highlight the pertinent quantum-based implications for supply chains and the research domain.

METHOD

This paper utilizes the theory synthesis type of conceptual method. In this regard, Jaakkola (2020) states that "theory synthesis paper seeks to achieve conceptual integration across multiple theories or literature streams. Such papers offer a new or enhanced view of a concept or phenomenon by linking previously unconnected or incompatible pieces in a novel way" (p. 21). There are two main components of the theory synthesis type of conceptual method: summarization and integration (Jaakkola, 2020).

Summarization refers to the encapsulation and reduction of knowledge to a manageable whole (Jaakkola, 2020; MacInnis, 2011). This is consistent with the statement by Gilson and Goldberg (2015) that a well-grounded conceptual paper is underpinned by a tight and narrow focus on conceptual

pieces. Accordingly, this paper provides a narrowed elaboration of three conceptual pieces and their relevant subsets with respect to the research focus. These three conceptual pieces are blockchain, supply chain, and quantum computers.

The integration establishes the link among conceptual pieces by which new insights occur (Jaakkola, 2020; MacInnis, 2011). Correspondingly, the three main conceptual pieces of this study are connected and help unfold the impact of quantum computers on blockchain-based supply chains. As past literature largely did not address these three concepts together, such integration offers a novel understanding that can be important for the future of supply chain users of blockchain.

Furthermore, the adequateness of the conceptual method can be supported by the data collection difficulties that naturally associate with such a research focus. In this regard, Yadav (2010) states that a significant advantage of a conceptual study refers to its unrestrained nature in relation to data availability (i.e., this approach suits well with the phenomena within which the data access is not easy). Quantum computers are just emerging and still have a long way toward maturity and vast practical applications. Hence, gaining access to germane empirical evidence can have struggles that can hinder the targeted contributions of this paper. As a result, the conceptual method is a good solution to tackle the issue of limited empirical data availability.

WHAT IS BLOCKCHAIN?

The beginning of blockchain goes back to 2008 when Satoshi Nakamoto used it as the key element to support the transactions of digital currency called Bitcoin (Nowiński & Kozma, 2017; Zhao et al., 2016). Since then, the application of blockchain has far exceeded the digital currencies (Zhao et al., 2016), continuing to grow into various areas such as healthcare (Fernández-Caramés et al., 2019; Jayaraman et al., 2019), supply chain management (Rana et al., 2021; Rejeb et al., 2019), and e-voting (Baudier et al., 2021; Schwab & Davis, 2018).

While there is no universally agreed-upon definition of blockchain, the conducted attempts share similar elements (Van Hoek et al., 2019). Blockchain is mainly referred to as a technology platform that enables a reliable and secure database of digital content (e.g., information, record, and transaction) among multiple participants (Manners-Bell & Lyon, 2019; Van Hoek et al., 2019; Zhao et al., 2016). Blockchain falls into the category of distributed ledger technologies which implies that this technology platform stores and exchanges digital content without needing control from a centralized party (Manners-Bell & Lyon, 2019; Schwab & Davis, 2018; Van Hoek et al., 2019).

To put it simply, blockchain is a chain of blocks that incorporate contents that are stored on them (Dolgui et al., 2020; Mondal et al., 2019; Xu et al., 2021). Each block contains a timestamp, information on the current block's contents, the current block's hash value, and the hash value of the previous block (Bakar & Rosbi, 2018; Ying et al., 2018). A blockchain is copied on multiple nodes, which are normally in the form of computers across the blockchain networks and are also responsible for validating the blocks (Van Hoek et al., 2019; Ying et al., 2018).

There are varied validation mechanisms, degrees of control, and ownership in blockchains. These variances enable distinguishing blockchains into two different types (Van Hoek et al., 2019). One type is "public" blockchain (e.g., Bitcoin and Ethereum), where the platform is completely decentralized, accessible to the public without an owner, and the validation process requires nodes to solve a complex mathematical process that can be run by anyone incentivized via payments through cryptocurrencies (Van Hoek et al., 2019; Viriyasitavat & Hoonsopon, 2019).

The second type is "permissioned" blockchain, in which control and ownership are shared among the authorized involved users (that know each other but do not necessarily trust each other), and it is common among supply networks (Van Hoek et al., 2019). In this type of blockchain, content availability is based on the users' agreements (Van Hoek et al., 2019; Viriyasitavat & Hoonsopon, 2019).

