Quantum Pliers Cutting the Blockchain

Quantum pliers cutting the Blockchain

Edoardo Giusto, *Student Member, IEEE,* Mohammad Ghazi Vakili, *Student Member, IEEE,* Filippo Gandino, *Member, IEEE,* Claudio Demartini, *Senior Member, IEEE,* and Bartolomeo Montrucchio, *Member, IEEE*

Abstract—Recent years have seen the continuous evolution of technology, which led to the definition of frameworks such as the Internet of Things (IoT) and Industry 4.0. These paradigms are producing enormous quantities of data every single day. These data are subject to data analysis, shared publicly or kept secret. Traditionally, this task was carried out using databases. With the advent of Blockchain and other Distributed Ledger Technologies (DLT), instead, these data have a new way of being stored and shared (or kept private). The last actor role in this play is acted by Quantum Computers, since sufficiently large Quantum Computers are expected to seriously threaten the security and integrity of DLTs thanks to their totally different way of representing information. This paper aims to investigate the real threats for blockchain due to Quantum Computing and review post-quantum DLT solutions for traceability applications.

Index Terms—Traceability, IoT, Industry 4.0, Blockchain, Quantum Computing.

1 Introduction

Global scale of industrial production has reached dimensions for which it is difficult for a human being to keep the pace at which the data have to be recorded [1]. This process has necessarily been automatised with the help of a plethora of different technologies. This task automatization is crucial when it comes to traceability applications, which find natural employment in the automotive domain, both from a supply chain perspective and from a vehicle management perspective. There is also the need for storing these traceability data in a decentralized way [2], either to avoid a single point of failure or to ensure the data cannot be altered by some malicious entity. Blockchain and other Distributed Ledger Technologies (DLTs) are then the way to go if such needs are in place [3].

A blockchain is a distributed ledger of timestamped records (transactions), built in such a way that it is tamper proof.

The integrity of blockchains relies basically on two points: *a)* the signature scheme encrypting it and *b)* the fact that one malicious actor is supposed not to be able to control the majority of the network's computing power.

Several DLTs also feature the possibility of implementing Smart Contracts, which are pieces of code that can automatically enforce actions depending on the status of the ledger.

All these amenities and commodities provided by DLTs could cease with the advent of large Quantum Computers - i.e. with a sufficient number of qubits to become dangerous. This kind of devices could, for instance, be used to break the RSA cryptosystem or to take over the entire ledger network using their suitability to solve mathematical problems [4].

Several companies and research centers are trying to address this issue by designing and implementing quantum-resistant DLT.

- *The authors are with Department of Control and Computer Engineering, Politecnico di Torino, Torino, Italy*
  E-mail: edoardo.giusto@polito.it

Manuscript received April 30, 2019.

The rest of the paper is organised as follows: in Section 2 the general concepts of blockchains are shown; in Section 3 some traceability examples are described; in Section 4 some information about quantum computers are provided; in Section 5 the possible attacks of quantum computers to blockchains are described; in Section 6 some possible solutions are presented; in Section 7 some implementations of these solutions are reported; in Section 8 conclusions are drawn.

2 Blockchain concepts

The first description of such a chain is related to the proposal of the Bitcoin cryptocurrency [5]. The blockchain is composed of blocks linked together using some cryptographic function. Every block contains a hash of all the previous blocks in the chain. Participants in the blockchain are nodes storing the entire ledger. These nodes, called *miners*, serve also as validators for the new blocks, carrying out the so-called *Proof-of-Work* (PoW). Bitcoin uses Hashcash [6] PoW, in order to show that a significant computing power is used to solve a difficult mathematical problem. For a block to be valid, it has to hash to a value that is less than a certain target. Bitcoin protocol adjusts the difficulty of the target in such a way that a new block is generated about every 10 minutes on average. As soon as one miner finds the solution, the solution is broadcasted to other miners for checking. A given block in the chain cannot be altered without the alteration of all the subsequent linked blocks, a task which would require the consensus of the majority of the network. It is important to understand how a transaction is performed: the system is kept secure by public-private key pair; sender and receiver have to generate a public address using their public keys; the sender signs the transaction using his private key and thus proving s/he owns the key pair.

