

Received January 31, 2021, accepted February 27, 2021, date of publication March 8, 2021, date of current version March 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3064297

MuReQua Chain: Multiscale Relativistic Quantum Blockchain

GERARDO IOVANE 

Department of Computer Science, University of Salerno, 84084 Fisciano, Italy

e-mail: giovane@unisa.it


ABSTRACT In this paper, we introduce a new approach to fix the validation of a block and the assignment of a new block in a blockchain infrastructure by using a novel negotiation procedure. The block validation and assignment are reached thanks to negotiation procedures based on an extended probability environment. Also, by using a multiscale approach (typical of Complexity Theory) and Quantum and Relativistic Mechanics, the result appears to solve some of the most relevant questions in the Blockchain context, which are the democracy and the randomness of the validator of a block and the assignment of the new one. The selection of actors to mine is invariant concerning the number of addresses, i.e., the coins of owners, which have more chance to be selected generally. This work is the companion of CQKD (Computational Quantum Key Distribution), as we will see in the introduction, where we considered the infrastructural question of the key distribution; also, it is a very effective application of the decision and reasoning in incompleteness or uncertainty conditions as described in the previous and prodromic paper as described in the introduction too.

INDEX TERMS Blockchain, decision support systems, uncertainty condition, reasoning with incomplete information.

I. INTRODUCTION: THE BLOCKCHAIN AND DECENTRALIZED LEDGER TECHNOLOGIES

This work completes the results in [1] by using the paradigm in [2] into the context of blockchain. While at the launch of Bitcoin, the term blockchain was associated exclusively with digital coin transactions, after ten years, we understand how broad the transaction term is and how it can refer to transactions that are not only financial. The blockchain or, more generally, digital ledger technologies (DLTs) have many applications, such as:

- the transcription of acts in registers, which are immutable over time (digital contract, smart contract, etc.);
- the digitization of put and call agreements;
- the digitization of taking off agreements;
- the securitization of assets;
- the register of titles (such as educational and academic ones);
- the creation of tickets, which enable the acquisition of products and services;
- the creation of good discounts for those which are part of an ecosystem;

The associate editor coordinating the review of this manuscript and approving it for publication was Srinivas Sampalli .

- the distribution of personal, group, or collective vouchers, etc.

Even today, the scenario is evolving; just think of the misuse of terms. For example, we often refer to digital currencies or cryptocurrency by referring to digital coins or complementary coins, whereas by that term, we should refer to instruments issued exclusively by central banks. Therefore, to date, we can more correctly state that there are several crypto coins, no cryptocurrency, multiple tokens. To date, only China announced the imminent introduction of the digital currency E-Yuan. Also, blockchain's scope and potential are still being discovered, as we see new examples of use day by day.

The blockchain has the potential, among other things, to offer participation, democracy, equity, equality, transparency, traceability, security, and privacy at the same time.

Money is becoming virtual, but there are several aspects to deal with, such as:

- 1) transaction security;
- 2) psychological response linked to the lowering of emotion connected to a tool no longer material;
- 3) the confidence of the issuer.

Compared to this last point, it is worth a brief reflection. Confidence in central banks and paper currency lies in

holding currency in our own pockets or our availability. Can we assume the same is true in a digital euro, a digital dollar, a digital pound, a digital yuan, a digital ruble, etc.? Would a consumer show more confidence in a digital currency know that behind it is the banking system or a digital token linked to a productive activity? In the first case, that is, of a bank, there would be the perceived security and security known so far; in the second, there would be confidence that money, to lose value, should see the collapse of productive activity or an economic sector. But in this case, it would also be easy for a common consumer to differentiate his portfolio into different tokens, in a similar way in which multi-currency portfolios are harmonized today. The scenario is very intriguing, and it will be interesting to analyze how public opinion, consumers, and savers will respond.

Blockchain will certainly play a major role in this scenario. We will see the evolution of public ledgers, the competition of permissionless and permissioned solutions, the challenge towards quantum-resistant solutions, the diversification, and the multiplication of use cases. In fact, since the advent of Bitcoin [3] a piece of the road has already been made. The Ethereum [4] solution with its blockchain and smart contract has set another milestone, letting it be understood that transactions can be not only financial but of all kinds and types, from which many blockchain initiatives, of more or less satisfactory value and maturity, have entered the market attracting the curiosity of an increasingly diverse audience.

The latest interesting innovation of thinking regarding blockchain is Algorand [5], which, according to what the founder says, is quite democratic. But why only quite and not totally democratic? Why is a technology such as a blockchain, which aims to offer a tool for democracy and digital governance, itself risks not being democratic? In this work, starting from Algorand's valuable contribution, we will try to take a step forward concerning this intrinsic limit in all blockchains and related to the consent and possession of tokens and addresses, which means that those with more tokens can have more power.

In the present scenario also GSCS (General Secure Consensus Scheme) for decentralized blockchain systems appears of specific interest and suggestion concerning consensus [6].

The focus of this work is centered on two fundamental aspects of blockchain technologies.

- The construction of keys resistant to quantum attacks. Here they are generated by a computational infrastructure, which is intrinsically quantum from a conceptual point of view.
- The generation of consensus based on a negotiation mechanism.

Relative to the first point, each node of the blockchain is a multipurpose node. Moment by moment this node can be functionalized differently, in order to contribute to the creation of keys within the node network. In its entirety, this network will act as a Computational Quantum Key Distributor (CKQD) service provider.

With regard to the second point, each node – interested in mining – will participate in the activities, which will be regulated by the negotiation mechanism. As we will see the negotiation is described thanks to a generalized, relative, multi-level consensus perspective.

The work is organized as follows. In Section II, we introduce a quantum infrastructure, able to resist a quantum attack, as described in [1]. In Section III, we consider the negotiation context by using an extended probabilities paradigm which includes sentiment and consensus as fully described in [2]; later a toy model for negotiating is presented. Then, in Section IV, we realize a realistic model for negotiating, and we introduce some considerations on the fairness of the negotiation price. Finally, the last section deals with the negotiation approach as a consensus mechanism for the blockchain and the assignment and validation of blocks. In addition, Section V introduces the new concept of Financion, i.e., the quantum of the interaction of Financial Field, considered as token and reward for mining; then the section outlines the conclusions.

II. INFRASTRUCTURAL QUESTIONS

A. CQKD (COMPUTATIONAL QUANTUM KEY DISTRIBUTION)

In this section, let us resume the results in [1]. Quantum Resistant Cryptography (QRC) is a very active and current field at date. In this context, algorithms are developed to be secure against attacks by quantum computers. The most popular public-key algorithms are not quantum resistant at date [7], [8]. A very useful review on quantum-resistant infrastructure and blockchain is in [9]. At date QRC research is focused on the following approaches mainly: i) Lattice-based cryptography [10]–[17]; ii) Multivariate cryptography [18]–[21]; iii) Hash-based cryptography [22], [23]; iv) Code-based cryptography [24]; v) Supersingular elliptic curve isogeny cryptography [25]–[27]; vi) Symmetric key quantum resistance [28], [29].