Blockchain in Supply Chains

Businesses express varied maturity levels regarding the benefits that they experience from blockchains (Van Hoek et al., 2019). Nevertheless, despite the existing limitations, there are numerous benefits associated with the implementation of blockchain into supply chains (Manners-Bell & Lyon, 2019; Van Hoek et al., 2019). In general, content immutability, authentication, transparency, traceability, smart contracting, decentralization, and efficiency are the common benefits identified in various literature (Alazab et al., 2021; Francisco & Swanson, 2018; Manners-Bell & Lyon, 2019).

Blockchain platforms provide an immutable and authenticable block of content among participants that enable transparency and traceability of processes among supply chain users and can be utilized for various purposes such as counterfeiting prevention, insight creation on various topics (e.g., customer demands), data exchange, and inspections (Agrawal et al., 2021; Francisco & Swanson, 2018; Mandolla et al., 2019; Van Hoek et al., 2019).

Content validation and ownership are distributed across the network to prevent centralized control and enhance decentralization (Saberi et al., 2019; Van Hoek et al., 2019). Moreover, blockchain eliminates the cost burden of backup servers from a single party and reduces the dependency on a middleman, resulting in higher efficiency (Choi et al., 2019; Kshetri, 2018; Sharma et al., 2018). Blockchain also enables the smart contracts through which contractual agreements are digitalized via codes that enable synchronized and automated executions once the pre-defined conditions are met (Chang, Chen, and Lu, 2019; Dolgui et al., 2020).

Furthermore, transaction cost theory can also be utilized to develop insights into the impact of blockchain on transaction costs associated with supply chain relations (Ahluwalia et al., 2020; Schmidt & Wagner, 2019). According to this theory, there are two key factors that influence transaction cost: bounded rationality and opportunism (Grover & Malhotra, 2003; Rindfleisch & Heide, 1997). Rindfleisch and Heide (1997) refer to bounded rationality as the ability limitation of decision-makers for processing information with careful consideration of all binding aspects and conditions of the contract. In this regard, they emphasize the word "limitation" and argue that it should not be confused with potential "stupidity" that can occur on the part of an actor or individual (Rindfleisch & Heide, 1997). An important factor that impacts bounded rationality is the degree of uncertainty; under an uncertain environment, bounded rationality is a more significant issue as greater dedication is needed because there are more aspects to consider (Grover & Malhotra, 2003). Opportunism addresses the dishonest behaviors in the exchange relationship that are based on self-interest, such as cheating, lying, and intentional deviation from the agreements (Grover & Malhotra, 2003; Williamson, 1975). The opportunistic behaviors engender the need for behavior monitoring and control, which increases the transaction cost (Grover & Malhotra, 2003).

In this context, blockchain can impact the transaction cost associated with supply chain relationships. For instance, a smart contract's clear, pre-defined procedure and immutable as well as authenticable contents limit the opportunistic behaviors; a transparent and reliable blockchain platform decreases the environmental uncertainty; and the automated execution of smart contracts reduces human involvement, which affects bounded rationality (Chang, Chen, and Wu, 2019; Schmidt & Wagner, 2019; Treiblmaier, 2018).

Blockchain can decrease trust issues in supply chains. The principle-agent theory addresses the relationship between two actors who are participating in an exchange of resources and capabilities, usually via contracts (Braun & Guston, 2003; Steinle et al., 2014). In a supply chain context, the buyer-suppler relationship is a good example of the relationship between the principal and agent. Under the contract, the supplier (agent) is obliged to perform certain tasks, which equips that supplier with comparatively more knowledge about the details of (and surrounding) the task compared to the buyer (Steinle et al., 2014; Treiblmaier, 2018). Due to this information asymmetry, the buyer (principal) needs to establish cost-incurring trust and control mechanisms to prevent supplier's divergence (Jensen & Meckling, 1976; Steinle et al., 2014; Treiblmaier, 2018). In this regard, blockchain transparency and reliable content accessibility reduce the information asymmetry in the business relationship between

the principal and agent; hence, the trust and control mechanisms become less costly (Chang, Chen, and Wu, 2019; Treiblmaier, 2018).

One of the important characteristics of blockchain is security which plays a significant role in the realization of benefits (Chalmers et al., 2019; Fernández-Caramès & Fraga-Lamas, 2020; Kumar et al., 2020; Saberi et al., 2019). Lack of security eventually challenges the core of blockchain promises. For example, without blockchain security tools, it may become possible to manipulate blockchain contents, forge users' identities, disrupt the trust mechanism, and distort smart contracts.

BLOCKCHAIN SECURITY

Blockchain security mainly depends on two main cryptographic concepts: public-key/asymmetric cryptography and hash function (Fernández-Caramès & Fraga-Lamas, 2020; Mandolla et al., 2019; Rejeb et al., 2019).