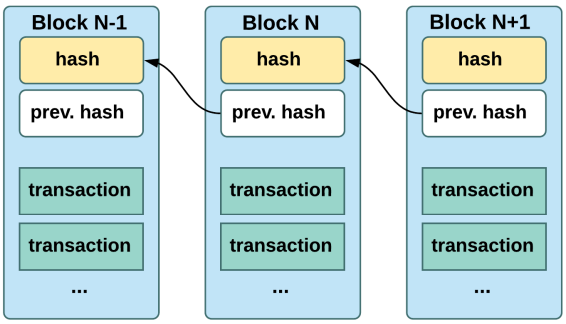

Fig. 1: Blockchain blocks linking concept.

3 Traceability Scenarios

In this section, two example applications of DLTs for traceability-related purposes are presented.

3.1 Smart contracts - Traceability

The main branch of application is related to the realization of smart contracts [8]. Smart contracts are in practice pieces of code, programs, written in some programming language. This kind of tool first appeared in the Ethereum [9] blockchain. Smart contracts are written in such a way that the set of conditions in the program matches the clauses making up the actual contract written and signed on paper.

Among the sectors in which blockchain is very useful, there is the **supply chain**. Goods can be tracked from raw material to finished product (as in Fig. 2). Furthermore, the inclusion of smart contracts makes it possible to directly and automatically pay the company which is the source of some goods, just by interrogating the incoming deliveries of boxes identified by some kind of tag. In this way, the company in charge of the delivery can be automatically paid. Moreover, there is an added advantage in the single update of a shared ledger, instead of updates to several separate databases which can get into conflict.

For all final products, the **list of components** can be kept up to date and a single component can be traced back up to the original manufacturer (i.e. parts in a car).

This data has for sure also direct implications in **insurance applications**. In fact, tags identifying goods are read throughout the entire supply chain, passing the responsibility of the transported load from entity to entity.

3.2 Digital wallet / digital twin

One of the main fields of application for the blockchain technology is the automotive sector.

The term *digital wallet* is intended as a wallet owned not by a physical person, but by a device, which could in principle be a vehicle, having the ability to automatically pay some other devices in an automatic way for some service they may provide. It is required some sort of digital information related to the car, with a *logical id* stored in the blockchain which binds to a physical vehicle in the real world.

There are **insurance** applications also in the automotive domain, as the automatic payment of the insurance fee for the car and the automatic update of ledger related to vehicle and insurance contractor in case of accident or selling. On a daily basis, a moving vehicle could **autonomously pay** for the parking spots it occupies, for the tolls encountered on the road or for the access to some restricted areas, which are ever more common in city centers due to pollution control. Moreover, such a blockchain-enabled car can autonomously pay for **refueling** (as in Fig. 3), whether the fuel is petrol or diesel or electricity. In case of need, the car could take care of paying planned or unplanned **repairs**, while keeping the ledger up to date in case of component substitution. Furthermore, it has to be noted that money flow could happen also in the other way. Cars can actually **make money** by selling services, such as deliveries, rides or ads on the bodywork.

4 Quantum Computing

Quantum Computing is going to be a breakthrough not only in the computing field per se, but also on all the other fields which intensively use computing power to carry out calculations and simulations. This is due to the radically different way in which the information is represented inside a quantum computer. The base of computation, the qubit (instead of a simple bit), presents two crucial characteristics: *superposition* and *entanglement*. In some way, superposition means that the qubit is both 0 and 1 at the same time. This results in the fact that, if you have an array of n qubits, you are actually handling 2^n states altogether, hence the so-called *quantum speedup*. Entanglement instead means that two or more qubits are linked together in a peculiar quantum-mechanical way. In fact, they have formed a bond, a special way to influence each other, even if they are placed at a great distance. Albert Einstein referred to this phenomenon as *"spooky action at a distance"*. Among the two, the superposition feature could actually undermine the immutability of the DLT systems. We will see why in the next section.

