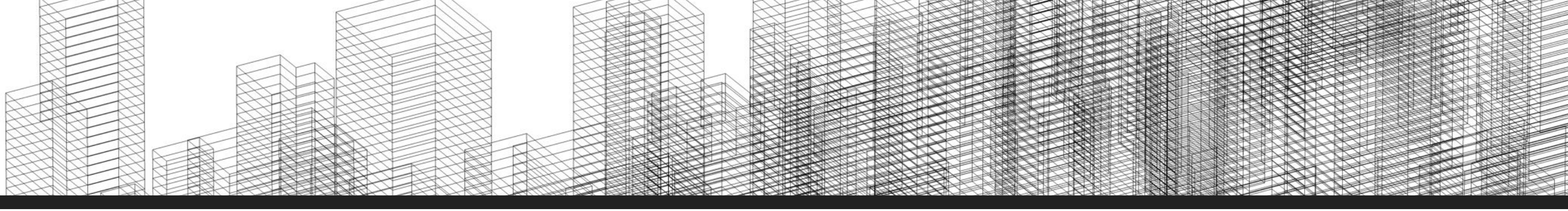
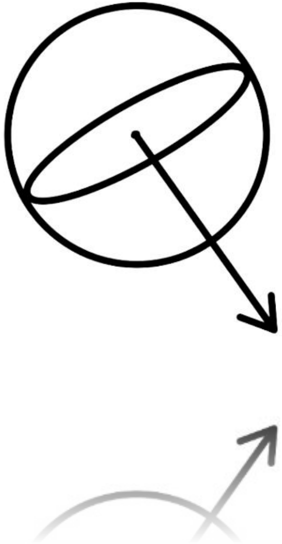




QUANTUM BLOCK CHAIN

Distributed ledger technologies based on Quantum Mechanics

Our Team

Pablo Veganzones

Physicist and Mathematician Theoretical physics master's degree student

Pablo Viñas

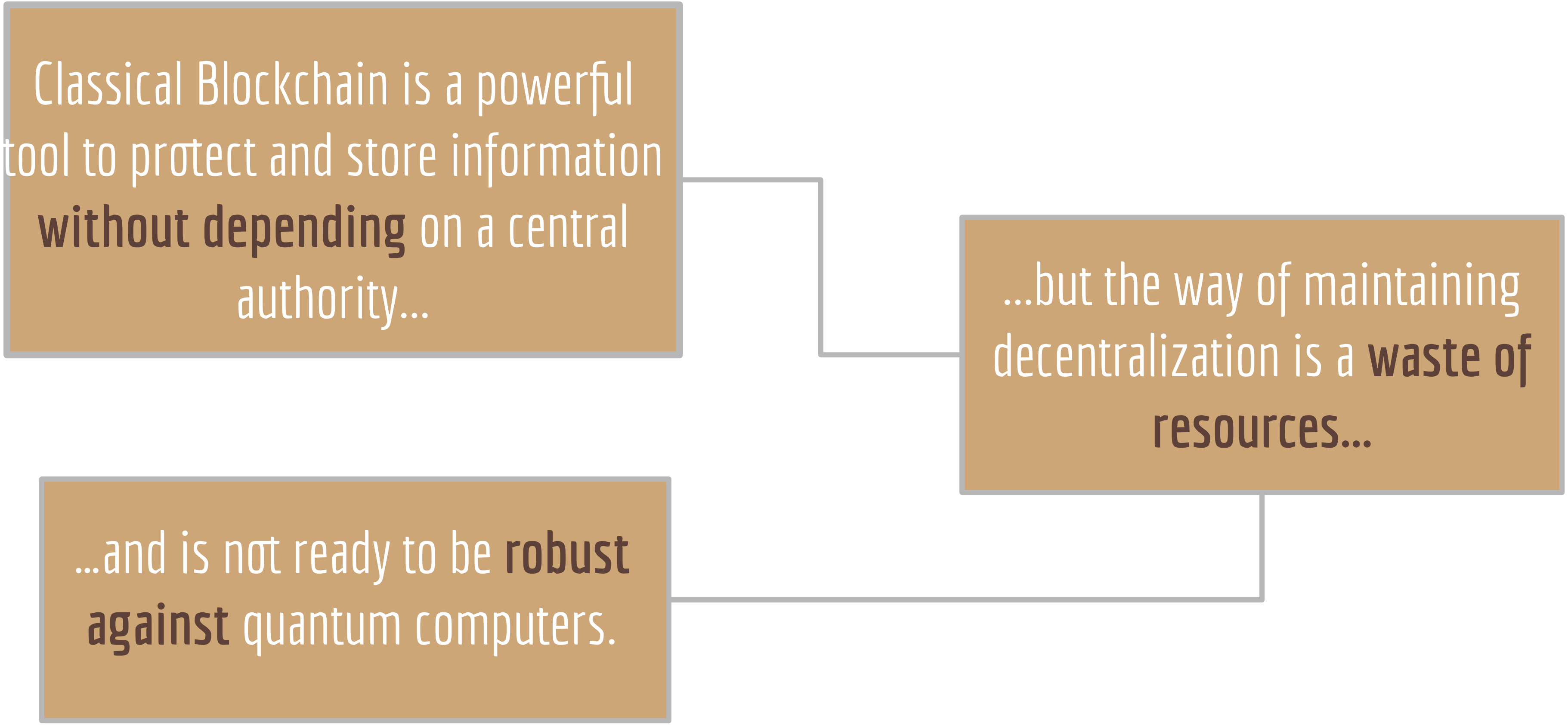
Physicist - Theoretical physics master's degree student