Asymmetric Cryptography

Asymmetric cryptography uses public and private keys to authenticate content exchanges between the involved users, utilizing what is known as "digital signature" (Fernández-Caramès & Fraga-Lamas, 2020; Niranjanamurthy et al., 2019). As the names imply, a private key is always kept private, and public keys are available for others (Zhang et al., 2018).

In blockchains, typical digital signatures involve hashing the content (via hash function) by the user, which results in fixed-size hash output (Zheng et al., 2018). The hash output is encrypted by a private key which creates the digital signature, and then the signature is verified by others using the same user's public key (Fernández-Caramès & Fraga-Lamas, 2020; Zheng et al., 2018). Due to secure mathematical relation between pair of public and private keys, when one verifies the signature by a public key, it guarantees that only the user who has the private key has created the signature (Fernández-Caramès & Fraga-Lamas, 2020). Hence, the authentication is established.

Asymmetric cryptography is also necessary for the blockchain wallet. The wallet contains a public key that provides the public address of the wallet through the hash function (the public address is used to send/receive the digital content), and a private key which is used for wallet accessibility, management, and signature (Dikshit & Singh, 2017; Dwyer, 2015; Fernández-Caramès & Fraga-Lamas, 2020).

Hash Function

In simple terms, the hash function transforms and maps the content of arbitrary sizes into a fixed-size hash output/value that is unique (almost always) to the original content input (Di Pierro, 2017; Eltayieb et al., 2020). In other words, a fixed-size hash value is collusion-free, which means that no two content inputs should have the same hash output. The smallest change in content input, such as adding a single character, will lead to a completely different hash output (Wong et al., 2019). The hash function is also preimage resistant and deterministic (Lee & Lee, 2017). The former refers to the feature through which the hash function becomes difficult to invert, and the latter ensures that identical content input always results in the same hash output. The hash function, with regard to the aforementioned characteristics, plays an important role in blockchain security.

The hash function makes the blockchain immutable and tamper-proof. Every block contains its own hash and the hash of the previous block, which makes the blocks connected to each other (Bakar & Rosbi, 2018; Fernández-Caramès & Fraga-Lamas, 2020; Ying et al., 2018). If the block's content is later altered, the hash of it will also change which then no longer match the same block's hash in the subsequent block, making it invalid (Rejeb et al., 2019; Wong et al., 2019).

The hash function is also used for address generation, reducing the public address size, and content hashing during the signature process (Fernández-Caramès & Fraga-Lamas, 2020; Raikwar et al., 2019; Wang et al., 2019).

Security Algorithms and One-Way Function

These two main cryptographic concepts are underpinned by "one-way function", which refers to the function through which mathematical computations are easy in one direction but perceived to be computationally infeasible in the inverse direction (De Leon et al., 2017).

In asymmetric cryptography, public and private keys behave as one-way functions, which means that from a private key, it is easy to get to the public key, but the opposite direction is computationally hard and infeasible (Kenekayoro Patrick, 2011). In blockchains, the two most common algorithms for public-key cryptography are Elliptic Curve Cryptography (ECC) and Rivest–Shamir–Adleman (RSA), which are used for security and key pairs generation, based on mathematical problems that produce one-way function (Chandel et al., 2019; Dasgupta et al., 2019; Grecuccio et al., 2020).

The security level of both ECC and RSA are based on the "security bits" (Chandel et al., 2019; Fernández-Caramès & Fraga-Lamas, 2020; Lenstra, 2002). Due to the different natures of RSA and ECC, the required number of bits to offer the same security strength are different between them (Chandel et al., 2019). For example, a 256-bit ECC key is equivalent to a 3072-bit RSA key. Each one requires a higher number of bits in its own class to offer stronger security (e.g., 256-bit ECC provides stronger security than 224-bit ECC). Barker and Dang (2016, Table 2) provide a detailed comparison of each algorithm's strengths.

The most commonly adopted hash function in a blockchain is the Secure Hash Algorithm (SHA), which is used to produce the fixed-size hash output from the content input (Dasgupta et al., 2019; Di Pierro, 2017). SHA is a family of cryptographic hash functions that were originally developed by the National Security Agency (NSA) and the Federal Information Processing Standard in the United States (Ajao et al., 2019). The early version of SHA (i.e., SHA-1) eventually cracked; therefore, it can no longer offer the required security (Dasgupta et al., 2019; Xue et al., 2019). Instead, the second (SHA-2) and third (SHA-3) versions have been introduced to fulfill the security gaps, and as of writing, the second version, SHA-256, is a commonly used algorithm in blockchain hashing and generates the fixed 256-bit hash (Dasgupta et al., 2019; Fernández-Caramès & Fraga-Lamas, 2020; Sheetal & Venkatesh, 2018). Hash and its algorithm also behave as a one-way function (Sheetal & Venkatesh, 2018; Verma & Garg, 2017).