In this broad scenario, this section aims to enhance the ideas behind the work of Bennett and Brassard BB84 [30] taking advantage of the still unexpressed and not totally discovered potential of Distributed Ledger and Blockchain. Here we report a methodology specifically designed for blockchain and distributed ledgers, which, although based on concepts proper to Quantum Mechanics, it can be used whether the channel nodes are physically quantum – as we shall see – that they are “computably quantum,” i.e., standard ones.

Therefore, the use of such a methodology, on the one hand, may encourage the development of quantum nodes, but on the other hand, as a new methodology, it can be used immediately, even on non-quantum nodes and channels.

This work combines at the same time QKD and Distributed Ledger or Blockchain as a conceptual idea and by extending QKD to blockchain environments.

Before we begin the protocol description; we need to define the physical state and its possible functions.

Let us consider a Blockchain with several D nodes. Each $d_i \in D$ node can be in one of the following states:

- i) o-off
- ii) b-busy
- iii) a-active, i.e., idle and ready.

Once the sender Alice verifies nodes' availability to receive a computational load related to key generation and transmission, Alice proceeds to functionalize the nodes. Each node can behave in one of the following functions:

- 1) QSG – Quantum Spin Generator;
- 2) BG – Base Generator;
- 3) QPP – Quantum Photon Polarizer;
- 4) PFE – Photon Fusion Engine;
- 5) QPM – Quantum Photon Meter;
- 6) QPC – Quantum Photon Collider.

Let us look in detail at the IO of the different functions of the nodes, their behavior, and their status.

Typically, a node will receive a statement record which contains the following information:

```
[key_gen_id, process_id, node_type,
  sender_address, receiver_address]
```

where `key_gen_id` will serve to disambiguate competing key construction processes, `process_id` will disambiguate different processes within the same key building process, `node_type` is the type of job you wish to assign to the node, concerning the fixed key generation process (this means that in another key generation process, the same node can act differently), `sender_address` will be the sender address, and `receiver_address` will be the address (i.e., addresses) of the receiver (i.e., receivers) of the specific key generation process (i.e., `key_gen_id`) and subprocess (i.e., `process_id`).

QSG – Quantum Spin Generator. Functionalization of a node of type QSG_i requires that the node randomly choose between spin up or spin down or more easily to generate a random binary digit (i.e., 0 or 1). Therefore, a node, which is functionalized in this way, will put itself in the busy state for the other nodes, it will generate the binary digit, and it will transmit it to the sender Alice and QPP_i receiver addresses; then it will refresh itself, and it will re-enter the active state.

BG – Base Generator. A functionalization of a node of type $BG_{A,i}$ requires that node to behave as a generator of a randomly chosen base between $\perp = (0, \pi/2)$ and $\times = (-\pi/4, \pi/4)$. Therefore, a node that is functionalized in this way will put itself in a busy state. It will generate the base, and then it will transmit the base to the QPP_i receiver address; consequently, it will refresh itself, and it will put itself in the active state.

QPP acts as a polarizer; this means that for each digit to process it obtains a value (i.e. the spin) by the Quantum Spin Generator (QSG), $s \in (0.1) \subset \mathbb{N}_0$. Moreover, for each digit to process it also obtains a base value by the Base Generator (BG), b included into the discrete set: $\{-\pi/4, 0, \pi/4, \pi/2\}$. Then QPP performs the polarization, i.e. projects s on b . For

example, suppose to have a sequence of unpolarized spin s_i given by QSG_i :

1 1 1 0 1 0 1 0

Suppose to have the following basis given by BG_i :

$\perp \perp \times \times \perp \times \perp \perp$

where $\perp = (\rightarrow, \uparrow) = (0, \pi/2)$ and $\times = (\swarrow, \nearrow) = (-\pi/4, \pi/4)$, then the polarizers QPP_i will give at all the following computational polarized photons, i.e. the following polarization string:

$\uparrow \uparrow \nearrow \swarrow \uparrow \swarrow \uparrow \rightarrow$

PFE – Photon Fusion Engine. Functionalization of a node of type PFE requires that the node perform a fusion among the different polarizations received from QPP_i . This job is very delicate, and as we will see, it requires big attention since this node could be fragile. Considering that the node cannot know the order of arrival of polarizations from QPP_i and also taking into account that – for security reasons – does not know how many QPP_i will send it polarizations, it is necessary to functionalize with two more elements from Alice. So Alice has to send the length lk , which is how many QPP_i will send the polarization and the law to sort them. Therefore, for considering this type of nodes, the initialization record transmitted by Alice will be changed in

```
[key_gen_id, process_id, [node_type],
  sender_address, receiver_address]
```

where if the node is of *PFE* type, then

```
[node_type]=[PFE, lk, sorting rule]
```

otherwise, it will be

```
[node_type]=[node_type, 0. 0]
```

Therefore, a node, which is functionalized in this way, will put itself in the busy state for the other nodes, it will perform the polarization fusion, it will transmit to QPM receiver addresses; then it will refresh itself, and it put itself in the active state.

QPM – Quantum Photon Meter. Functionalization of a node of type QPM requires that the node measures the polarization of Alice packet using the bases $BG_{B,i}$ randomly chosen by Bob. This job is delicate, too, as in the previous case, and it requires big attention since this node could be fragile. Considering that the node cannot know the order of arrival of $BG_{B,i}$ – for security reasons too – QPM will ask Bob to send to QPM the following information record.

```
[key_gen_id, [process_id], [node_type],
  sender_address, receiver_address]
```

where `key_gen_id` is the same received by Alice, while `[process_id]` is the vector containing the unique assignment codes given by Bob to the $BG_{B,i}$. In this way, QPM can

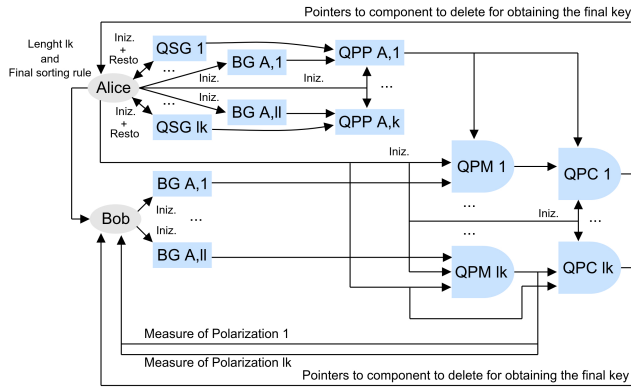


FIGURE 1. An optimized CQKD protocol, with QSG (Quantum Spin Generator), BG (Base Generator), QPP (Quantum Photon Polarizer), QPM (Quantum Polarization Meter), and QPC (Quantum Photon Collider).

process the information and sort the information coming from $BG_{B,i}$ according to Bob's record.