Adriana Palos

Physicist - Theoretical physics master's degree student

Gabriel Escrig

Physicist - Theoretical physics master's degree student



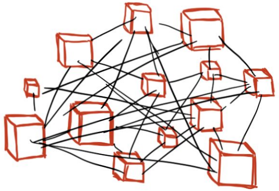
Classical Blockchain is a powerful tool to protect and store information **without depending** on a central authority...

...but the way of maintaining decentralization is a **waste of resources...**

...and is not ready to be **robust against** quantum computers.

Motivation

It seems natural to adapt the blockchain model to:



Maintain the advantages of blockchain technology

Avoid the waste of resources

Be robust against quantum computing

...and we thought ¿QUANTUM?

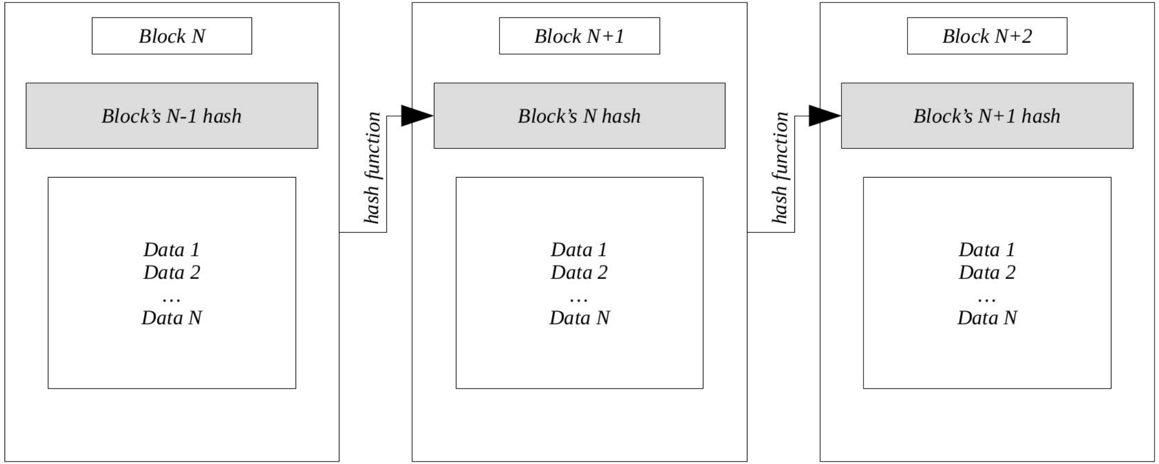
Our Proposal

We explore the advantages of defining a new "Proof of Fidelity" to solve the mentioned problems while maintaining the main purposes of a decentralized system.

We also use quantum random generators and quantum teleportation to make the system secure.

Okay but... ¿What is a Blockchain?

A set of blocks linked to each other...