WHAT THREATENS BLOCKCHAIN SECURITY, AND HOW CAN IT BE RESOLVED?

In the early 80s, Richard Feynman underpinned what is known as quantum computing (Djemame & Batouche, 2016; Feynman, 1982; Nguyen & Kim, 2019). Modern (i.e., classical) computing operates on the basis of one of two positions, 0 and 1, which forms the so-called "bits" of information, whereas quantum computing utilizes "qubits," which includes 0 and 1 as well as all the states in between (Mosteanu & Faccia, 2021; Nguyen & Kim, 2019; Vedral & Plenio, 1998).

Blockchain's asymmetric cryptography uses algorithms that are based on mathematical problems that produce one-way functions and make the inverse calculations very long for classical computers (Gheorghiu et al., 2017; Kiktenko et al., 2018). However, by using Shor's algorithm, powerful quantum computers can perform these inverse calculations and solve the mathematical problems astronomically faster (Fernández-Caramès & Fraga-Lamas, 2020; Gheorghiu et al., 2017; Kiktenko et al., 2018; Raz, 1999). The difference in calculations can go from decades or centuries (or even millennium) by classical computers to seconds, minutes, or hours using quantum computers. This means that it will no longer be infeasible to break the core of contemporary blockchains' asymmetric cryptography. For instance, through classical computers, it would require a billion dollars in 30 to 40 years to break into cryptosystems with 112 security bits (Chen et al., 2016), whereas 160-bit ECC can be broken with 1000-qubits and 1024-bit RSA with about 2000-qubits quantum computer (Proos & Zalka, 2003).

For what concerns the hash function, quantum computers, using Grover's algorithms, can only speed up the brute force attack by a quadratic factor (Fernández-Caramès & Fraga-Lamas, 2020; Gheorghiu et al., 2017). Hence, it is usually suggested to increase the hash output size (Chen et al., 2016; Fernández-Caramès & Fraga-Lamas, 2020). Nevertheless, Grover's algorithm can be utilized for fast mining in public blockchains like Bitcoin, which enables quick recreation of the entire blockchain and can violate its integrity (Fernández-Caramès & Fraga-Lamas, 2020; Gheorghiu et al., 2017).

While these threats are of particular significance, other relevant quantum security dangers may also exist that are potentially not yet fully discovered (Gheorghiu et al., 2017). Fortunately, powerful quantum computers are still being developed, and currently, the strongest available has 64 qubits, claimed by Honeywell (Shankland, 2020). There are varied estimations on when quantum computers will be strong enough to threaten contemporary blockchain security (Stevens, 2020). While some estimate that the emergence of sufficiently powerful quantum computers may occur within a couple of years, others predict their arrival to happen further in the future, such as in the year 2026 or 2031 (Chen et al., 2016; Gheorghiu et al., 2017; Mosca, 2018; Stevens, 2020).

There are two potential solutions for creating quantum resistance: one refers to "post-quantum cryptography" that utilizes mathematical problems, other than conventional ones, that are perceived to be secure against quantum attacks; another one is "quantum cryptography," which utilizes properties of quantum mechanics to provide security (Kiktenko et al., 2018; Mosca, 2018). However, post-quantum cryptography can be associated with technical complications and inefficiencies (Campbell, 2019; Gheorghiu et al., 2017; Kiktenko et al., 2018). Also, quantum cryptography requires quantum computation and communication tools that will not be conveniently accessible for practical use in the near future (Gheorghiu et al., 2017).

Moreover, the development of quantum-resistant cryptography and relevant transformation requires a significant amount of time and effort (Campbell, 2019; Chen et al., 2016) that may imply a lack of preparedness when sufficiently powerful quantum computers are available. In this regard, Chen et al. (2016) call for immediate action on the matter. They state that:

It has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing. (p. 2)

IMPLICATIONS FOR SUPPLY CHAIN

The threat of quantum computers to conventional blockchains implies that information (digital content) security will not be guaranteed anymore within the supply chain context. It will be able to endanger any blockchain functionality that roots into private keys. Private keys that were supposed to be kept secret, will then be conveniently attainable through corresponding public keys as mathematical problems become efficiently reversible (Gheorghiu et al., 2017; Kiktenko et al., 2018). Hence, an attacker can replace a supply chain user, take actions they desire (e.g., gain access to sensitive information or insert false data into the blockchain), and sign content without anyone being able to detect it (Gheorghiu et al., 2017). Since actors' identities will no longer be securely verifiable, false blocks and malicious directives can be created, which can impact smart contracts and can undermine supply chain traceability and transparency. In addition, the integrity of public blockchains like Bitcoin can become vulnerable to fast mining through quantum-based attacks (Fernández-Caramès & Fraga-Lamas, 2020; Gheorghiu et al., 2017), which can threaten the pertinent cryptocurrency users within the supply chain landscape.