Therefore, for considering this type of nodes, the initialization record transmitted by Alice or Bob will be changed in

```
[key_gen_id, [process_id], [node_type],
  sender_address, reciver_address]
```

where if the node is of QPM type, then

```
[node_type]=[PFE, lk, sorting rule]
```

otherwise, it will be

```
[node_type]=[node_type, 0. 0]
```

while for data coming from Alice

```
[process_id]=[process_id, 0. 0],
```

the [process_id] coming from Bob is

```
[process_id]=[process_id, BGB,1_address,
  BGB,lk_address].
```

Therefore, a node that is functionalized in this way will put itself in the busy state for the other nodes, it will perform the measurements of Alice's polarization in Bob's base, it will transmit to Bob by fragmenting the results on lk $QPP_{B,i}$, and by sending Bob the sorting rule, and it will transmit to QPC receiver addresses the polarization strings of Bob; then it will refresh itself, and it put itself in the active state.

QPC – Quantum Photons Collider. Functionalization of a node of type QPC requires that the node compare two strings of polarization as received by QPM, and it will select the positions where they are equal. Therefore, a node, which is functionalized in this way, will put itself in the busy state for the other nodes, it will perform the matching, and it will send Alice and Bob the correct indexes by indicating to delete the wrong ones; it will refresh itself, and it will put itself in the active state.

Let us see in detail how the protocol works, as schematized in Figure 1.

- 1) Alice measures the length of the code to be encrypted lc and sets a key length of $lk = \lfloor 2.5lc \rfloor$;
- 2) Alice pings the nodes of the Blockchain network and annotate the nodes which respond and are active, noting the number of active nodes $\#(n)$;
- 3) Alice verifies if $\#(n) \geq \alpha$ with $\alpha = 5lk$; if $(\#(n) \geq \alpha) = TRUE$ then select the first α nodes randomly, else Iteration Jobs $IJ = \lceil \alpha / \#(n) \rceil$ and she allocates IJ jobs per node;
- 4) Scrolling the list of nodes from top to bottom, Alice chooses the nodes which will operate as QSG; if $\#(n) < lk$ she will assign more than one job of this type to the nodes;
- 5) Scrolling the list of nodes from bottom to top, Alice chooses the nodes which will operate as BG; if $\#(n) < lk$ Alice will assign more than one job of this type to the nodes automatically;
- 6) Alice selects for each pair $(QSG)_i - (BG)_{A,i}$ a $(QPP)_{A,i}$;
- 7) Alice opens a unique transaction ticket, $id_process$;
- 8) Alice transmits the following command to each node

```
[id_process, id_subprocess, node_type,
  num==0. send to: Address 1, Address 2];
```

if $node_type$ is type QSG, the node will return Alice as address 1 and a QPP as address 2 the value of the spin; if $node_type$ is type BG, the node will return the randomly selected base component only to address 2 i.e. QPP;

if $node_type$ is type QPP, the node will return the polarization value into the base BG to address 2 i.e. to QPM;

- 9) Each node carries out its job and transmits the result to the competent nodes in the following format

```
[id_process, id_subprocess, result]
```

- 10) Alice receives lk QSG values, starting from the table of the received records as

```
[id_process, id_subprocess, node_type,
  num, send to: Address 1, Address 2],
```

and she generates a new random order by changing the order of the records;

- 11) Alice notifies Bob the length lk of the key, the final sorting rule to rearrange the results coming from QPC, and the QPM address in the following format

```
[id_process, lk, sorting rule,
  send to: address 2==QPM];
```

- 12) Bob proceeds as Alice in step 2;
- 13) Bob proceeds as Alice in step 3;
- 14) Bob checks if $\#(n) \geq lk$ and proceeds similarly to Alice in step 5;

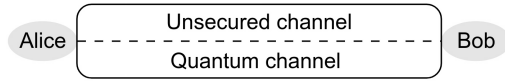


FIGURE 2. A classic BB84 scheme.

- 15) Bob assigns lk jobs to the nodes, which will operate as $(BG)_{B,j}$ with $j = 1, \dots, lk$, giving them the following command

```
[id_process, id_subprocess,
    node_type==BG, value,
    send to address2==QPM];
```

- 16) For each $id_process$, QPM will receive from QPP a polarization state and from Bob, i.e., $(BG)_{B,j}$, the verses;
- 17) According to the rules of the Quantum Mechanics – that is by working as polarization projector – QPM will match a record, that is it will represent the polarization of a photon by Alice along the base of Bob and will return (without keeping copies): i) to Bob the respective polarizations and ii) to QPC each polarization of Alice and that one measured by Bob;
- 18) QPC will perform the collision and notifies Bob and Alice of the pointers to the correspondents of the key that must be deleted;
- 19) Bob and Alice will perform the sorting of records according to the order given by Alice to Bob, and they carry out the cancellation by getting the final key with which to encrypt the message if the final length $l > le$, otherwise, Alice will command to start the process again until $l > le$.

In principle, a similar decentralized solution can also work without encryption since an attacker Eve to reconstruct the key need to have control on the total set of nodes involved in the key construction; this means $6lk$, or a smaller number than $6lk$ if the active nodes are a limited number smaller than $6lk$, but in this case, Eve must be persistent, i.e., she must have the control of the nodes and be able to synchronize the sniffed results. We can understand that an Eve action is theoretically possible, but it is not effective.

We started from a scheme of BB84 to realize one-time pad encryption, which can be sketched as

The strength was the approach to send on the unsecured channel just information of good pointers to extract a reduced key, while on the quantum channel, the polarization.

B. AN OPTIMIZED CQKD

Suppose we introduce two computational quantum components, named Quantum Photon Transmission Component (QPTC) and Quantum Photon Receiver Component (QPRC). In that case, the protocol shown in Figure 1 can be arranged in the following conceptual and fascinating way easily by taking into account that QPTC and QPRC are decentralized, as sketched in Figure 3.

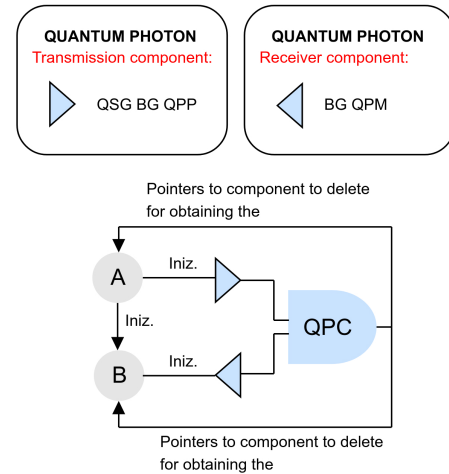


FIGURE 3. A blockchain oriented BB84 scheme.

Here in the following, we present a new way to use the power of nodes and a decentralized ledger and blockchain to decentralize the key construction for exchanging a message peer to peer. This is made by using Quantum Mechanics, but in a novel vision based on BB84, named Computational Quantum Key Distribution (CQKD), where the nodes act as agents to generate dynamically and randomly: i) Spin (QSG), ii) Base of Representation (BG), iii) Photon Polarization (QPP), iv) Quantum Measure (QPM), v) Quantum Collision (QPC).