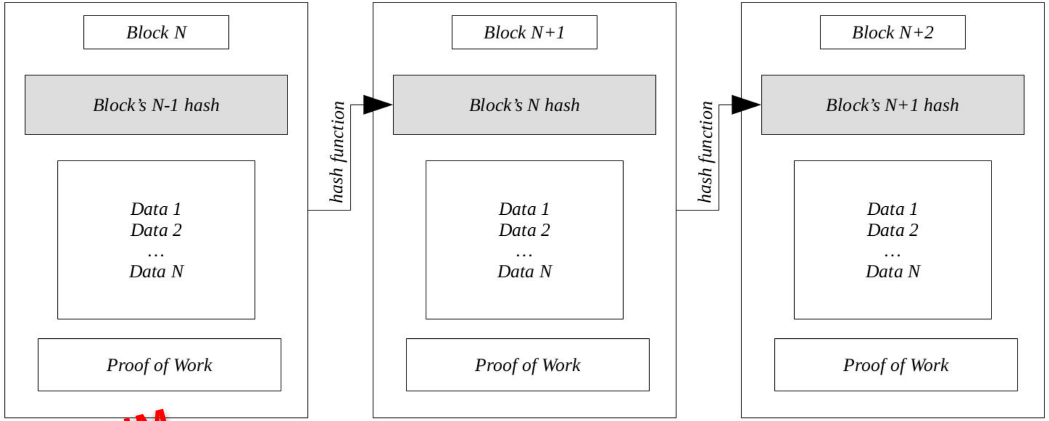


...where each block contains a set of data we want to store

And... ¿The problems?

In some applications such as cryptocurrencies we add a code to each block, known as *proof of work* and must be brute-force tested to obtain a final hash of the block of a specific number of zeros...

WASTE OF RESOURCES



NOT SAFE IN QUANTUM COMPUTING

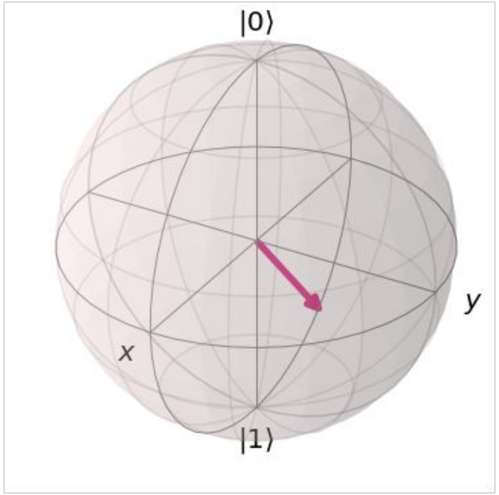
...and the transactions are made with public-key cryptography

Introducing *Proof of fidelity*

If nodes use quantum channels to send states using teleportation, a way to randomize the process is to compare fidelity between all the possible states sent by the quantum channel.

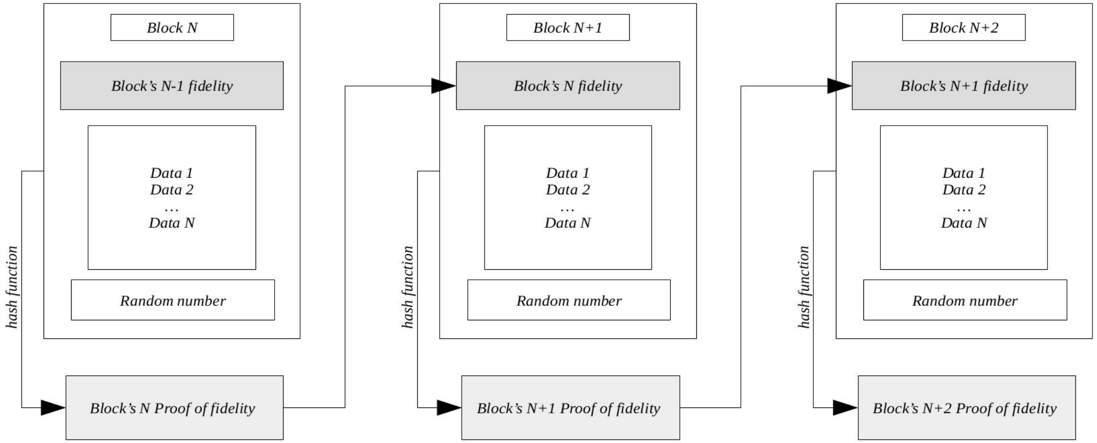
We will define the winner node as the node with maximum fidelity with respect to any of the others (that would have to solve the block). As fidelity is symmetric, a consensus is required to choose a privileged node between the two potential winners.

Also, the process could be deterministic if the order in which one node receives information is known, so a quantum random number generator is used to avoid the problem.