From the perspective of principle-agent and transaction cost theories, the trustworthy supply chain environment that is enabled by blockchain will become disrupted, rooms will be open for opportunistic behaviors, and uncertainty will increase. Involved actors will then have new security concerns, and bounded rationality will be impacted. Furthermore, the need for intermediaries will be evident again as blockchain security primitives are compromised, and new costs will be added.

Overall, the threat of quantum computers makes the future application of blockchains uncertain for supply chains. This uncertainty can seriously challenge the utopia of supply chains where processes heavily rely on blockchains, engendering second thoughts on whether to strive toward investment in blockchains or not.

The dichotomy between quantum threats and quantum-resistant cryptography prevents accurate predictions about the future role of quantum computers in blockchains. While certain estimations imply that the quantum threat is real and can be closer than the solution, there are also more optimistic perspectives (Campbell, 2019; Chen et al., 2016; Gheorghiu et al., 2017; Mosca, 2018; Stevens, 2020). Nevertheless, building pertinent business strategies for blockchains may require stronger certainty, as stakes are quite high.

Notwithstanding the uncertainty, a significant dedication and multi-lateral cooperation are needed among various actors such as states, software and standard developers, academia, blockchain specialists, cryptography experts, and businesses to accelerate the development and wide implementation of a well-grounded quantum solution (Campbell, 2019; Gheorghiu et al., 2017; Mosca, 2018).

THEORETICAL IMPLICATIONS

This study targets to provide one of the first steps regarding the upcoming impact of quantum computers on blockchain-based supply chains. To the best of the author's knowledge, quantum impact on blockchains has not been previously discussed in the supply chain context, whereas the large worldwide investment in this technology can be under serious threat in soon future.

Due to the subject's novelty and lack of sufficient scholarly attention, it is evident that future researchers can redirect their efforts toward this topic. Future research avenues can conduct empirical investigations into the awareness of businesses about the quantum impact and the possible contributions that they can offer to thwart the threat. Studies can also focus on the preparedness of businesses, at individual and supply chain levels, for smooth adoption of quantum-resistant cryptography, as emphasized by Mosca (2018).

Furthermore, as the impact of quantum computers on blockchain-based supply chains goes beyond the boundary of supply chain management, future research may need to incorporate knowledge from various disciplines to create comprehensive insights that contribute to the subject domain.

REFERENCES

Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & Industrial Engineering*, *154*, 107130. doi:10.1016/j.cie.2021.107130

Ahluwalia, S., Mahto, R. V., & Guerrero, M. (2020). Blockchain technology and startup financing: A transaction cost economics perspective. *Technological Forecasting and Social Change*, *151*, 119854. doi:10.1016/j.techfore.2019.119854

Ajao, L. A., Agajo, J., Adedokun, E. A., & Karngong, L. (2019). Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry. *J—Multidisciplinary Scientific Journal, 2*(3), 300-325.

Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2021). Blockchain technology in supply chain management: An empirical study of the factors affecting user adoption/acceptance. *Cluster Computing*, *24*(1), 83–101. doi:10.1007/s10586-020-03200-4

Anderberg, A., Andonova, E., Bellia, M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F., Spirito, L. (2019). *Blockchain now and tomorrow: Assessing multidimensional impacts of distributed ledger technologies* (EUR 29813 EN). Publications Office of the European Union. 10.2760/901029

Bakar, N. A., & Rosbi, S. (2018). Robust framework diagnostics of blockchain for bitcoin transaction system: A technical analysis from Islamic financial technology (i-FinTech) perspective. *International Journal of Business and Management*, *2*(3), 22–29. doi:10.26666/rmp.ijbm.2018.2.4

Barker, E., & Dang, Q. (2016). *Nist special publication 800-57 part 1, revision 4.* NIST, Tech. Rep, 16.