The present approach's beauty is that it can work with any kind of channel, secured and unsecured, common communication network, wi-fi, light-fi, quantum via fiber optics, and any combination of the infrastructure used by users at the date.

We can observe the key generation process can be considered as a mining process; it can be done autonomously and continuously by the nodes organized in the mining pool to produce key at any time and distribute the keys immediately and just in time when an Alice and a Bob need to exchange peer to peer a message. This is strongly effective and shows the power of blockchain and distributed ledger clearly.

By taking into account the full decentralization of the key products, the communication channels could also be unsecured ones in principle. But nothing prevents you from using Perfect Forward Secrecy or PFS as we tested if the number of nodes is very small, according to [26], [31]. As it is known since the end of 2011, Google has provided forward secrecy with Transport Layer Security (TLS) by default to users of its Gmail e-mail service, together with Google Docs and encrypted search among its services. In late 2013, Twitter also introduced this service to its users, and Microsoft said it would implement it. About 50% of sites that enable TLS to support some cipher suites which provide forward secrecy. In November 2014, WhatsApp said it had introduced end-to-end chat encryption in the latest release, limited to the Android version, excluding multiple chats and chats

containing multimedia messages. This guided our choice of the first test with further security of the transmission channels, but nothing prevents us from using other techniques such as ECDH, for example. As mentioned above, this additional security measure makes sense only if you operate in contexts where an attacker could take control of the entire network or all its nodes, vice versa encryption of key fragments becomes unnecessary, as the CQKD is intrinsically secure, thanks to the two basic supporting ideas, i.e., a dynamic and evolving procedure for generating key fragments by network nodes via Quantum Mechanics Principles (i.e., intrinsic crypto agility), the total distribution of key production (decentralization). Another element to consider is that the numbers of nodes of a blockchain are larger and larger at the date so that the encryption of key fragments could result in a surplus in common communication, thanks to the decentralization.

III. NEGOTIATION AND CONSENSUS

A. INTRODUCTION TO NEGOTIATION CONTEXT

As known in any commercial activity, the price does not coincide with performance, product, and service value. For example, in the real estate sector, it is common to find properties at a price lower than the construction price in times of crisis, as well as a speculative bubble time, the price can be even 20 times greater than the construction value.

The target of this section does not concern the formulation of a price model. It aims to offer a negotiation model between the parties that is based on info-uncertain and info-incompleteness. In other words, the objective is the realization of a negotiation model based on knowledge in conditions of incomplete information or uncertainty of information, that is, a real operating condition, which is normally far from the current theoretical price models.

The result will be an advanced methodology based on a new concept of the negotiated price, which will be obtained by extending the probability concept to that of occurrence.

In turn, the distribution of occurrence will be obtained from the linear combination of the distribution of probability, plausibility, credibility, and possibility, as we will see better below.

We call bid price the price of who offers a product or service; we associate to the bid price the distribution of credibility based on the seller's experience.

We call ask price the offer of who intend to buy and that based on his/her experience he/she will formulate the chosen price within the distribution of possibilities.

We call plausible price the offer made by a group of experts to buy or link the price-value combination to the distribution of plausibility.

Finally, we indicate with the probable price the most probable market price considered with its probability distribution.

The approach that we are going to describe below leads to more plastic modeling of reality than probabilistic models; instead of the probability associated with the price, we would have the occurrence $A(p)$, which is expressed by the following

distribution:

$$A(p) = \sum_{i=1}^4 a_i P_i(p_i) \quad (1)$$

with $\sum_{i=1}^4 a_i = 1$ and where $P_i(p_i)$ are distributions as follows:

- $i = 1$: $P_i(p_i)$ represents the probability P_1 of the price p_1 ;
- $i = 2$: $P_i(p_i)$ represents the plausibility P_2 of the price p_2 ;
- $i = 3$: $P_i(p_i)$ represents the credibility P_3 of the price p_3 ;
- $i = 4$: $P_i(p_i)$ represents the possibility P_4 of the price p_4 .

As for the probability distribution, we will have $0 \leq A(p) \leq 1$, where $A(p) = 0$ will correspond to an unacceptable price p , while $A(p) = 1$ will indicate an imposed price.

This extension of probable events was introduced in [2] for describing real contexts that occur in more than the standard probability describes.

The following random pairs represent the different prices with their relative probability, plausibility, credibility and possibility distributions: $[p_i, P_i(p_i)]$.

Corresponding to the distribution of occurrence, we will have the negotiated price defined as

$$p = \sum_{i=1}^4 \beta_i p_i \quad (2)$$

with $\sum_{i=1}^4 \beta_i = 1$. It is clear that such a model lends itself to commercial activities, to commercial activities with consent mechanisms such as in blockchain, to auctions, to online auctions with consent mechanisms, and more generally to any negotiation and negotiation activity with consent mechanisms. Such a model can be considered as a competitive-cooperative model dominated by knowledge and normalized by experience. Indeed, prices between the two main players compete and contrast with each other, but they are dominated by the plausible price and normalized by the probable price, as we will see below.

B. A TOY MODEL FOR NEGOTIATING

This section creates a toy trading model by analyzing the possible cases and the buy and sell options. This model will be prodromal to create a more realistic model.

The following figure shows Alice (asker) and Bob (bidder) as counterparties to negotiation and at the same time a "gas" of operators.

Conceptually, the process can be outlined in the following steps:

- 1) Alice (A) intends to buy and makes an offer a ;
- 2) Bob (B) intends to sell and formulates the offer price b ;
- 3) C_i are trading operators who are chosen (i.e., randomly extracted from the gas of operators) to make an offer based on their experience of value (or they are operators who have registered for an auction, etc.). Each C_i makes an offer o_i . In general, the operators C_i (at least three

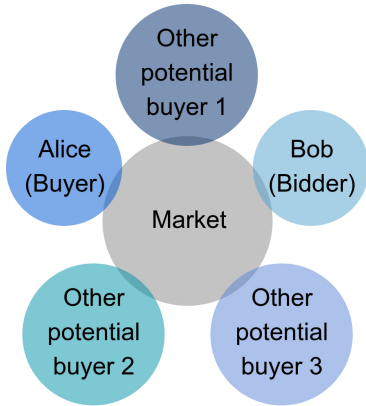


FIGURE 4. Buyer, seller, and market makers.

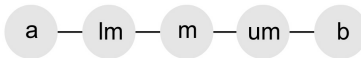


FIGURE 5. Segmentation of prices.

operators) are interested in the sale or as potential buyers or for the negotiation operation to be concluded.

We divide the difference between the ask price and bid price into regions as in the figure below.

Then, the following options may occur:

- $o_i \leq a$,
- $a < o_i \leq lm$,
- $lm < o_i \leq m$,
- $m < o_i \leq um$,
- $um < o_i \leq b$,
- $o_i > b$,

where lm means lower mean value, m means mean value and um means upper mean value; formally,

- $m = (a + b)/2$,
- $lm = [a + (a + b)/2]/2 = (3a + b)/2$,
- $um = [(a + b)/2 + b]/2 = (a + 3b)/2$.