5 Possible Attack Scenarios to the Blockchain

As pointed out in [4], there are several possible attack scenarios on distributed ledgers, which can be categorized by the operating principle to which it is aimed to: attacks on *Proof-of-Work* or attacks on *Signatures*.

5.1 Attacks on Proof-of-Work

Exploiting superposition, Grover's search algorithm [10] on a quantum computer can allow performing PoW quadratically-faster with respect to a classical computer approach. Grover's algorithm, given a function and its output, can invert that function, finding the input generating that output. It is theoretically possible that a single large quantum computer, applied to the PoW task, would be able to take over the entire ledger network. It could be in fact able to validate transactions faster than the rest of the network, successfully performing *double-spending* transactions [11]. Of course, this scenario would not be possible if more than one miner had access to superior computing capabilities.

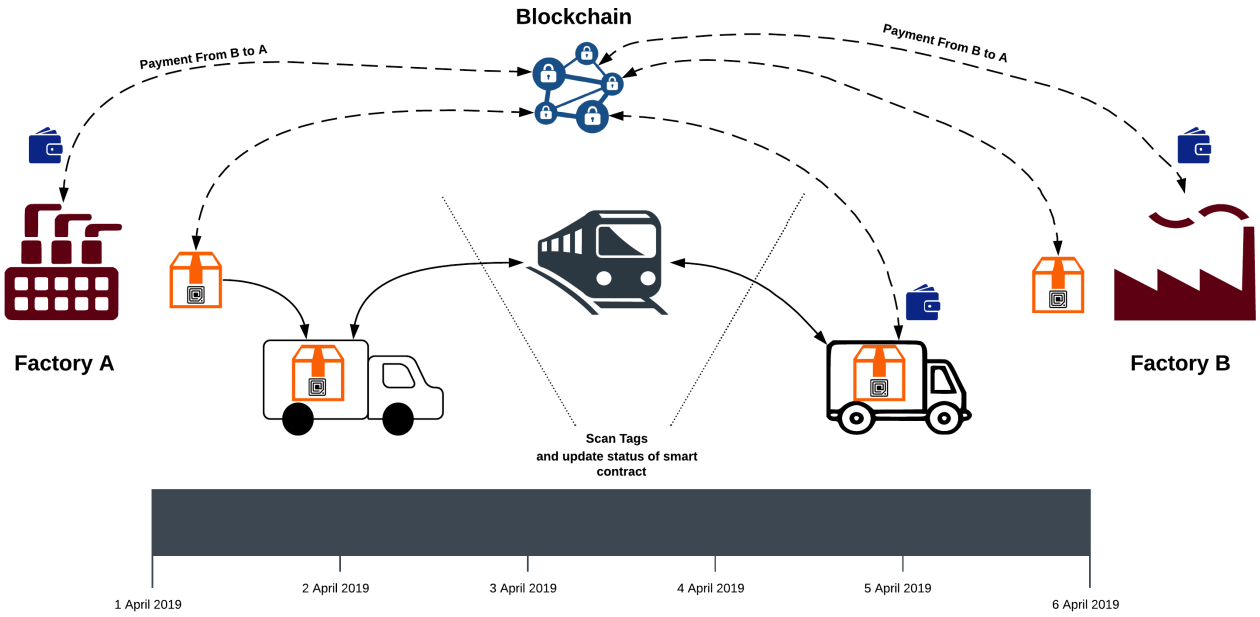

Fig. 2: Traceability example [7]

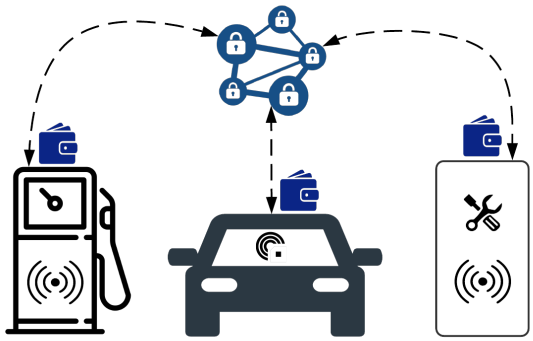

Fig. 3: Car automatic payment [7]