Our blockchain schema

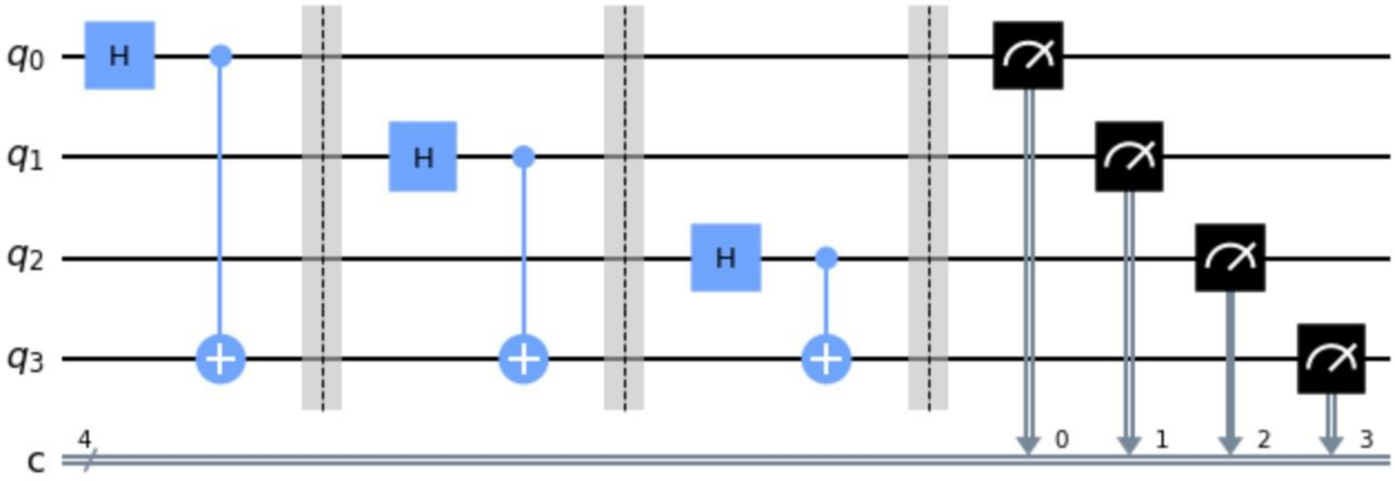
From the fidelity we obtain a connection between one block and the next one, linking them as a chain (since each block would have a different fidelity).



Adding in each block a random number to prevent predictions.

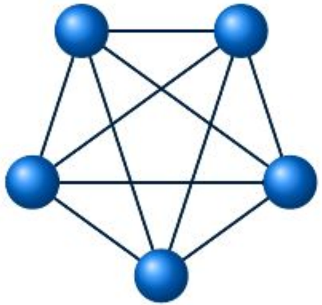
Random number generator

There is no better way to generate random numbers than by using quantum. And the *Qiskit* circuit we used is:



Our Toy Model

In our code we tested this Quantum Blockchain with a 5-node network:



·Simulating transactions in its nodes,

·Creating blocks to pack the transactions

·Calculating all the fidelitys with the hash functions explained in the *Article* to establish the node that will solve the block, and adding it to the blockchain.

Our Toy Model

We can visualize the data stored in a block:

Node	Old Wallet	Random number	Transaction 4	Transaction 5	Transaction 6	Payment	Wallet	prev_fidelity 0	prev_fidelity 1	prev_fidelity 2	prev_fidelity 3	prev_fidelity 4	prev_fidelity 5
0	20.0	100101110	2.0	0.0	0.0	0.6	22.6	0.062924	0.674504	0.145469	0.994129	0.267230	0.748068
1	20.0	1110001	-2.0	3.0	0.0	0.6	21.6	0.776847	0.976582	0.441195	0.092311	0.033508	0.034642
2	20.0	1001000010	0.0	-3.0	-1.0	0.2	16.2	0.960607	0.679451	0.166075	0.058551	0.577587	0.031761
3	20.0	1011100111	0.0	0.0	1.0	0.2	21.2	0.732749	0.988374	0.210153	0.304485	0.477863	0.941506
4	20.0	1100011111	0.0	0.0	0.0	0.2	20.2	0.899596	0.904187	0.802784	0.043552	0.697191	0.343771

Educational Value

The potential of blockchain technologies is undeniable. However, sometimes we forget the underlying science and purposes. That’s because it is easy to get carried away by the hype and... let’s face it, the potential financial benefit.

However, imagine how a quantum blockchain could exploit that fact. A large number of people would be introduced in a practical way to the key concepts of quantum mechanics and quantum computing, sometimes without even realizing it!

Conclusions and future lines of investigation

Through this work, we have reviewed the main concepts of our Quantum Blockchain system and the new concept of Proof of Fidelity. Probably the most important thing to note is that the system is consistent in terms of security without wasting a vast amount of computational power, making its carbon footprint much smaller.

Future investigations could be made involving scalability to a large number of nodes and different schemes of connection between them, as well as the possibility of not only sending, but also storing quantum information.

THANKS FOR YOUR ATTENTION :)

BLOCK CHAIN
QUANTUM