C. POSSIBLE CASES

Below, we report the possible scenarios which may occur concerning the offers of operators other than the asker and the bidder.

- 1) Low Attractor: all additional buyers C_i present a bid less than or equal to lm ;
- 2) High Attractor: all additional buyers C_i present a bid greater than or equal to um ;
- 3) Central Attractor: all additional buyers C_i present an offer o_i in the range $lm < o_i < um$;
- 4) Low Concentration: 2 out of 3 (or at least 66%) of additional C_i buyers have an offer of less than um ;
- 5) High Concentration: 2 out of 3 (or at least 66%) of additional C_i buyers have an offer greater than lm ;
- 6) Equilibrium: each buyer C_i presents an offer into the different sub-intervals: less than lm , between lm and um , greater than um respectively.

D. BUY AND SELL OPTIONS

Concerning the six possible cases described above, the following may occur.

- 1) The price is fixed at lm .
 - A can make the offer at a price lm ; if B accepts, the operation is completed;
 - if A does not formulate the offer and B has accepted the price lm , the operator C_i with an offer o_i closest to lm wins the purchase;
 - if B does not accept the price lm , then the goods/services are withdrawn from sale.
- 2) The price is set at um .
 - A can make the offer at a price um ; if B accepts, the operation is completed;
 - if A does not formulate the offer and B has accepted the price um , the operator C_i with an offer o_i closest to b wins the purchase;
 - if B does not accept the price um then the goods/services are withdrawn from sale.
- 3) The price is fixed at $p = \max(o_i)$ with $i = 1, 2, 3$.
 - A can exercise the right of pre-emption and makes the offer at a price p ; if B accepts, the operation is completed;
 - if A does not formulate the offer and B has accepted the price p , the operator C_i with an offer $o_i = p$ wins the purchase;
 - if B does not accept the price p then the goods/services are withdrawn from sale.
- 4) The price is fixed at $p = [(2lm + m)/3] = [(2a + b)/3]$.
 - A can exercise the right of pre-emption and makes the offer at a price p ; if B accepts, the operation is completed;
 - if A does not formulate the offer and B has accepted the price p , the operator C_i with the highest offer wins the purchase, paying the price p ;
 - if B does not accept the price p then the goods/services are withdrawn from sale.
- 5) The price is fixed at $p = [(m + 2um)/3] = [(a + 2b)/3]$.
 - A can exercise the right of pre-emption and makes the offer at a price p ; if B accepts, the operation is completed;
 - if A does not formulate the offer and B has accepted the price p , the operator C_i with the highest offer wins the purchase, paying the price p ;
 - if B does not accept the price p then the goods/services are withdrawn from sale.
- 6) The price is fixed at $p = m$.
 - A can exercise the right of pre-emption and makes the offer at a price p ; if B accepts, the operation is completed;
 - if A does not formulate the offer and B has accepted price p , the operator C_i with the highest offer wins the purchase by paying the price p ;

- if B does not accept the price p then the goods/services are withdrawn from sale.

IV. A REALISTIC MODEL FOR NEGOTIATING

Starting from the negotiation model described above and the previous toy model, let us try to create a realistic negotiation model. The solution we propose is based on a competitive model, i.e., the seller and the buyer are conflicting on the price and therefore negotiate to take advantage of the deed of sale. The model we are studying here is a knowledge-based model, mainly because the seller in formulating the bid price considers his historical price base about a series of Critical Success Factors (CSF) such as the cost of acquiring raw materials, transformation and production costs, promotion and marketing costs, research and innovation costs, after-sales assistance costs, scarcity or abundance of the product or equivalent products on the market, etc. Furthermore, both the seller and the buyer have specific skills or experiences related to negotiation. Therefore, the model considers not only knowledge (i.e., competencies) and experience (i.e., skills). Thanks to at least three third-party operators or potential buyers, who participate in the negotiation, the model is also cooperative and competitive. In this way, the different operators become an active part in the construction of the negotiation price. These latter operators also use knowledge and skills and therefore confirm what has already been anticipated. It is a model of construction of the negotiating price, which is competitive-cooperative, dominated by knowledge, and normalized by experience, as we will better clarify with the following example.

Let us go back to the example of the previous toy model and let b be the bid price, or the credible price, with its base of experience and knowledge represented by the distribution of credibility $C_r(p_{bid})$; let a be the asking price, with its base of experience and knowledge given by the distribution of possibilities $P_0(p_{ask})$. In this study for simplicity, we assume that although different from a cognitive point of view, competencies and abilities converge indiscriminately in knowledge, that is, as a whole, in the respective distributions of credibility and possibility, as it will happen later for the distribution of plausibility and probability. Let p_i (with $i \geq 3$) be the prices formulated (i.e., the offers) by the three operators-observers interested in the negotiation if the buyer is not interested in paying the final negotiating price. Furthermore, let $Pl(p_{obs})$ be the plausibility distribution of the price proposed by the observers-operators with a mean value $p_{obs_mean} = \sum \frac{p_i}{n}$. Let us analyze how the toy model is transformed into the present realistic model for the six cases considered previously.

- 1) We define the negotiation price as

$$p = \rho_1 p_{bid} + \rho_2 l_m + \rho_3 p_{ask}$$

with $\sum \rho_i = 1$ and $\rho_2 \geq \rho_1 + \rho_3$. Without an information base coming from machine learning, a reasonable choice could be $\rho_2 = 0.5$ and $\rho_1 = \rho_3 = 0.25$; it

means that the negotiation price is dominated by the third operators, but is normalized by all the operators.

- 2) The present case is similar and specular to the previous one, providing the following negotiation price

$$p = \rho_1 p_{bid} + \rho_2 u_m + \rho_3 p_{ask}$$

with $\sum \rho_i = 1$ and $\rho_2 \geq \rho_1 + \rho_3$, with the same conditions on the ρ_i weights.

- 3) By defining $p_{obs-max} = \max\{p_i\}$ the maximum offer produced by the three observers, the negotiation price follows as

$$p = \rho_1 p_{bid} + \rho_2 p_{obs-max} + \rho_3 p_{ask}$$

with $\sum \rho_i = 1$ and different possible chooses for ρ_i . In this scenario, there are several reasonable choices about the importance to give to observers or co-participants in the negotiation. The condition $\rho_2 \geq \rho_1 + \rho_3$ continues to apply, but there are different ways of achieving it, such as, for example, $\rho_2 = 0.6$ and $\rho_1 = \rho_3 = 0.2$, but also about a case dominated by observers as $\rho_2 = 0.8$ and $\rho_1 = \rho_3 = 0.1$, or a case still more extreme that we could define full dominated, i.e., $\rho_2 = 1$ and $\rho_1 = \rho_3 = 0$. Experience in complex systems, as well as the logic of consensus, suggest dominated and fully dominated approaches, such as the previous scenario, are more equilibrated with respect to the asker and bidder.