Baudier, P., Kondrateva, G., Ammi, C., & Seulliet, E. (2021). Peace engineering: The contribution of blockchain systems to the e-voting process. *Technological Forecasting and Social Change*, *162*, 120397. doi:10.1016/j.techfore.2020.120397 PMID:33071364

Braun, D., & Guston, D. H. (2003). Principal-agent theory and research policy: An introduction. *Science & Public Policy*, *30*(5), 302–308. doi:10.3152/147154303781780290

Campbell, R. Sr. (2019). Evaluation of post-quantum distributed ledger cryptography. *The Journal of The British Blockchain Association*, *2*(1), 7679. doi:10.31585/jbba-2-1-(4)2019

Chalmers, D., Matthews, R., & Hyslop, A. (2019). Blockchain as an external enabler of new venture ideas: Digital entrepreneurs and the disintermediation of the global music industry. *Journal of Business Research*, *125*, 577–591. doi:10.1016/j.jbusres.2019.09.002

Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., & Ni, T. Y. (2019). A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. In *Future of Information and Communication Conference* (pp. 988-1003). Springer.

Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, *144*, 1–11. doi:10.1016/j.techfore.2019.03.015

Chang, S. E., Chen, Y. C., & Wu, T. C. (2019). Exploring blockchain technology in international trade. *Industrial Management & Data Systems*, *119*(8), 1712–1733.

Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). US Department of Commerce, National Institute of Standards and Technology. doi:10.6028/NIST.IR.8105

Choi, T. M., Wen, X., Sun, X., & Chung, S. H. (2019). The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. *Transportation Research Part E, Logistics and Transportation Review*, *127*, 178–191. doi:10.1016/j.tre.2019.05.007

Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. *Journal of Banking and Financial Technology*, *3*(1), 1–17. doi:10.1007/s42786-018-00002-6

Davies, S., & Likens, S. (2018). *Blockchain is here. What's your next move?* PWC. https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

De Leon, D. C., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: Properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, *19*(5), 92–95. doi:10.1109/MCSE.2017.3421554

Dikshit, P., & Singh, K. (2017). Efficient weighted threshold ECDSA for securing bitcoin wallet. In 2017 ISEA Asia Security and Privacy (ISEASP) (pp. 1-9). IEEE. doi:10.1109/ISEASP.2017.7976994

DiVincenzo, D. P. (2000). The physical implementation of quantum computation. *Fortschritte der Physik: Progress of Physics*, *48*(9-11), 771–783. doi:10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E

Djemame, S., & Batouche, M. C. (2016). Quantum Genetic Computing and Cellular Automata for Solving Edge Detection. *The First International Conference on Computer Science's Complex Systems and their Applications (ICCSA)*.

Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., & Werner, F. (2020). Blockchain-oriented dynamic modeling of smart contract design and execution in the supply chain. *International Journal of Production Research*, *58*(7), 2184–2199. doi:10.1080/00207543.2019.1627439

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, *17*, 81–91. doi:10.1016/j.jfs.2014.11.006

Eltayieb, N., Elhabob, R., Hassan, A., & Li, F. (2020). A blockchain-based attribute-based encryption scheme to secure data sharing in the cloud. *Journal of Systems Architecture*, *102*, 101653. doi:10.1016/j.sysarc.2019.101653

Fernández-Caramès, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 21091–21116. doi:10.1109/ACCESS.2020.2968985

Fernández-Caramés, T. M., Froiz-Míguez, I., Blanco-Novoa, O., & Fraga-Lamas, P. (2019). Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. *Sensors (Basel)*, *19*(15), 3319. doi:10.3390/s19153319 PMID:31357725

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, *21*(6/7).

Firdaus, A., Ab Razak, M. F., Feizollah, A., Hashem, I. A. T., Hazim, M., & Anuar, N. B. (2019). The rise of "blockchain": Bibliometric analysis of blockchain study. *Scientometrics*, *120*(3), 1289–1331. doi:10.1007/s11192-019-03170-4

Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, *2*(1), 2. doi:10.3390/logistics2010002

Gheorghiu, V., Gorbunov, S., Mosca, M., & Munson, B. (2017). *Quantum-proofing the blockchain*. Blockchain Research Institute: University of Waterloo.