5.2 Attacks on Signatures

As said, public/private key cryptosystems in the majority of DLTs rely on some mathematical function, such as the *integer factorization problem*, which is very difficult for a classical computer to solve, but that would not be the case for a quantum computer, as Peter Shor demonstrated in 1994 [12]. Indeed, a quantum computer executing Shor's algorithm could compute the private key associated with a public key (i.e. the address in the Bitcoin network), opening the path for several attacks, for instance:

- **Address reuse** - In order to spend cryptocurrency, addresses have to be revealed. Once revealed, an attacker could use the public key to retrieve the private one. For the sake of security, a new pair of public and private key should be generated for every transaction, which has a small, but not negligible cost.
- **Transaction in progress** - When a transaction is issued, the public key is revealed. If a quantum attacker is able to retrieve the associated private key before the transaction is accepted and stored on the blockchain, it could effectively steal all the remaining crypto-money on the compromised account.

6 Possible Solutions to the Quantum Threat

In this section are presented some countermeasures for quantum attacks on *PoW* and on *signatures*.

Disclaimer: at the time of writing, there are yet no standards for Post-Quantum Cryptography. The National Institute of Standards and Technology (NIST) is at the second call of the standardization process [13].

6.1 Countermeasures on Proof-of-work

Alternative implementations of PoW could be proposed, as pointed out in [4], which could be:

- Flexibly difficult - adapting to the network load, as in the original Bitcoin blockchain;
- Asymmetric - difficult to solve for one node, but easy to be checked by all the other nodes;
- No quantum advantage - there should not be any quantum computing algorithm able to make this problem simple.

Another viable solution could be to shift to some other consensus algorithm, such as *Proof-of-Stake* [14].

6.2 Countermeasures on Signatures

Critical characteristics of DLT signature schemes are [4] [15] [16]:

- *Size* of signatures and public keys - since they have to be stored somewhere;
- *Time* - required to check the signatures.

Signatures should be strong as possible from the security point of view, and as small as possible to reduce the storage size and the checking time.

The best performing in this sense are *hash*-based and *lattice*-based cryptosystems, having the smallest dimension for the sum of signature and public key length [4].

7 Quantum-safe DLTs

The most relevant and most adopted DLTs which are designed to include quantum-resistant features are: *QRL*, *Corda* and *IOTA*. Again, the reader has to keep in mind that still no standard exists at the moment [13].

7.1 QRL

QRL stands for Quantum Resistant Ledger [17]. QRL secures its signatures against quantum computing power using a hash-based scheme, which is organised as an asymmetrical hypertree. It uses W-OTS+ (a variant of Winternitz One Time Signature scheme) and has the ability of quickly sign transactions. This ledger has been designed to be a public blockchain, with a cryptocurrency perspective. There should be a minimum fee for issuing a transaction, but its load should be floating and set by the market demand. This ledger is thus mining based, with a planned block time of 60 seconds, which is fair compared to the 10 minutes of the Bitcoin blockchain. The cryptocurrency proposed is the *quantum*, which has the *Shor* as fraction (10^{-9}). Transactions fee should be small and calculated in *Shor* units. QRL is for sure a very interesting open-source starting to create a large fanbase. It has to be noted though that at the moment, this project does not include Smart Contracts capability, which is crucial for the the traceability of tomorrow.