- 4) In the present case, the negotiation price is defined as

$$p = \rho_1 p_{bid} + \rho_2 p_{obs} + \rho_3 p_{ask}$$

with $p_{obs} = (2a + b)/3$, $\sum \rho_i = 1$ and different chooses for ρ_i as above, where a general good choice remains $\rho_2 = 0.5$ and $\rho_1 = \rho_3 = 0.25$.

- 5) In analogy with the previous case, the negotiation price is defined as

$$p = \rho_1 p_{bid} + \rho_2 p_{obs} + \rho_3 p_{ask}$$

with $p_{obs} = (a + 2b)/3$, $\sum \rho_i = 1$ and different chooses for ρ_i as above, where a general good choice remains $\rho_2 = 0.5$ and $\rho_1 = \rho_3 = 0.25$.

- 6) This last case is more delicate than the previous ones since the operators do not agree on the price, no attractors are created, much fewer price concentrators. This has stimulated an in-depth study on the distribution of occurrence, which we will analyze in the following section. Meanwhile, here we define the negotiation price as

$$p = \rho_1 p_{bid} + \rho_2 m + \rho_3 p_{ask}$$

with $\sum \rho_i = 1$, $\rho_2 = 0.4$ and $\rho_1 = \rho_3 = 0.3$.

As you can easily see, the third observer operators' weight is slightly greater than the two main operators. Also, here this is not the only reasonable choice; indeed, another one could be $\rho_1 = \rho_2 = \rho_3 = 0.33$, i.e., equipartition of the weights.

Looking at the weights considered in the six previous scenarios, it is also easy to notice that they tend to keep a perfect balance between the buyer and the seller, without benefiting either one or the other. In the following section, we will also analyze cases of distribution asymmetry, that is, how to describe scenarios in which, for some reason, the buyer or seller may have an advantage over the other.

A. CONSIDERATIONS ON THE FAIRNESS OF THE NEGOTIATION PRICE

How much is the negotiation price defined above appropriate? In the scientific field, when dealing with stochastic variables, it is customary to replace the crisp value X of a measure or data with an ordered pair, so-called soft pair,

$$(X_{best}, P(X_{best}))$$

where X_{best} is generally a position index, like the mean value, the median or mode, which best represents the set of measures or data with respect to the single measure or single data and $P(X_{best})$ is the probability with which the data X_{best} may occur. Even if the paradigm exposed here exceeds and extends the classic probabilistic approach by providing the expert opinion of third party operators through the distribution of plausibility and the centrality of the operators of the sale through the distribution of credibility and possibility, we can use the same approach of soft computing, just described, that is to pass from the crisp variable X to the soft ordered pair $(X, P(X))$, thanks to the use of the occurrence distribution and proceeding analogously to what has been seen previously. In other words, the negotiation will not be represented by the negotiating price p , but by the ordered pair $(p, A(p))$, where $A(p)$ represents the occurrence, or the combination of probability, plausibility, credibility, and possibility. In other words, as previously mentioned, the negotiation price becomes a reference for everyone, as the various operators participated in its creation: the seller, the buyer, and third-party operators interested in the negotiation or who were called to participate as expert observers. Here, choosing different weights in front of the different distributions, which compose the occurrence $A(p)$, makes the model extremely versatile. As described in [2] there may be unlikely but plausible phenomena that occur more often than predicted through probability, so there may be unlikely, implausible, but credible and possible phenomena or events. This led the authors of [2] to envision a model that would extend the classical probabilistic model, providing for the role of committees of experts (which generate the plausibility distribution) and of individuals or groups (which generate the credibility and possibility distributions), to include the concept of consensus in a new fashion, different with respect to a lacking and not very responsive probabilistic vision to some current realities. The work in [2] also extends the result in [32]; in fact, while the evidence theory by Dempster-Shafer concerns the plausibility, in [2] the authors considered and modeled also the credibility and the possibility in addition and combination with the classical probability and the plausibility. Thanks to the introduction of

the ordered pair $(p, A(p))$ constituted by the price p and the occurrence of the price $A(p)$, we can evaluate how much the price p of the negotiation is congruous.

- 1) From the analysis of the first momentum we have: i) if $p < p_{best}$, where p_{best} is the mean price of the occurrence distribution, the negotiation gives advantage to the buyer; ii) if $p > p_{best}$, the negotiation gives advantage to the seller.
- 2) From the analysis of the second momentum of the distribution of occurrence, we could estimate the discrepancy of the negotiating price concerning the competitive-cooperative model, dominated by knowledge and normalized by the experience of the operators involved. In other words, the second moment will provide us with information about the dispersion of possible negotiation prices. In the case of occurrence $A(p)$, this dispersion will not be purely probabilistic but will also consider experts' opinion thanks to the plausibility and the positions of the buyer and seller thanks to credibility and possibility, with a consensus view. Furthermore, precisely due to its intrinsic nature, the second momentum expressed as variance or standard deviation calculated on the occurrence distribution will estimate any instability and volatility of the negotiating price.
- 3) Similarly to ordinary Statistics, based on probability, also here concerning the occurrence, the third momentum will provide an estimate of the distribution asymmetry, allowing us to evaluate whether the negotiation is favorable for the buyer (a distribution with left asymmetry and right tail, or unbalanced in ask), for the seller (a distribution with asymmetry on the right and tail on the left or unbalanced in the bid) or fair value (symmetric distribution).
- 4) Finally, the fourth momentum that is the kurtosis of the occurrence $A(p)$, will provide information on the concentration of negotiating prices, that is, prices which are not very concentrated and variable (if the occurrence $A(p)$ is a platycurtic distribution), very concentrated prices (if the occurrence $A(p)$ is a leptokurtic distribution), normally concentrate prices (if occurrence $A(p)$ is a normal distribution).

By negating the Basic Probability Assignment (BPA) for considering the Body of Evidence (BOE) as for Dempster-Shafer, the work by Wu *et al.* [33] gives us relevant support. In fact, [33] gives a new and very interesting classification method in the evidence theory context, where the BPA is negated. In details, the authors arrive at a very effective procedure based on the following five steps: i) generate BPA; ii) calculate the negation of BPA; iii) determine the weight of each body of evidence-based on belief entropy; iv) calculate the weighted mass function; v) data fusion using Dempster's combination rule. This procedure in the present work can be used by using at step five the distribution functions $A(p)$, where we recall the $A(p)$ is a weighted

combination of the probability, plausibility, credibility, and possibility distribution $A_i(p)$ of the price p . Moreover, another customization is made with respect to step three of the procedure, where we can determine the weight of each BOE by considering and evaluating the entropy $E(A_i)$ for each A_i .