Ghobakhloo, M. (2018). The future of manufacturing industry: A strategic roadmap toward industry 4.0. *Journal of Manufacturing Technology Management*, *29*(6), 910–936. doi:10.1108/JMTM-02-2018-0057

Grecuccio, J., Giusto, E., Fiori, F., & Rebaudengo, M. (2020). Combining blockchain and IoT: Food-chain traceability and beyond. *Energies*, *13*(15), 3820. doi:10.3390/en13153820

Grover, V., & Malhotra, M. K. (2003). Transaction cost framework in operations and supply chain management research: Theory and measurement. *Journal of Operations Management*, *21*(4), 457–473. doi:10.1016/S0272-6963(03)00040-8

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? In *Digitalization in supply chain management and logistics: Smart and digital solutions for an industry 4.0 environment. Proceedings of the Hamburg International Conference of Logistics (HICL)*, Vol. 23 (pp. 3-18). Berlin: Epubli GmbH.

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 1-9.

Jayaraman, R., Salah, K., & King, N. (2019). Improving opportunities in healthcare supply chain processes via the internet of things and blockchain technology. *International Journal of Healthcare Information Systems and Informatics*, *14*(2), 49–65. doi:10.4018/IJHISI.2019040104

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360. doi:10.1016/0304-405X(76)90026-X

Kenekayoro Patrick, T. (2011). One way functions and public key cryptography. *African Journal of Mathematics and Computer Science Research*, *4*(6), 213–216.

Khatri, Y. (2019, April 5). *Russian gas giant Gazprom to execute business contracts on a blockchain*. CoinDesk. https://www.coindesk.com/russian-gas-giant-gazprom-to-execute-business-contracts-on-a-blockchain

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, *3*(3), 035004. doi:10.1088/2058-9565/aabc6b

Kouhizadeh, M., Zhu, Q., & Sarkis, J. (2020). Blockchain and the circular economy: Potential tensions and critical reflections from practice. *Production Planning and Control*, *31*(11-12), 950–966. doi:10.1080/09537287.2019.1695925

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. doi:10.1016/j.ijinfomgt.2017.12.005

Kumar, V., Ramachandran, D., & Kumar, B. (2020). Influence of new-age technologies on marketing: A research agenda. *Journal of Business Research*, *125*, 864–877. doi:10.1016/j.jbusres.2020.01.007

Lee, B., & Lee, J. H. (2017). Blockchain-based secure firmware update for embedded devices in an internet of things environment. *The Journal of Supercomputing*, *73*(3), 1152–1167. doi:10.1007/s11227-016-1870-0

Lenstra, A. K. (2002). Citibank, NA and technische universiteit eindhoven. *Coding Theory And Cryptology*, *1*, 175. doi:10.1142/9789812388841_0005

Liu, S. (2020, May 13). *Blockchain - Statistics & Facts*. Statista. https://www.statista.com/topics/5122/blockchain/?fbclid=IwAR322FUbOmERyAD0U0bvWB-8dAA6THhZ2X2mb6NkwwQ6pLIVe910oirM2js

MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. *Journal of Marketing*, *75*(4), 136–154. doi:10.1509/jmkg.75.4.136

Mandolla, C., Petruzzelli, A. M., Percoco, G., & Urbinati, A. (2019). Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry. *Computers in Industry*, *109*, 134–152. doi:10.1016/j.compind.2019.04.011

Manners-Bell, J., & Lyon, K. (2019). *The logistics and supply chain innovation handbook: Disruptive technologies and new business models*. Kogan Page Publishers.

Mondal, S., Wijewardena, K. P., Karuppuswami, S., Kriti, N., Kumar, D., & Chahal, P. (2019). Blockchain inspired RFID-based information architecture for food supply chain. *IEEE Internet of Things Journal*, *6*(3), 5803–5813. doi:10.1109/JIOT.2019.2907658

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security and Privacy*, *16*(5), 38–41. doi:10.1109/MSP.2018.3761723

Mosteanu, N. R., & Faccia, A. (2021). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. *Journal of Open Innovation*, *7*(1), 19. doi:10.3390/joitmc7010019

Nguyen, D. M., & Kim, S. (2019). Multi-bits transfer based on the quantum three-stage protocol with quantum error correction codes. *International Journal of Theoretical Physics*, *58*(6), 2043–2053. doi:10.1007/s10773-019-04098-4

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Computing*, *22*(6), 14743–14757. doi:10.1007/s10586-018-2387-5

Nowiński, W., & Kozma, M. (2017). How can blockchain technology disrupt the existing business models? *Entrepreneurial Business and Economics Review*, *5*(3), 173–188. doi:10.15678/EBER.2017.050309

O'Dea, S. (2020, May 25). *Europe: Anticipated impacts of blockchain 2018*. Statista. https://www.statista.com/statistics/942216/europe-expected-impact-of-blockchain/#statisticContainer

Proos, J., & Zalka, C. (2003). *Shor's discrete logarithm quantum algorithm for elliptic curves.* arXiv preprint quant-ph/0301141.

Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 148550–148575. doi:10.1109/ACCESS.2019.2946983

Rana, R. L., Tricase, C., & De Cesare, L. (2021). Blockchain technology for a sustainable agri-food supply chain. *British Food Journal*. Advance online publication. doi:10.1108/BFJ-09-2020-0832

Raz, R. (1999). Exponential separation of quantum and classical communication complexity. In *Proceedings of the thirty-first annual ACM symposium on Theory of Computing* (pp. 358-367). doi:10.1145/301250.301343

Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, *11*(7), 161. doi:10.3390/fi11070161

Rindfleisch, A., & Heide, J. B. (1997). Transaction cost analysis: Past, present, and future applications. *Journal of Marketing*, *61*(4), 30–54. doi:10.1177/002224299706100403

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. doi:10.1080/00207543.2018.1533261

Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management*, *25*(4), 100552. doi:10.1016/j.pursup.2019.100552

Schwab, K., & Davis, N. (2018). *Shaping the future of the fourth industrial revolution*. Currency.

Shankland, S. (2020, June 18). *Honeywell says it's got the fastest quantum computer on the planet For now*. CNET. https://www.cnet.com/news/honeywell-says-its-got-the-fastest-quantum-computer-on-the-planet/

Sharma, P. K., Kumar, N., & Park, J. H. (2018). Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Transactions on Industrial Informatics*.

Sheetal, M., & Venkatesh, K. A. (2018). Necessary requirements for blockchain technology and its applications. *International Journal of Computer Science and Information Technologies*.

Steinle, C., Schiele, H., & Ernst, T. (2014). Information asymmetries as antecedents of opportunism in buyer-supplier relationships: Testing principal-agent theory. *Journal of Business-To-Business Marketing*, *21*(2), 123–140. doi:10.1080/1051712X.2014.903457

Stevens, R. (2020, May 12). *Quantum computers could crack Bitcoin by 2022: Quantum computers could one day be used to crack the encryption of cryptocurrencies like Bitcoin. And that day could come sooner than anticipated*. Decrypt. https://decrypt.co/28560/quantum-computers-could-crack-bitcoins-encryption-by-2022

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management*, *23*(6), 545–559. doi:10.1108/SCM-01-2018-0029

Van Hoek, R., Fugate, B., Davletshin, M., & Waller, M. A. (2019). *Integrating blockchain into supply chain management: A toolkit for practical implementation*. Kogan Page.

Vedral, V., & Plenio, M. B. (1998). Basics of quantum computation. *Progress in Quantum Electronics*, *22*(1), 1–39. doi:10.1016/S0079-6727(98)00004-4

Verma, A. K., & Garg, A. (2017). Blockchain: An analysis on next-generation internet. *International Journal of Advanced Research in Computer Science*, *8*(8), 429–432. doi:10.26483/ijarcs.v8i8.4769

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32–39. doi:10.1016/j.jii.2018.07.004

Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, *127*, 43–58. doi:10.1016/j.jnca.2018.11.003

Williamson, O. E. (1975). Markets and hierarchies. Academic Press.

Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature Communications*, *10*(1), 1–8. doi:10.1038/s41467-019-08874-y PMID:30796226

Xu, P., Lee, J., Barth, J. R., & Richey, R. G. (2021). Blockchain as supply chain technology: Considering transparency and security. *International Journal of Physical Distribution & Logistics Management*, *51*(3), 305–324. doi:10.1108/IJPDLM-08-2019-0234

Xue, X., Wang, C., Liu, W., Lv, H., Wang, M., & Zeng, X. (2019). A RISC-V processor with area-efficient memristor-based in-memory computing for hash algorithm in blockchain applications. *Micromachines*, *10*(8), 541. doi:10.3390/mi10080541 PMID:31426443

Yadav, M. S. (2010). The decline of conceptual articles and implications for knowledge development. *Journal of Marketing*, *74*(1), 1–19. doi:10.1509/jmkg.74.1.1

Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. *International Journal of Information Management*, *39*, 1–4. doi:10.1016/j.ijinfomgt.2017.10.004

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, *16*, 267–278. doi:10.1016/j.csbj.2018.07.004 PMID:30108685

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, *2*(1), 1–7. doi:10.1186/s40854-016-0049-2

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. doi:10.1504/IJWGS.2018.095647

Fakhreddin Rad is a PhD candidate in the School of Social Sciences, subject of Business Studies, at Södertörn University. Rad's research interests include industry 4.0 and its underlying technologies within the supply chain context. Rad holds a Master of Science with specialisation in Business Process and Supply Chain Management.