7.2 Corda

Corda is an open-source, distribute ledger platform developed by R3 company [18]. It secures the signatures using a tree-like hash-based scheme, as we have seen with QRL, but using W-OTS-T (another variant of the W-OTS scheme). It has been specially designed with financial applications in mind, but it can also be used in a variety of other fields, such as insurance, government and supply chain. It is a permissioned blockchain, meaning that only entitled actors can participate in the network, for added security. This case is particularly useful within or in between companies who signed some deal. Speaking of which, Corda has a crucial feature regarding Smart Contracts. In parallel with the actual smart contract code, developed either in well known Java or Kotlin, it can natively support also legal prose contracts, in such a way that they could be complementary to classical paper contracts. The adjunct factor is that this kind of contract is signed by all participants and safely stored in the tamper-proof blockchain. In order to ensure the fulfilment of the contract regulations, observer nodes could be included as supervisors, upon the access permission to the ledger has been granted. The ledger is updated using transactions, which change its state. Transactions have to be *valid*, meaning their smart contract code runs successfully and has the needed signatures, and *unique*, there is no other transaction which evolves from a previous state. The consensus on the transaction is reached only by parties involved in that transaction, i.e. only those parties share these data. It has to be noted that in this kind of ledger there is no concept of PoW, thus there is no way in which a quantum computer could attempt an attack on mining capabilities of the network. Moreover, it does not use a native cryptocurrency, which means it is easily integrable in current financial applications without the hassle of forcing the involved parties into adopting another currency.

7.3 IOTA

The other option is not based on the blockchain, but on the concept of *tangle*. IOTA [19] is an open-source cryptocurrency for the Internet-of-Things (IoT) industry. The main feature of this novel cryptocurrency system is the so-called tangle, a directed acyclic graph (DAG) for storing transactions. It is made to be used also by small nodes with not much computing power. In fact, it is best suitable in *Machine-to-Machine* (M2M) micropayment applications, where the transaction fee could be larger than the actual amount of exchanged money. This kind of approach could be very useful if applied to the various use cases described before.

In order to issue a transaction, a node has first to verify two previous transactions. Unlike in classical blockchain ledgers, where there are transaction issuing nodes and mining nodes (with great computing power), in IOTA it is sufficient to check two previous transactions, while yours will be checked by some subsequent one. In this way, the IOTA ledger results in being transaction fee-free, re-balancing the roles of the participants in the network.

It has to be noted that the IOTA network is asynchronous. Nodes in the network may or may not see the same set of transactions from which to choose the two to validate. Moreover, nodes do not have to reach consensus on what transaction has the right to stay in the ledger. Thus, all transactions can be in the ledger, but only the ones fulfilling some particular requirements will be actually validated, others will be orphaned. The particular requirements are defined in the *tip selection algorithm*, which has flexible metric helping in the choice. One of the basic ideas is: the more a node is involved in the verification, the less likely its transaction will be rejected. Thus, a node still has incentive in participating the network even if not issuing any transaction. IOTA developers present the definition of *weight* of a transaction, which is proportional to the work produced by the issuing node for it. The higher the weight, the more important the transaction.

Given its different structure, a tree instead of a chain, this kind of ledger is more flexible with respect to classical blockchain. Moreover, for what concerns its resistance to quantum threats, since there is no mining, such an attack could not be tempted. Instead, a *large weight* attack could be

carried out, but it is sufficient to block this at the protocol level, imposing a limit on the maximum transaction weight. The time spent validating some transaction is not so different from the time required to perform several tasks to issue a transaction, thus there is not much advantage in using a quantum computer applied to this kind of ledger.

The foundation is intensively working on Qubic [20], a name which comes from quorum-based computation. This platform is not intended to simply handle smart contracts, but involves the use of oracle machines to bridge the physical and a parallel, logical world, also featuring the outsourcing of computing powers for IoT device to use it at disposal.

8 Conclusion

As discussed in the past sections, the blockchain approach and specifically smart contract capabilities have changed the aspect of supply chain future and payment for goods. These technologies have been safe enough until now but might not be so safe in the future.

We discussed the possible advantages of using a quantum computer to solve problems that could not be solved in the past in a very short time and how this becomes a threat for current DLTs. It is now the time in which quantum computers are actually rebooting computing and actions have to be taken now because the future may come sooner than we think. This is why some big enterprises and research centers are already trying to exploit these advantages riding this new wave.

As shown before, there are some companies which are offering the quantum-proof DLTs solutions based on quantum-resistant algorithms: QRL, Corda (R3) and IoTa. Moreover, some of them also provide Smart Contract capabilities which can be very effective for the presented use-cases.

We foresee other possible alternatives will come out very soon to exploit the usefulness of blockchain and to tackle its threats.