V. CONCLUSION: THE NEGOTIATION APPROACH AS A CONSENSUS MECHANISM FOR THE BLOCKCHAIN AND THE ASSIGNMENT AND VALIDATION OF BLOCKS, AND THE FINANCION

This section aims to build a new method of validating the current block and assigning the next block within a blockchain solution. The method that we will describe is based on the price negotiation mechanism described above, suitably customized to create a block validation and assignment mechanism for a blockchain that is intrinsic: i) multiscale (and therefore scalable); ii) quantum (and therefore quantum-resistant); iii) relativistic (and therefore full distributed and so decentralized). Therefore, the solution that we describe, using the fundamentals of Multiscale Analysis, Quantum Physics, and Theory of Relativity, creates an avant-garde blockchain in the international scenario, offering an answer to the main issues currently emerging regarding the potential fragility of blockchain technologies based. The word Lemma generally means a proposition with well-defined hypotheses and incontrovertible proof. Therefore, the statement of S.Micali of the Algorand group about the falsity of the blockchain trilemma is widely acceptable. More correctly, we should have spoken of principle, therefore valid until proven otherwise. The trilemma's questioning was carried out first of all by Algorand and continues to happen also with this paper. In Section II, as in [1], a blockchain architecture core, named CQKD – Computational Quantum Key Distribution, was introduced. It was not simply quantum-resistant but intrinsically quantum. This was possible thanks to a conceptual innovation that we called a computational photon, a polymorphic information packet, which, in analogy to photonic polarization, adapts itself to the transport medium/channel. This gives a new and novel answer to the fundamental aspects of the blockchain relating to: i) nodes or sources of potential attacks and therefore intrinsic fragility of the blockchain regardless of the good faith and correct action of the miners; ii) the full decentralization mechanism; iii) the security of the keys. Inheriting the results of the previous paper [1], the attention of this paper is instead aimed at the consensus mechanism and the assignment of blocks or jobs. Since these are digital tokens, without wishing to enter into the merits, whether they are a digital currency, crypto coin, or tokens, the dematerialization requires and has required everyone's specific attention concerning the issue of forking and double-spending. Even the most traded crypto coins today, such as Bitcoin and Ethereum, have had to take this issue into due consideration to not frustrate the success of their project. Also, the previously mentioned Algorand at MIT, based on its novel and superfast message-passing Byzantine

agreement, has paid great attention to the choice of validation and block assignment and, therefore, to the consensus protocol. In this paper, which completes the previous one [1], we have not left out this aspect too, which we consider so relevant. Specifically, the mechanism adopted here can be considered a conceptual evolution of the already robust Algorand approach. But here, we intend to better regulate the weight of those which work in blockchain to offer the declared democracy, which is one of the aspects known since the initial paper by Satoshi Nakamoto. In fact, in Algorand and Bitcoin, those which own more coins or more addresses are more likely to be extracted and weigh in new blocks' assignments or to validate previous blocks. Without a doubt, anyone who is interested in investing in technology should have no reason to drown it. However, it is equally true that often interest and democracy are not only not synonymous but even have opposite values. Let us then analyze the method proposed here, which aims to be intrinsic: 1. multiresolution, 2. relativistic, 3. quantum. In Section II and in the paper [1], to which we refer, the themes two and three have been widely discussed, precisely because they are of fundamental importance and have a strong architectural impact. They were solved, as mentioned, by introducing the concept of the computational photon, both for the analogy with Physics and for identifying its adaptivity and crypto-agility with respect to the carrier medium or support. What is a photon from a quantum point of view? The photon is the quantum of interaction of the electromagnetic field; in other words, when two entities interact electromagnetically, they exchange photons, from which derives the world that we can observe with our sight, but not only with all the machines that man has built, from those for medical diagnostics to smartphone we use. Just as the photon is a physical model to describe a packet of information in terms of energy and frequency, similarly, a computational photon is the quantum packet of information exchanged by two operators, coming into contact concerning elementary information or more information packets to exchange. Such a conceptual model can be further defined now, in which we will deal with the multiscale effects in a blockchain. Indeed the scalability or better still the scale-invariance which, in analogy to the quantum leaps of an atomic system, when it absorbs and emits photons, allows us to give a name even more specific to the computational photon, defining it as *financion*, or the quantum packet of the interaction of the financial field. The financial field concept is not the subject of this study because the financial context has the mathematical structure of the field with its typical mathematical properties, but the verification is trivial and follows directly from the definition.

For the price negotiation method described above to be considered a consensus and block assignment protocol, it is necessary to constrain some aspects and clarify others.

- 1) Alice (asker) could accept or decline the negotiation at the final negotiated price.
- 2) Bob (bidder) could also refuse the negotiation and collect the goods/services previously offered for sale.

- 3) For the prices presented by the various third party operators, it is necessary to understand what they correspond to in the competition for the allocation of blocks and how the rewards are propagated into the chain.
- 4) Finally, it will be necessary to understand how to choose miners more democratic and less fragile by overcoming the concentration of power or weight present today in all blockchains in relation to the token addresses owned.

The solutions to the four indicated questions are simpler than imaginable thanks to the path presented in paper [1] and thanks to what has developed here above.

Let us see how this is done.

Except for the seller node and the buyer node, not all other nodes can participate in the negotiation. In fact, the other nodes to be drawn and participate in the negotiations must be active, that is, they must be in a position to participate in the construction of CQKD keys. What does it mean? This means that nodes which can apply for post-current block mining are serving the CQKD in one of the possible expected functionalizations, namely QSG, BG, QPP, PFE, QPM, QPC.

For points 1 and 2, we proceed as follows. Token addresses have a time flag, so they are historicized. In general, mining increases in computational complexity over time; therefore, from a historical-statistical point of view, the most remote addresses are generally related to holders with more tokens; from this, it follows a partition of the addresses in classes (for example 3, 5, 7 classes, etc. as the chain increases in size). The first simple way to extract Alice is a random algorithm on the class and rolling between one class and another, i.e., now Alice is chosen from class 1, then from class 2, etc. Who is Alice? Before Alice was the potential buyer, here, concerning the blockchain, she becomes the candidate for the new block assignment to be mined. Who is Bob? Bob was the seller in the product/service negotiation algorithm; here, Bob is the miner who has finished mining the current block and must receive the reward for his work. Which are the other three or more operators participating in the negotiation (or auction)? In this case, they are three of Alice's competitors and chosen randomly and rolling among the classes. This point is essential for the multiscale of the solution; in fact, the partition into classes and the rolling mechanism choose who will mine the next block highly democratic while preserving what has been said about the cooperativeness and competitiveness simultaneously offered by the price negotiation algorithm.

Then, let us consider the process to get a deeper understanding of what happens.

- 1) Bob notifies the conclusion of the activity on block B1, with a Byzantine mechanism similar to that used by Algorand, and the price in a sealed envelope his work to receive the reward.
- 2) Alice is drawn with a random-rolling algorithm.
- 3) Alice makes her offer in a sealed envelope.
- 4) the random-rolling algorithm also draws Alice's three or more competitors.
- 5) The three operators present their offer in a sealed envelope.

- 6) The negotiation price in finacion is calculated and made public.

These six points are preparatory to answer the four questions indicated above.

7. At this point, to always guarantee execution, it is sufficient that Alice's answer about whether or not to accept the price to be paid is a parametric attribute of type random Boolean.

8. Similarly, for Bob, we will have a Boolean = 1, which is unconditional acceptance of the negotiated price.

9. Vice versa, Alice's three or more competing operators will be into the deed only if Alice's random Boolean attribute will be equal to 0 (corresponding to the denial of acceptance of the negotiation price).

10. Whoever wins the next block's mining will pay Bob the reward and start the mining, with no possibility of forking or double-spending.

In conclusion, what has been described here:

- provides answers to the four questions indicated above;
- creates a complete blockchain solution of the new generation, that is a Multiscale Relativistic Quantum Chain (from now on MuReQua Chain);
- solves many of the weaknesses which have emerged to date in the current blockchains and described here, first of all, crypto agility to be quantum-resistant, the scalability, the decentralization, and real democracy;
- introduces the concept of Finacion, understood as the quantum of interaction of the Financial Field, i.e., the quantum of the transactions and the mining rewards.

Future studies and developments must consider:

- massive stress tests to analyze the robustness of the infrastructure;
- pervasive approaches to develop the community, which use MuReQua solution;
- the development of a specific study to analyze the impact of key generations on big number of requests and users.

REFERENCES

- [1] G. Iovane, "Computational Quantum Key Distribution (CQKD) on decentralized ledger and blockchain," *J. Discrete Math. Sci. Cryptogr.*, to be published.
- [2] G. Iovane, P. D. Gironimo, M. Chinnici, and A. Rapuano, "Decision and reasoning in incompleteness or uncertainty conditions," *IEEE Access*, vol. 8, pp. 115109–115122, 2020.
- [3] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://www.bitcoin.org/bitcoin.pdf>
- [4] *Ethereum*. Accessed: Jun. 12. 2016. [Online]. Available: <https://github.com/ethereum/>
- [5] J. Chen and S. Micali, "Algorand," 2016, *arXiv:1607.01341*. [Online]. Available: <http://arxiv.org/abs/1607.01341>
- [6] J. Wang, Y. Ding, N. N. Xiong, W.-C. Yeh, and J. Wang, "GSCS: General secure consensus scheme for decentralized blockchain systems," *IEEE Access*, vol. 8, pp. 125826–125848, 2020.
- [7] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.
- [8] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*. Springer, 2009, pp. 1–14.
- [9] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

- [10] C. Peikert, "Lattice cryptography for the Internet," in *Proc. 34rd Int. Workshop Post-Quantum Cryptogr.*, 2014, pp. 197–219.
- [11] T. Güneysu, V. Lyubashevsky, and T. P. Oprelmann, "Practical lattice-based cryptography: A signature scheme for embedded systems," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Leuven, Belgium, 2012, pp. 530–547.
- [12] J. Zhang, Z. Zhang, J. Ding, M. Snook, and O. Dagdelen, "Authenticated key exchange from ideal lattices," in *Advances in Cryptology—(EUROCRYPT) (Lecture Notes in Computer Science)*, vol. 9057, E. Oswald and M. Fischlin, Eds. Berlin, Germany: Springer, 2015, pp. 719–751.
- [13] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Proc. CRYPTO*, R. Canetti and J. A. Garay, Eds. 2013, pp. 40–56, 2013.
- [14] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, H. Gilbert, Ed. 2010, pp. 1–23.
- [15] D. Stehlé and R. Steinfeld, "Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices," in *Advances in Cryptology—(EUROCRYPT) (Lecture Notes in Computer Science)*, vol. 6632, K.G. Paterson, Ed. Berlin, Germany: Springer, 2011, pp. 27–47.
- [16] C. Easttom, "An analysis of leading lattice-based asymmetric cryptographic primitives," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0811–0818.
- [17] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.
- [18] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," *Advances in Cryptology—(EUROCRYPT) (Lecture Notes in Computer Science)*. Berlin, Germany: Springer, 1988, pp. 419–453.
- [19] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88," in *Advances in Cryptology—(CRYPT) Berlin, Germany: Springer*, 1995, pp. 248–261.
- [20] J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms," *Advances in Cryptology—(EUROCRYPT) (Lecture Notes in Computer Science)*, vol. 1070, U. Maurer, Ed. pp. 33–48, 1996.
- [21] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," *Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Secur.* (Lecture Notes in Computer Science), vol. 3531, J. Ioannidis, Ed. New York, NY, USA: 2005, pp. 164–175.
- [22] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn, "SPHINCS: Practical stateless hash-based signatures," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* (Lecture Notes in Computer Science), vol. 9056, E. Oswald and M. Fischlin, Eds. Berlin, Germany: Springer, 2005, pp. 368–397.
- [23] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," in *Proc. 21st Annu. ACM Symp. Theory Comput. (STOC)*, 1989, pp. 33–43.
- [24] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, E. Dahmen, Eds. 2009, pp. 95–145.
- [25] L. De Feo and P. Jao, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Post-Quantum Cryptography (Lecture Notes in Computer Science)*, vol. 7071, B. Y. Yang, Eds. Berlin, Germany: Springer, 2011, pp. 19–34.
- [26] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Des., Codes Cryptogr.*, vol. 2, pp. 107–125, Jun. 1992.
- [27] X. Sun, H. Tian, and Y. Wang, "Toward quantum-resistant strong designated verifier signature from isogenies," in *Proc. 4th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2012, pp. 292–296.
- [28] R. A. Perlner and D. A. Cooper, "Quantum resistant public key cryptography: A survey," in *Proc. 8th Symp. Identity Trust Internet*, 2009, pp. 85–93.
- [29] M. Campagna, T. Hardjono, L. Pintsov, B. Romansky, and T. Yu, "Kerberos revisited quantum-safe authentication," in *Proc. ETSI Quantum-Safe-Crypto Workshop*, Sep. 2013, pp. 1–18.
- [30] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comp., Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179.
- [31] P. Higgins, "Pushing for perfect forward secrecy, an important Web privacy protection," *Electron. Frontier Found.*, to be published.
- [32] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *Ann. Math. Stat.*, vol. 38, pp. 229–325, Mar. 1967.
- [33] D. Wu, Z. Liu, and Y. Tang, "A new classification method based on the negation of a basic probability assignment in the evidence theory," *Eng. Appl. Artif. Intell.*, vol. 96, Nov. 2020, Art. no. 103985.



GERARDO IOVANE received the Diploma degree (Hons.) from the Nunziatella Military School, the Laurea degree (*cum laude*) in nuclear and sub-nuclear physics, the master's degree in research activities from CERN, Geneva, and the Ph.D. degrees in physics, mathematics, and innovation engineering and economics from the Institute for Advanced Studies in Defense (IASD). He is currently an Associate Professor with the Department of Computer Science, University of Salerno. He has authored monographs and books and more than 150 scientific articles, essays, and speeches for national and international conferences.

• • •