References

[1] T. M. Fernández-caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[2] G. Strawn, "Blockchain," *IT and Twenty-First Century Employment*, vol. 21, no. 1, pp. 91–92, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8657387/

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[4] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on Bitcoin, and how to protect against them," pp. 1–21, 2017. [Online]. Available: http://arxiv.org/abs/1710.10377%0Ahttp://dx.doi.org/10.5195/ledger.2018.127

[5] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, Oct. 2008," *URL http://www. bitcoin. org/bitcoin. pdf.(cited on pp. 15 and 87)*, pp. 1–9, 2008.

[6] A. Back, "Hashcash - A Denial of Service Counter-Measure," *Http://Www.Hashcash.Org/Papers/Hashcash.Pdf*, 2002.

[7] "Image created using Creative Commons icons found in www.onlinewebfonts.com/icon."

[8] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, 1997.

[9] "Ethereum Project." [Online]. Available: https://www.ethereum.org/

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," pp. 212–219, 1996. [Online]. Available: http://arxiv.org/abs/quant-ph/9605043

[11] V. Gheorghiu, S. Gorbunov, M. Mosca, and B. Munson, "Quantum-Proofing the Blockchain," *Blockchain Research Institute (BRI)*, no. November, 2017.

[12] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 1994, pp. 124–134. [Online]. Available: http://ieeexplore.ieee.org/document/365700/

[13] "Round 2 Submissions - Post-Quantum Cryptography — CSRC." [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

[14] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," 2012, pp. 1–6. [Online]. Available: https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf

[15] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, and T. Schroeter, "Blockchained Post-Quantum Signatures," 2018.

[16] "QRL - The Quantum Resistant Ledger." [Online]. Available: https://theqrl.org/

[17] P. Waterland, "Quantum Resistant Ledger (QRL)," Tech. Rep. October, 2016. [Online]. Available: http://theqrl.org/whitepaper/QRL_whitepaper.pdf

[18] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda : An Introduction," pp. 1–15, 2016.

[19] S. Popov, "The Tangle," 2018.

[20] "Qubic: Quorum-based Computations - Powered by IOTA." [Online]. Available: https://qubic.iota.org/

Edoardo Giusto Edoardo Giusto obtained the B.S. degree in 2015 and M.S. degree in 2017 from Politecnico di Torino. He is currently a Ph.D. Student at the Department of Control and Computer Engineering at Politecnico di Torino. His research interests include WSNs, IoT, Smart Societies and Quantum Computing.

Mohammad Ghazi Vakili Mohammad Ghazi vakili received the B.Sc in Telecommunication Engineering and the M.Sc. degree in Mechatronic Engineering from Politecnico di Torino University, Italy, in 2017. He is currently a Ph.D. student at the Department of Control and Computer Engineering at Politecnico di Torino, Italy. His research interests concern Industry 4.0 (future of factories) focus on Automation, Industrial Networks, and Quantum Computing in Industry 4.0.

Filippo Gandino Filippo Gandino obtained his M.S. in 2005 and Ph.D. degree in Computer Engineering in 2010, from the Politecnico di Torino. He is currently an Associate Professor with the Department of Control and Computer Engineering, Politecnico di Torino. His research interests include ubiquitous computing, RFID, WSNs, security and privacy, network modeling and digital arithmetic.

Claudio Demartini Claudio Demartini is currently a Full Professor with the Politecnico di Torino, where he teaches information systems as well as innovation and product development. He is also the Chair of the Department of Control and Computer Engineering and a member of the Academic Senate of the Politecnico di Torino. His research interests include software engineering, architectures, intelligent systems, and education.

Bartolomeo Montrucchio Bartolomeo Montrucchio received the M.S. degree in electronic engineering and the Ph.D. degree in computer engineering from the Politecnico di Torino, Turin, Italy, in 1998, and 2002, respectively. He is currently an Associate Professor of Computer Engineering with the Department of Control and Computer Engineering, Politecnico di Torino. His current research interests include image analysis and synthesis techniques, scientific visualization, sensor networks, RFIDs and quantum computing.